Nevada Enterprise

Prohibited and Controlled Articles Policy

SP-2300.001 (Excerpt)

8.6 / Annex 1

Supersedes: NNSA/NFO "Prohibited and Controlled Articles Policy," 12-15-2014

Prepared by: Mission Support and Test Services, Security Operations

PROHIBITED ARTICLES

The following requirements are issued under the authority of the M&O Contractor and approval by the ODFSA. The following are to be implemented consistently and equally across all NvE organizations, facilities, areas, and operations. This consistent implementation requires all NvE organizations to follow these requirements without the option of imposing more restrictive requirements on facilities, areas, or operations.

Responsibilities

Workers must not bring prohibited articles onto NvE property without proper authorization. Workers who observe the introduction or presence of a prohibited article will contact the OCC at 5-0311 or their FSO.

CPF must conduct appropriate entry and exit inspections (where applicable) of personnel, vehicles, packages, and hand-carried articles in accordance with DOE and NvE requirements. The CPF must follow requirements in general security orders or post orders for unauthorized prohibited articles, as necessary.

M&O Security Operations Section has the primary responsibility for maintaining the prohibited articles policy and coordinating authorization (via SES Director or designee) for prohibited articles on NvE property in accordance with the applicable security plan.

Prohibited Articles List

The following prohibited articles must not be brought on NvE property:

- Firearms and Ammunition
- Explosives
- Dangerous Weapons
- Alcoholic Beverages
- Controlled Substances (e.g., Illegal drugs and associated paraphernalia)
- Pepper spray or mace
- Optical Devices
- Vehicle Cameras
- Global Positioning System (GPS)
- Animals
- Unmanned aircraft (Non-Government)
- Items prohibited by local, state, or federal law

PROHIBITED ARTICLE EXCEPTIONS

Firearms and Ammunition

Government-owned weapons and ammunition for lawfully armed CPF, Office of Secure Transportation personnel, military/military police, federal agents, including investigative officers, federal/military protective detail personnel, and NNSA federal employees are allowed on NvE property if on official business.

Weapons and ammunition for LLEA and armored transportation (vendor) crew (e.g., Loomis) are allowed on NvE property if on official business. The office/individual who is the host must coordinate access with the M&O Security Operations Section prior to the visitor's arrival. When such individuals arrive at the NNSS or NLVF, commercial truck drivers/commercial delivery drivers must present their badges and credentials (if applicable) to the CPF at Station 100 or Station 850. Visitors must declare that they are armed and on official business, and provide the name of the office/individual with which/whom they have business. CPF must verify the provided information by referring to prior written approval by the M&O Security Operations Section or by speaking directly with an M&O Security Operations representative.

Government-owned weapons and ammunition for SPP-approved activities are allowed on NvE property.

At the NNSS, over-the-road truck drivers/commercial delivery drivers are authorized to temporarily store their privately-owned weapons and ammunition (prohibited articles) in a CONEX [container] located within the NNSS truck parking lot, outside of Station 100, south of Building 1002, within a fenced area:

CPF will unlock the gate and the CONEX during working hours and secure the gate and the transportainer during non-working hours.

When drivers request to store their weapons they will be directed to the CONEX.

This service is not for M&O, CPF, or other DOE and/or contractor/subcontractor employees.

Explosives

Government-owned explosives and incendiary devices are only authorized on NvE property in order to perform properly approved work or SPP activities.

Road flares carried as part of vehicle safety equipment are authorized only in a PPA and LA.

Dangerous Weapons

"Dangerous weapon" means a weapon, device, instrument, material, animate or inanimate that is used for or is readily capable of causing death or serious bodily injury, except that such term does not include a pocket knife with a blade of less than 2.5 inches in length.

This requirement does not prohibit workers from possessing knives for official work or fixed blade knives with a blade length longer than 2.5 inches that are to be used in the preparation of food (such as steak knives, cooking knives, cake knives) when in compliance with all other requirements in this SSP.

For interpretation of this requirement, workers should contact a Security Operations representative or their local FSO.

Government-owned items for SPP approved activities are allowed on NvE property.

Alcoholic Beverages

Alcohol sold by NNSS Mercury Cafeteria or Steak House staff, as part of an approved event, is authorized for consumption at that location and NNSS official housing quarters.

Sealed containers are authorized if part of a gift exchange, being held in an individual's private vehicle for an offsite event, or being transported to NNSS official housing quarters.

Controlled Substances

Controlled substances and delivery paraphernalia in the possession of or under the control of Fire and Rescue and Occupational Medicine are authorized.

Legally prescribed (and 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.

Pepper Spray and/or Mace

A single personally owned chemical irritant self-defense dispenser of 2 ounces or less is authorized for possession in a GAA, PPA, or LA. These personal protection devices are not allowed in any Protected Area (PA) or Material Access Area (MAA), no exceptions.

Oleoresin capsicum (OC) spray is authorized to be carried by uniformed CPF personnel.

Optical Devices

Government owned optical devices may be authorized for introduction into security areas, but only when used to perform properly approved work or SPP activities.

Personally-owned optical devices are only authorized for use within PPA, but may not be used at any other security areas under the purview of NNSA/NFO and must be secured in the individual's vehicle at all times.

Vehicle Cameras/Vehicle Event Recorders

Government owned/Government vendor vehicle cameras/vehicle event recorders are authorized in PPA. Government owned/Government vendor vehicle cameras/vehicle event recorders are authorized in LA, Vault/VTR, PA, and MAA, but while there, the recording capability must be disabled.

Personally-owned vehicle cameras are authorized in PPA, but may not be connected to a recording device.

Personally-owned recording devices are allowed introduction into PPA but are not authorized for use and may only be stored within a personal vehicle.

GPS Devices

Government-owned/vendor device GPS function is authorized in all security areas.

Personally-owned GPS devices are only authorized in PPA and LA.

Animals

Service Animal. A service animal is defined as an animal that has been trained to assist or accommodate a person with a disability. Service animals are authorized in all areas unless a safety reason exists. Introduction of service animals into a PA/MAA requires an appropriate 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. Federal, state, and local law enforcement agency personnel, in performance of their duties, are authorized to bring their search animals onto the NvE property.

NOTE: Exceptions not identified above can be submitted to the ODFSA through the SES Director. The requesting organization will provide the SES Director with a justification and supporting information for their request.

Incidents Involving Prohibited Articles

Introducing an unauthorized prohibited article onto NvE property is a reportable security incident. A worker who introduces an unauthorized prohibited article onto NvE property may be subject to disciplinary and legal action. Unauthorized prohibited articles on NvE property may be confiscated by the CPF, other authorized personnel, or LLEAs.

If the CPF or other authorized personnel discover a prohibited article that violates local, state, or federal laws, additional action may be taken (such as contacting an LLEA).

NvE prohibited article requirements do not apply to shared public parking lots for leased facilities.

CONTROLLED ARTICLES

Controlled articles are items that personnel may introduce into NvE Security Areas, after certain conditions have been met (see applicable restriction in the table). These conditions vary depending on the attributes of the article itself as well the Security Area(s) where the article will be present. 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.

Article	Owner	PPA	LA	VAULT VTR	PA MAA	Restrictions
Camera/Recording Device (Audio, video [still or motion]) (If camera/recording device is a Cellular/Smart Phone, then see also Cellular/Smart Phone Restrictions)	DOE/NNSA Managed	(2)	(1) (2) (3)	(1) (2) (3)	(1) (2) (3)	(1) NFO-321 is required prior to device use/introduction to the area. (2) Upon conclusion of the picture taking and/or recording, the device and its media must be reviewed by a Derivative Classifier/Reviewing Official prior to distribution or downloading to an automated information system. (3) When authorized for use in an LA, VTR, PA/MAA, or classified discussion, meeting, or computing area, the device and its media must be controlled as a classified "working paper," protected at the highest level and most restrictive category for which the area is authorized, until reviewed by a Derivative Classifier.
	Non-DOE/NNSA Managed	(1)	⊘	⊘	⊘	(1) See prohibited articles Section 8.6.4.8.3 (vehicle event recorders). Personally-owned Camera/Recording Devices are allowed in PPAs but are not authorized for use, such devices must be stored within a personal vehicle. The restriction to store device within a personal vehicle does not apply to Cellular Phones/Smart, instead see Cellular Phone/Smart section(s) for these types of devices.

Article	Owner	PPA	LA	VAULT VTR	PA MAA	Restrictions
Pagers	DOE/NNSA Managed	✓	(1) (2) (3) (4)	(1) (2) (3) (4)	⊘	(1) This policy does not allow for the introduction into areas where Top Secret, Special Access Program, Sensitive Compartmented information, or Nuclear Command and Control information is stored, processed or discussed or, in TEMPEST protected areas. (2) Devices may not be operated within 10 feet of classified computer systems. (3) Devices may not be operated within 10 feet of equipment copying or faxing classified information. (4) Devices may not be operated within 10 feet of secure communications equipment.
	Non-DOE/NNSA Managed	✓	⊘	⊘	⊘	

Article	Owner	PPA	LA	VAULT VTR	PA MAA	Restrictions
Cellular/Smart Phone (See Camera/Recording Device Restriction of use)	DOE/NNSA Managed	(1) (2)	(1) (2) (3) (4) (5) (6) (7) (8)	(1) (2) (3) (4) (5) (6) (7) (8)	(1) (2) (3) (4) (5) (6) (7) (8)	(1) Hotspot (Wi-Fi) functionality must be disabled. (2) May be used to conduct telephone calls, texting, email, browsing, and other functions, not associated with recording. (3) Cellular Phones/Smart are not authorized in LAs and above. Exceptions can be submitted to the ODFSA through the M&O SES Director. The requesting organization will provide the M&O SES Director with a justification and supporting information for their request. Note that (4)-(7) will be evaluated per request. (4) Cellular Phones/Smart may not be operated within 10 feet of classified computer systems. (5) Cellular Phones/Smart may not be operated within 10 feet of equipment copying or faxing of classified information. (6) Cellular Phones/Smart may not be operated within 10 feet of secure communications equipment. (7) This policy does not allow for the introduction into areas where Top Secret, Special Access Program, Sensitive Compartmented information, or Nuclear Command and Control information is stored, processed or discussed or, in TEMPEST protected areas. (8) NOTE: Cellular Phones/Smart are not authorized to be introduced into these security areas even for the purposes of taking pictures.
	Non-DOE/NNSA Managed	(1) (2) (3) (4) (5) (6)	⊘	⊘	⊘	(1) Hotspot (Wi-Fi) functionality must be disabled. (2) May be used to conduct telephone calls, texting, email, browsing, and other functions, not associated with recording. (3) Audio and video (still and motion) recording functions may not be used. (4) Cellular air cards are permitted. (5) Cellular phones, tablets, and cellular air cards owned by subcontractors and companies doing business with DOE/NNSA are permitted unless otherwise prohibited under any other controls within this policy. (6) Non-DOE/NNSA devices may not be connected to government managed equipment or resources, except where specifically authorized.

Article	Owner	PPA	LA	VAULT VTR	PA MAA	Restrictions
Tablets (iOS, Android, Windows RT Operating Systems) (See Camera/Recording Device Restrictions)	DOE/NNSA Managed	✓	(1) (2) (3) (4) (5) (6) (7)	(1) (2) (3) (4) (5) (6) (7)	(1) (2) (3) (4) (5) (6) (7)	(1) DOE/NNSA managed tablet may be introduced into security areas unless otherwise prohibited under any other controls within this policy. (2) DOE/NNSA or OGA managed tablets must meet the established configuration approved in the respective ISSP by the ODFSA or designee. (3) User shall disable wireless communications technology of the device before introduction. (4) Hotspot functionality must be disabled. (5) Cellular functions (calling, texting, video conferencing) may not be used. (6) Devices may not be operated within 10 feet of classified computer systems, equipment copying or faxing classified information, or secure communications equipment. (7) This policy does not allow for the introduction into areas where Top Secret, Special Access Program, Sensitive Compartmented information, or Nuclear Command and Control information is stored, processed or discussed or, in TEMPEST protected areas.
	Non-DOE/NNSA Managed	(1) (2) (3) (4) (5) (6)	⊘	⊘	⊘	(1) Tablets owned by subcontractors and other companies doing business with DOE/NNSA are allowed if approved by the respective host Security organization unless otherwise prohibited under any other controls within this policy. (2) Use of the “Internet Only” is allowed when approved by the host Cyber Security organization. (3) May not be connected to government equipment or resources. (4) Hotspot functionality must be disabled. (5) Audio and video (still and motion) recording functions may not be used. (6) Devices may not be connected to government managed equipment or resources, except where specifically authorized.

Article	Owner	PPA	LA	VAULT VTR	PA MAA	Restrictions
Computers (Systems with full-featured operating systems such as desktops, laptops, and servers) (See Camera/Recording Device and Cellular/Smart Phone Restrictions)	DOE/NNSA Managed	✓	(1) (2) (3)	(1) (2) (3)	(1) (2) (3)	(1) DOE/NNSA managed computers may be introduced into security areas unless otherwise prohibited under any other controls within this policy. (2) DOE/NNSA or OGA managed computers must meet the established configuration approved in the respective ISSP by the ODFSA or designee. (3) User shall disable wireless communications technology of the device before introduction.
	Non-DOE/NNSA Managed	(1) (2) (3)	⊘	⊘	⊘	(1) Computers owned by subcontractors and other companies doing business with DOE/NNSA are allowed if approved by the respective host Security organization unless otherwise prohibited under any other controls within this policy. (2) Use of the “Internet Only” is allowed when approved by the host Cyber Security organization. (3) May not be connected to government equipment or resources.

Article	Owner	PPA	LA	VAULT VTR	PA MAA	Restrictions
Peripheral Devices with Built-in Wireless (Hardware devices with embedded 802.11x, Infrared, or other wireless technologies, e.g., printers, scanners, RFID, NFC) (See Cellular/Smart Phone RESTRICTIONS)	DOE/NNSA Managed	(1) (2) (3) (4)	(1) (2) (3) (4) (5) (6) (7) (8)	(1) (2) (3) (4) (5) (6) (7) (8)	(1) (2) (3) (4) (5) (6) (7) (8)	(1) Must be approved by the ODFSA or designee. (2) Must be in compliance with the Spectrum Management Policy. (3) Equipment using wireless technology as a transmitter must be documented with TEMPEST/TSCM. (4) Bluetooth keyboards are prohibited. (5) Devices may not be operated within 10 feet of classified computer systems. (6) Devices may not be operated within 10 feet of equipment copying or faxing of classified information. (7) Devices may not be operated within 10 feet of secure communications equipment. (8) This policy does not allow for the introduction into areas where Top Secret, Special Access Program, Sensitive Compartmented information, or Nuclear Command and Control information is stored, processed or discussed or, in TEMPEST protected areas.
	Non-DOE/NNSA Managed	⊘	⊘	⊘	⊘	

Article	Owner	PPA	LA	VAULT VTR	PA MAA	Restrictions
Test, Measurement, and Diagnostic Equipment with Built-in Wireless (Embedded 802.11x, Infrared, or other wireless technologies)	DOE/NNSA Managed	(1) (2)	(1) (2) (3) (4) (5) (6)	(1) (2) (3) (4) (5) (6)	(1) (2) (3) (4) (5) (6)	(1) Tools authorized for test, measurement, diagnostics operated in support of an official function. (2) Equipment using wireless technology as a transmitter must be documented with TEMPEST/TSCM. (3) Devices may not be operated within 10 feet of classified computer systems. (4) Devices may not be operated within 10 feet of equipment copying or faxing of classified information. (5) Devices may not be operated within 10 feet of secure communications equipment. (6) This policy does not allow for the introduction into areas where Top Secret, Special Access Program, Sensitive Compartmented information, or Nuclear Command and Control information is stored, processed or discussed or, in TEMPEST protected areas.
	Non-DOE/NNSA Managed	⊘	⊘	⊘	⊘	

Article	Owner	PPA	LA	VAULT VTR	PA MAA	Restrictions
Non-Cellular Wireless Portable Electronic Devices (See Camera/Recording Device and Cellular Phone Restrictions)	DOE/NNSA Managed	✓	(1) (2) (3) (4) (5) (6)	(1) (2) (3) (4) (5) (6)	(1) (2) (3) (4) (5) (6)	(1) Must be approved by ODFSA or designee. (2) Equipment using wireless technology as a transmitter must be documented with TEMPEST/TSCM. (3) Devices may not be operated within 10 feet of classified computer systems. (4) Devices may not be operated within 10 feet of equipment copying or faxing of classified information. (5) Devices may not be operated within 10 feet of secure communications equipment. (6) This policy does not allow for the introduction into areas where Top Secret, Special Access Program, Sensitive Compartmented information, or Nuclear Command and Control information is stored, processed, or discussed in TEMPEST protected areas.
	Non-DOE/NNSA Managed	(1)	⊘	⊘	⊘	(1) May not be connected to government equipment or resources.

Article	Owner	PPA	LA	VAULT VTR	PA MAA	Restrictions
Data Storage Devices (e.g., USB thumb drives, external USB or Firewire hard drives, CD, DVD, other types of electronic storage device) (See Camera/Recording Device, Cellular/Smart Phone Restrictions)	DOE/NNSA Managed	(1)	(1)	(1)	(1)	(1) Only specified portable data storage devices are permitted to be used. Portable data storage devices, e.g., USB-type must use full disk encryption if containing CUI or when removed from site.
	Non-DOE/NNSA Managed	(1)	(1) (2) (3)	(1) (2) (3)	(1) (2) (3)	(1) May not be connected to or introduced into government equipment or resources. (2) External storage devices owned by subcontractors and other companies doing business with DOE/NNSA may be allowed if approved by the host organization Cyber Security; May require inspection by TSCM. (3) Personally-owned external storage devices are prohibited.

Article	Owner	PPA	LA	VAULT VTR	PA MAA	Restrictions
Wireless Access Points	DOE/ NNSA Managed	(1)	(1) (2) (3) (4) (5)	⊘	⊘	(1) Authorized when documented within an approved security plan, ISSP, or Project Security Plan approved by the ODFSA or designee. (2) Devices may not be operated within 10 feet of classified computer systems. (3) Devices may not be operated within 10 feet of equipment copying or faxing of classified information. (4) Devices may not be operated within 10 feet of secure communications equipment. (5) This policy does not allow for the introduction into areas where Top Secret, Special Access Program, Sensitive Compartmented information, or Nuclear Command and Control information is stored, processed.
	Non-DOE/ NNSA Managed	⊘	⊘	⊘	⊘	

Article	Owner	PPA	LA	VAULT VTR	PA MAA	Restrictions
Unclassified Video Conferencing	DOE/ NNSA Managed	(1)	(1) (2) (3)	(1) (2) (3)	(1) (2) (3)	(1) Authorized when following applicable procedures, (i.e. DC review). (2) Areas must be sanitized prior to use, to prevent inadvertent compromise of information. (3) Personal devices with a built-in webcam may be used within pre-approved areas (e.g., NNSS dorms) for video conferencing as outlined in the facility security plan.
	Non-DOE/ NNSA Managed	(1)	⊘	⊘	⊘	

Article	Owner	PPA	LA	VAULT VTR	PA MAA	Restrictions
Two-Way Radios	DOE/ NNSA Managed	(1) (2)	(1) (2) (3) (4)	(1) (2) (3) (4)	(1) (2) (3) (4)	(1) Contractor Protective Force radios are authorized in all areas unless a safety reason exists. (2) Fire and rescue radios are authorized in all areas during emergency response and emergency response exercises unless a safety reason exists. (3) Two-Way Radios NNSA Managed or Government-owned radios are authorized under emergency and operational situations when coordinated through M&O Security Operations. (4) Permanent installations of radios must be documented with the TEMPEST Program Office.
	Non-DOE/ NNSA Managed	(1)	⊘	⊘	⊘	(1) Personally owned two-way radios are allowed in the PPA but must be turned off and may not be operated.

Article	Owner	PPA	LA	VAULT VTR	PA MAA	Restrictions
Wireless Medical Devices	DOE/ NNSA Managed	✓	NA	NA	NA	NA
	Non-DOE/ NNSA Managed	(1)	(1) (2) (3) (4) (5)	(1) (2) (3) (4) (5)	(1) (2) (3) (4) (5) (6)	(1) May not be connected to government equipment or resources. (2) Report device to M&O Security Operations before security area introduction. (3) Devices may not be operated within 10 feet of classified computer systems, equipment copying or faxing of classified information, secure communications equipment. (4) Wireless accessory equipment or controllers are not authorized. (5) This policy does not allow for the introduction into areas where Top Secret, Special Access Program, Sensitive Compartmented information, or Nuclear Command and Control information is stored, processed or discussed or, in TEMPEST protected areas. (6) Device must be submitted for review through the facility's electronic equipment process, if applicable.

Request to Introduce Non-Policy Approved Controlled Articles

Novel instances (i.e., not contained in the tables above) of unassessed controlled articles are subject to Cyber Security, Technical Security, and Vulnerability Analysis and Risk Planning review and evaluation prior to introduction into NvE Security Areas. The resulting review will be submitted for ODFSA review for concurrence/approval or denial.

In order to facilitate the review and evaluation, the following information is required to be submitted:

-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

Once this information is submitted to Cyber Security and/or Technical Security, a review of an existing specification sheet(s), instruction manual, and/or discussion to the manufacturer will occur.

Cyber Security and/or Technical Security will look at the area where the equipment is intended for use, (e.g., is there classified processing in the immediate vicinity) to determine if the article can be introduced without introducing a technical security hazard.

Consideration for necessity, such as if it needs to be this device, will occur.

Based on all the information determined during the review, the equipment may require an examination to see how it performs and if it performs as described.

Following review/evaluation the Technical Security Team will provides the results to the TSCM Operations Manager (TSCMOM) who will advise the NFO ODFSA:

-In favor of introduction

-In disfavor of introduction

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

Vulnerability Analysis and Risk Planning:

-Based on Cyber Security/Technical Security input, will analyze impacts and determine impact to risk.

-Will ensure a USC will be generated defining impacts to risk.

-Will ensure USC is submitted to the ODFSA for notification, concurrence, or approval.

NOTE: Medical device, (e.g., hearing aids) documentation will be submitted to the M&O SES Director.