HANFORD MISSION INTEGRATION SOLUTIONS

Administrative Procedures

HMIS-PRO-SEC-417

Controlling Prohibited and Controlled Articles

Revision 0, Change 2

Published: 05/10/2022
Effective: 05/10/2022

Program: Safeguards and Security
Topic: Security

Subject Matter Expert: Mercer, John M
Functional Manager: Ames, Mark A

Use Type: Administrative

- No USQ Required

JHA: Administrative
Periodic Review Due Date:02/04/2025
Rev. 0, Chg. 2

Change Summary

Description of Change

Modify NOTE under step 4.2.5 and correct spelling (‘remote’ from ‘remoted’) in Appendix A, A.1.1, 8th bullet.

Table of Contents

1.0 PURPOSE

This procedure lists prohibited and controlled articles. It provides the requirements for requesting a pass to bring prohibited and/or controlled articles on to the Hanford Site using a *Prohibited/Controlled Article Pass*, and to account for and control the use of prohibited/controlled articles.

2.0 SCOPE

This Level 1 Administrative Procedure applies to Hanford Site employees and Hanford Site visitors who manage, account for, possess, transport, or use prohibited/controlled articles on the Hanford Site proper, or in U.S. Department of Energy (DOE) owned or leased facilities or in Site contractor owned or leased facilities located off the Site proper.

Hanford Site employees include all DOE employees, employees of DOE prime contractors and their subcontractors who perform work for or are otherwise associated with the Hanford Site. Hanford Site visitors are individuals who have business with or the need to access Hanford on or off-site properties for any reason.

Items identified as "prohibited articles" are prohibited anywhere on Site or in Site associated facilities unless authorized by a valid *Prohibited/Controlled Article Pass*. This policy does not apply to parking areas or pedestrian walkways at DOE owned or leased facilities and contractor owned or leased facilities located off the Site proper.

In the event a weapon is observed or reported in such a location Patrol shall make a safety contact with the individual in possession of the weapon or vehicle owner and determine why the weapon is present.

Items identified as "controlled articles" are prohibited in limited areas, protected areas and material access areas unless authorized by a valid *Prohibited/Controlled Article Pass*; these items are authorized in property protection areas.

NOTE: *Some of the facilities located off the Hanford Site and leased by DOE or Site Contractors have public access areas that may be used by the building owner or their designees for private, non-Hanford related activities. The prohibited and controlled articles policies do not apply to private activities located in the public access areas.*

3.0 RESPONSIBILITIES

This section identifies overall responsibilities within the prohibited/controlled articles program. Responsibilities related to individual process steps are shown in Section 4.0, Instructions.

3.1 Pass Requester/Holder

- Provide information to complete a *Prohibited/Controlled Article Pass Request* to Physical Security.

- Have *Prohibited/Controlled Article Pass* in possession when required.
- Protect the *Prohibited/Controlled Article Pass* from loss or theft. Complete required notifications if either occurs.
- Present *Prohibited/Controlled Article Pass* to Hanford Patrol whenever requested to do so.
- Return the *Prohibited/Controlled Article Pass* to Physical Security (Pass Processing/MSIN G3-49) when :
    - Employment is terminated
    - Job change eliminates need for the pass,
    - Pass requires modification
    - Pass expires or is no longer needed,
    - Return is requested by Security.

3.2 Pass Requester's Manager

- Provide written validation to Physical Security that possession of the *Prohibited/Controlled Article Pass* is "mission essential." Specify the security area(s) where the requester is authorized to transport or possess the prohibited/controlled article(s).
- Review and approve (or decline) completed *Prohibited/Controlled Article Pass Requests.*
- Designate an administrator to control "bearer" passes and the equipment designated on the passes.
- Ensure unused/unissued designated items and "bearer" passes are secured.
- Ensure SAS label numbers affixed to controlled articles remain legible and request new labels and/or passes as necessary.

3.3 Physical Security

- Complete the *Prohibited/Controlled Article Pass Request*, with the exception of signatures.
- Submit completed *Prohibited/Controlled Article Pass Request* forms via "Adobe Experience Manager" to the requesting manager for signature.
- Review and approve (or decline) completed *Prohibited/Controlled Article Pass Requests*.
- Notify requesting manager when *Prohibited/Controlled Article Pass* is approved and coordinate delivery of the pass and labeling of controlled articles as required.

4.0 INSTRUCTIONS

4.1 Discovery of Undeclared Firearms

4.1.1 General Actions

NOTE: *Concealed handguns that are covered by a valid "Washington State Concealed Pistol License" are treated as a prohibited article only. The Benton County Sheriff's Office (BCSO) shall be contacted if the individual is not in possession of a valid "Washington State Concealed Pistol License."*

In the event an individual who is on Site or attempting Site access is found in possession of a firearm (handgun or long gun), whether or not the individual possesses a valid *Washington State Concealed Pistol License*, his/her firearm and security badge shall be confiscated. If an individual already on site is discovered with a firearm, that individual's firearm and security badge shall be confiscated. The individual shall be escorted off Site by a Security Police Officer and the responsible manager/supervisor (or designee) or host, and the Contractor Security Duty Officer shall be notified by the Patrol Operations Center (POC).

4.1.2 Actions toward Site Employee

If an employee attempting site entry is found in possession of a firearm, the individual's manager/supervisor (or designee) shall be contacted by the POC to determine if the employee should be permitted access to the Site.

The manager/supervisor (or designee) should be aware of the warning signs of workplace violence and if the manager/supervisor (or designee) suspects the employee's behavior to be threatening, BCSO will be notified and the individual detained.

- If access is permitted, Patrol shall retain the firearm and release the security badge back to the employee.
- If access is not permitted, Patrol shall retain the firearm and the security badge. The security badge will be returned to the Central Badging Office for disposition.
- If the employee's manager/supervisor (or designee) cannot be contacted, access shall be denied and the POC shall retain the security badge. The employee shall be instructed to notify their manager/supervisor (or designee) at the earliest opportunity and advise them to contact the POC. The manager/supervisor (or designee) must contact the POC to determine if the employee should be permitted access to the Site.

4.1.3 Actions toward Site Visitor

If a visitor attempting Site entry is found in possession of a firearm, the manager/supervisor of the visitor's host shall be contacted by the POC to determine if the visitor shall be permitted access to the Site.

- If access is permitted, Patrol shall retain the firearm and release the security badge back to the visitor.
- If access is not permitted, Patrol shall retain the firearm and the security badge. The security badge will be returned to the Central Badging Office for disposition.
- If the host's manager/supervisor (or designee) cannot be contacted, access shall be denied and the POC shall retain the security badge. The host shall be instructed to notify his/her manager/supervisor (or designee) at the earliest opportunity and advise them to contact the POC.

4.1.4 Actions toward Delivery Driver

If a delivery driver attempting Site entry is found in possession of a firearm, the Contractor Security Duty Officer shall be contacted by the POC to determine if the driver shall be permitted access to the Site.

- If access is permitted, the driver must be escorted by a Site employee. Patrol shall retain the firearm and release the security badge back to the driver.
- If access is not permitted, Patrol shall retain the firearm and the security badge. The security badge will be returned to the Central Badging Office for disposition.
- If the Contractor Security Duty Officer cannot be contacted, access shall be denied and the POC shall retain the security badge.

4.2 Requesting a Prohibited/Controlled Article Pass

NOTE 1: *Prohibited/controlled articles may occasionally be authorized on Site; however, their use must be mission essential as determined by responsible management.*

NOTE 2: *Passes are **not** issued for privately owned controlled articles.*

Actionee	Step #	Source
Requester	1.	PROVIDE information required to complete a *Prohibited/Controlled Article Pass Request* (A-6002-705) to Physical Security (e-mail to ^Physical Security) in accordance with Appendix B.
Requester's Manager	2.	PROVIDE written validation to Physical Security (e-mail to ^Physical Security) that possession of the prohibited/controlled article by the requester is "*mission essential*."
	3.	SPECIFY the security area(s) where the requester is authorized to transport or possess the prohibited/controlled article(s).
	4.	IF access will be required to PNNL facilities, THEN INDICATE facilities to which access will be required
	5.	DESIGNATE an administrator to control "bearer" passes and the equipment designated on the passes. NOTE: **:** *Passes are to be reviewed annually and renewal requests for expired passes should be made approximately 30 days before expiration date.*

Actionee	Step #	Source
	6.	ESTABLISH a suspense file to ensure "bearer" passes remain current.
	7.	CONDUCT an inventory of the designated equipment annually during the pass renewal period.
	8.	ENSURE unused/unissued designated items and "bearer" passes are secured.
	9.	ENSURE each SAS registration number remains legible and REQUEST new numbers and/or passes as necessary. NOTE: *Passes for prohibited and controlled articles issued to an individual include a color photograph of the bearer. The likeness of the bearer shown on the pass must match the likeness shown on their security badge for the pass to be valid. Passes issued to "Bearer" for items used by multiple personnel do not include a photograph.*
Physical Security	10.	COMPLETE the *Prohibited/Controlled Article Pass Request*, with the exception of signatures.
	11.	SUBMIT the completed form via *Adobe Experience Manager* to the requesting manager for signature.
Requesting Manager	12.	RECEIVE e-mail message "^Forms Task Assignment – Process PCAPassRequest."
	13.	OPEN the e-mail, log on with your HLAN password. NOTE: *Managers may **not** approve pass requests for their own personal use.*
	14.	REVIEW the *Prohibited/Controlled Article Pass* and SELECT "Approve" or "Decline." NOTE 1: *Once the Prohibited/Controlled Article Pass Request is "Approved" by the manager, it will go via e-mail to the Contractor Security Approval for approval, or decline.* NOTE 2: *Should a Prohibited/Controlled Article Pass be "declined" the pass will return electronically to ^Physical Security.*
Physical Security	15.	NOTIFY the manager when *Prohibited/Controlled Article Pass* is approved.

Actionee	Step #	Source
		NOTE: *Controlled articles are labeled with a numbered, tamper-indicating Safeguards and Security label. The number displayed on the controlled article is reflected on the bearer's Prohibited/Controlled Article Pass. In unique situations where an individual's job responsibilities require they transport controlled articles not assigned to themselves (e.g., property specialist), a Prohibited/Controlled Article Pass may be issued that does not indicate specific SAS label numbers. A caveat is included on such passes clarifying why SAS label numbers are not provided.*
	16.	COORDINATE delivery of pass to the manager and labeling of controlled article(s) as required.
Requester's Manager	17.	BRIEF employee on limitations associated with use of the pass prior to issuance (e.g., locations and scope of work for which use of the pass is authorized).
	18.	ISSUE approved *Prohibited/Controlled Article Pass* to authorized employee.
	19.	PROVIDE an e-mail notification to ^Physical Security validating that the employee receiving the *Prohibited/Controlled Article Pass* has been briefed on limitations associated with use of the pass.

4.3 Reclaiming a Confiscated Item

NOTE: *Items not claimed within 30 days are donated to charity or destroyed.*

Actionee	Step #	Source
Owner/Bearer	1	CONTACT the Patrol Operations Center, 373-3800, for instructions to pick up legal weapons, ammunition, and incendiary devices.
	2.	CONTACT Physical Security, 376-5103 or 373-3932 for all other items not held as evidence, as illegal, or as contraband. NOTE**:** *Hanford Patrol issues a receipt for each confiscated item at the time of confiscation.*
	3.	PRESENT the receipt to reclaim the item.

5.0 RECORD IDENTIFICATION

All records are generated, processed, and maintained in accordance with HMIS-PRO-RM-10588, *Records Management Processes,* or HMIS-PRO-RM-32281, *Electronic Records Management,* as applicable.

Table 1. Records Capture Table

Name of Document	Submittal Responsibility	Retention Responsibility
Prohibited/Controlled Article Pass Request	Pass requester	Physical Security

6.0 SOURCES

6.1 Source Requirements

DOE O 205.1B Chg. 2, *Department of Energy Cyber Security Program*
DOE O 470.4B Chg. 1, *Safeguards and Security Program Planning and Management*
CRD O 470.4B, Chg. 1 (Supplemented Rev. 0), *Safeguards and Security Program Planning and Management*
CRD O 473.3A, Chg. 1 (Supplemented Rev. 0), *Protection Program Operations*

6.2 References

HMIS-PRO-FPROP-133, *Property Management Processes*
HMIS-PRO-RM-184, *Information Clearance*
HMIS-PRO-RM-10588, *Records Management Processes*
HMIS-PRO-RM-32281, *Electronic Records Management*
HMIS-PRO-SEC-416, *Reporting Security Incidents*

6.3 Forms

Prohibited/Controlled Article Pass Request, A-6002-705 (Contact Physical Security)

Appendix A. Requirements Matrix

NOTE: *For the tables in this section under the requirement "type" column, "V" means verbatim and "I" means interpreted.*

A.1 Prohibited/Controlled Articles

#	Requirement	Type V or I	Source
1.	The following items are prohibited articles anywhere on Site, or in DOE owned or leased facilities and contractor owned or leased facilities located off the Site proper: • Dangerous weapons. • Ammunition. • Explosives (to include simulated explosives). • Stun Guns • Incendiary devices. • Controlled substances (e.g., illegal drugs and associated paraphernalia, but not prescription medication), to include marijuana in any form and its derivatives (e.g., edibles, CBD oils). • Alcoholic beverages: Any beverage containing alcohol, including "near" and "non-alcoholic" beers, wines, teas, and energy drinks which identify alcohol as an ingredient. • Alcoholic beverages are not prohibited if used at officially sanctioned events in accordance with contractor policies and procedures in locations designated as Public Access Areas. • Unmanned Aircraft Systems (Drones): Any pilotless aircraft, whether controlled by remote, tethered or pre-programmed, brought onto or flown over the Hanford Site. **NOTE**: *Drones are not authorized for use on the Hanford Site expect with in compliance with DOE-RL approved procedures/protocols authorizing their use.* • Animals: Pets or other animals not recognized as a service animal. **NOTE:** *Further guidance on animals can be found in section A.5 "Service Animals" of this procedure.* • Any items prohibited by law	I	CRD O 473.3A, Chg 1 (Supp Rev. 0), Section D, XI. a. 1.- 7.

	NOTE: *The policy toward knives is clarified as follows:* ***Prohibited*** • *Spring blade knife, or any knife the blade of which is automatically released by a spring mechanism or other mechanical device, or any knife having a blade which opens, or falls, or is ejected into position by force of gravity, or by an outward, downward, or centrifugal thrust or movement.* • *Knives, folding or straight blade, with a blade exceeding four (4) inches in length.* • *Swords, machetes, hatchets, axes, straight razors, and similar cutting devices.* ***Exceptions*** • *A knife in possession of an employee that is recognized as a tool designed for use by the employee in performance of contract work.* • *A knife readily recognized as kitchen cutlery, i.e., carving knife, steak knife, etc. However, such knives found in locations inconsistent with their use (e.g., vehicle glove box) with blades exceeding four (4) inches will be confiscated.*		
2.	The following controlled articles are prohibited within limited areas, protected areas, and material access areas (privately owned items are not authorized within limited areas, protected areas and material access areas; government owned items may be authorized if identified on an approved *Prohibited/Controlled Article Pass*): • Radio frequency data transmitting equipment. • Cellular telephones/devices (includes Apple Watches and similar devices). • eReaders (e.g., Nook, Kindle). • Computers and other devices able to record, or transmit data as standalone units. Other devices include, but are not limited to Apple iPads and iPods, MP3 players, smart devices (e.g., Fitbit, iPhone, Apple watch, Blackberry, Android, etc.), personal electronic devices, Bluetooth devices, and Intermec property inventory devices. • Recording equipment (audio, video, and data). • Cameras (still, motion-picture, video).	I	CRD O 473.3A, Chg.1 (Supp Rev. 0), Section D, XI. b. 1. - 5.

	• Electronic equipment with a data exchange port capable of being connected to automated information system equipment. **NOTE 1:** *Government provided desktop computers are not considered controlled articles.* **NOTE 2:** *Devices or media that are unable to record, or transmit data as standalone units are not considered controlled articles. These include, but are not limited to floppy disks, CDs, removable hard drives, and flash drives (e.g., thumb drives, memory sticks, USB flash drives). See exception regarding flash drives in Note 3 below.* **NOTE 3:** *Flash drives (e.g., thumb drives, memory sticks, USB flash drives) are considered controlled articles and prohibited in rooms where classified information is processed. See Section A.6 for exception to this restriction.* **NOTE 4:** *Time-lapse and closed-circuit television cameras used for monitoring plant equipment or operations are not considered controlled articles. However, procurement and installation of such cameras must be approved by HMIS Physical Security in coordination with RL Security, Emergency Services & Information Management Division (SEI).* *GoPro cameras, dash cameras, etc., require notification to HMIS Physical Security prior to use.* *All photographs or videos captured by any camera are subject to the requirements of HMIS-PRO-RM-184, "Information Clearance."* ***NOTE 5:** Bluetooth medical devices (e.g., hearing aids, pacemakers) are not considered controlled articles provided the user is not in possession of an intermediary "streamer," "medallion," or "assistive listening device," which are prohibited in limited areas, protected areas and material access areas.*		
3.	In addition to the items listed above, all personal protective sprays (e.g., mace, pepper spray, etc.) are prohibited within limited areas, protected areas and material access areas.	I	CRD O 473.3A, Chg 1 (Supp Rev. 0), Section D, XI. d.
4.	The following items are prohibited in rooms wherein classified computer systems are located or classified discussions are	I	CRD O 473.3A, Chg 1

	held. These items are <u>prohibited in rooms wherein classified computer systems are located or classified discussions are held</u> even if they are listed on the item owner's valid *Prohibited/Controlled Article Pass*: • Radio frequency transmitting equipment. • Cordless and cellular telephones/devices (includes Apple Watches and similar devices). • eReaders (e.g., Nook, Kindle). • Computers and other devices able to record, or transmit data as standalone units. Other devices include, but are not limited to Apple iPads and iPods, MP3 players, smart devices (e.g., Fitbit, iPhone, Apple watch, Blackberry, Android, etc.), personal electronic devices and Intermec property inventory devices. • Recording equipment (audio, video, and data). • Cameras (still, motion-picture, video). • Electronic equipment with a data exchange port capable of being connected to automated information system equipment. • Flash drives (e.g., thumb drives, memory sticks, USB flash drives) (only in rooms where classified information is processed). *See section A.6 for exception to this restriction.* **NOTE 1**: *Government Owned video conference systems approved for classified use are not considered controlled articles.* **NOTE 2:** *Electronic equipment identified in a System Security Plan for a National Security System is authorized in rooms where classified information is processed.* **NOTE 3:** *Bluetooth medical devices (e.g., hearing aids, pacemakers) are not considered controlled articles provided the user is not in possession of an intermediary "streamer," "medallion," or "assistive listening device," which are prohibited in rooms wherein classified computer systems are located or classified discussions are held.* **NOTE 4**: *Hanford Patrol is authorized to search all vehicles and hand-carried items, and to confiscate any prohibited/controlled articles not listed on a valid Prohibited/Controlled Article Pass.*		(Supp Rev. 0), Section D, XI. b. 2.

A.2 Prohibited/Controlled Article Violations

#	Requirement	Type V or I	Source
1.	Incidents involving the attempted or actual introduction of controlled or prohibited articles into limited areas, protected areas or material access areas shall be reported as an incident of security concern in accordance with HMIS-PRO-SEC-416, *Reporting Security Incidents*.	I	CRD O 470.4B, Chg. 1 (Supp Rev. 0), Section A and DOE O 470.4B Chg. 1, Attachment 5,
2.	Incidents where the unauthorized introduction of cellular phones or portable electronic devices into a limited area is immediately identified upon entry and the item is immediately removed are not reportable.		
3.	Incidents where the unauthorized introduction of cellular phones or portable electronic devices into a limited area is **not** immediately identified upon entry shall be reported as an incident of security concern in accordance with HMIS-PRO-SEC-416, *Reporting Security Incidents*. The Area Security Representative shall be notified and the item shall be turned over to Information Security for a review of its contents (i.e., text, photographs, recordings). **NOTE**: *A list of Area Security Representatives is available on the HMIS Safeguards and Security (SAS) Intranet Site, SAS Points of Contact.*		
4.	Incidents where the unauthorized introduction of cellular phones or personal electronic devices into classified conference rooms is identified and the item is removed prior to or immediately after the review of classified conference room user requirements are not reportable.		
5.	Incidents where the unauthorized introduction of cellular phones or personal electronic devices into classified conference rooms is identified after the meeting has begun shall be reported as an incident of security concern in accordance with HMIS-PRO-SEC-416, *Reporting Security Incidents*. The Area Security Representative shall be notified and the item shall be turned over to Information Security for a review of its contents (i.e., text, photographs, recordings).		
6.	Incidents where the unauthorized introduction of cellular phones or personal electronic devices into classified work		

	locations (i.e., classified information systems [IS] are present) is immediately identified and the item removed and no classified IS are operating are not reportable.		
7.	Incidents where the unauthorized introduction of cellular phones or personal electronic devices into classified work locations is identified and classified IS are in operation shall be reported in accordance with HMIS-PRO-SEC-416, *Reporting Security Incidents*. The Area Security Representative shall be notified and the item shall be turned over to Information Security for a review of its contents (i.e., text, photographs, recordings).		

A.3 Secure Telephone Equipment (STE) Operation in Property Protection Areas

#	Requirement	Type V or I	Source
1.	The following requirements shall be implemented for utilization of STE located in a property protection area (PPA): • Contact recipient prior to use of STE. • Ensure no uncleared personnel are present within the immediate areas and that only cleared personnel with a need to know are present. • Ensure that any doors and windows (if applicable) are closed prior to initiating use of STE.	I	DOE O 205.1B Chg. 2, Attachment 1

A.4 Bearer's Requirements

#	Requirement	Type V or I	Source
1.	Each person who possesses, transports, or uses prohibited/controlled articles must have a valid *Prohibited/Controlled Article Pass* in his/her possession that lists each item and the security area(s) into which each item is authorized. Each function of a listed item must be identified, i.e., a PDA with a cellular telephone function must list both PDA and cellular telephone.	I	CRD O 473.3A, Chg 1 (Supp Rev. 0), Section D, XI. a. and b.

Controlled articles are labeled with a numbered, tamper-indicating Safeguards and Security label. The number displayed on the controlled article is reflected on the bearer's *Prohibited/Controlled Article Pass*. SAS labels shall only be applied to controlled articles with a DOE property label affixed which identifies the item as government property (for information regarding DOE property labels see HMIS-PRO-FPROP-133, *Property Management Process*).

NOTE: *In unique situations where an individual's job responsibilities require they transport controlled articles not assigned to themselves (e.g., property specialist), a Prohibited/Controlled Article Pass may be issued which does not indicate specific SAS label numbers. A caveat is included on such passes clarifying why SAS label numbers are not provided.*

Additionally, SAS labels are not affixed to government owned controlled articles in possession of non-Hanford personnel that are required to perform work at Hanford. A caveat is included on such passes clarifying why SAS label numbers are not provided.

In the event a SAS label is damaged or missing, contact Physical Security for a replacement label and *Prohibited/Controlled Article Pass*.

Each pass holder must:

- Use the pass exclusively for himself/herself. The use of the pass by any other person is not allowed under any circumstances.
- Protect the pass from loss or theft. Promptly notify the responsible manager, and the Area Security Representative or Physical Security at 373-3932 if either occurs.
- Present the pass to Hanford Patrol at established checkpoints whenever moving a prohibited/controlled article or having a prohibited/controlled article in his/her possession.
- Present the pass to Hanford Patrol whenever requested to do so.
- Return the pass to Pass Processing, MSIN G3-49, when:
  - Employment is terminated.

	▪ Job responsibility changes eliminate the need for the pass. ▪ The pass requires modification; e.g., the articles listed on the pass need to be changed or the bearer's name must be changed (marriage). ▪ It is requested by Security. ▪ It has expired or is otherwise no longer needed. **NOTE:** *In special circumstances, where an individual item is used by multiple personnel, a Prohibited/Controlled Article Pass may be issued to "Bearer." Such passes accompany the prohibited/controlled article regardless of the user. Administration and control of these passes is the responsibility of the individual to which the property is assigned.*		

A.5 Service Animal Access

#	Requirement	Type V or I	Source
1.	Department of Justice (DOJ) regulations implementing the Americans with Disabilities Act (ADA) define a service animal as a **dog** that is individually trained to do work or perform tasks for a person with a disability. Examples of such work or tasks include guiding people who are blind, alerting people who are deaf, pulling a wheelchair, alerting and protecting a person who is having a seizure, reminding a person with mental illness to take prescribed medications, calming a person with Post Traumatic Stress Disorder (PTSD) during an anxiety attack, or performing other duties. Service animals are working animals, not pets. The work or task a dog has been trained to provide must be directly related to the person's disability. Dogs are recognized as service animals under titles II and III of the ADA. The general policy set forth by the General Service Administrations (GSA) is that only service animals used to assist people with disabilities may be brought into federal facilities.	I	Americans with Disabilities Act and HMIS Legal Counsel
2.	To determine if a dog is a service animal, <u>only two questions may be asked</u>: • Is this animal required because of a disability?		

	• What work or task has this animal been trained to perform? The work or task a dog has been trained to provide must be directly related to the person's disability.		
3.	The ADA requires that an employer make reasonable accommodation to allow the individual with disabilities to work. In examining whether or not to permit a service dog to accompany an employee onto the Site, consideration must be given as to whether or not a reasonable accommodation can be made. In many Site areas, this would not be possible. For example, if an individual had a hearing disability and used a service dog to alert to sounds and if the dog was not able to distinguish between the various Site alarms, it would not be a reasonable accommodation that would allow the individual to work in an area where alarms were used.		
4.	Based on DOJ and GSA guidance, service animals may be permitted access to the Hanford Site and Site associated facilities on a case-by-case basis, provided that: • The owner is able to supervise and care for the animal. **NOTE:** *The care of a service animal is solely the responsibility of its owner.* • The animal's behavior does not pose a threat to the health or safety of the owner, other workers in the area, or the animal itself. A service animal will be removed from the Hanford Site or Site associated facilities if: • The animal is out of control and the animal's owner does not take effective action to control it, or • The animal poses a direct threat to the health and safety of others. In the event a service animal is removed from the Hanford Site or a Site associated facility, the owner of the service animal will:		

	• Notify the Area Security Representative and Human Resources Department of the service animal's removal, and • Return the *Prohibited/Controlled Article Pass* authorizing the service animal to HMIS Physical Security (Pass Processing/MSIN G3-49).		
5.	Under the ADA, service animals must be harnessed, leashed, or tethered, unless these devices interfere with the service animal's work or the individual's disability prevents using these devices. In that case, the individual must maintain control of the animal through voice, signal, or other effective controls.		
6.	Service animals should be permitted into all areas where it would be safe to take the animal, including, but not limited to general office space. **NOTE:** *Service animals "in training" are not considered service animals under this procedure and will not be allowed on the Hanford Site or in Site associated facilities.*		
7.	Service animals <u>are not</u> permitted access to areas where it would be unsafe to allow the service animal, such as radiation areas, surface contamination areas, or areas of construction or decontamination and decommissioning (D&D) work.		
8.	Other animals, to include pets and "comfort animals" **<u>are not</u>** permitted access onto the Hanford Site or in Site associated facilities. Dogs whose sole function is to provide comfort or emotional support <u>do not</u> qualify as service animals under the ADA.		
9.	Service animals may, but <u>are not</u> required to wear an identifying vest.		
10.	HMIS Physical Security will issue a *Prohibited/Controlled Article Pass* to Site employees in possession of service animals validating their authorization to possess the animal on the Hanford Site or in Site associated facilities. This pass must accompany the service animal anytime the animal is present on the Hanford Site or in Site associated facilities. Service animals in the possession of vendors or visitors will		

	be authorized by HMIS Physical Security on a case-by-case basis.		

A.6 Exceptions

- Hanford Patrol and local, state, and federal law enforcement personnel are authorized to transport or bear prohibited/controlled articles necessary to perform official duties.

- Fire Department personnel (including non-Hanford fire personnel who respond to a mutual aid call) are authorized to transport or bear prohibited/controlled articles necessary to perform official duties, including certain controlled substances necessary for the rendering of first aid.

- Long-distance commercial truck drivers making deliveries to the Site who declare legal firearms in their possession to Hanford Patrol at a Site barricade or to employees at 2377 Stevens Drive are not required to obtain a *Prohibited/Controlled Article Pass*.

  NOTE: *Hanford Patrol retains the firearms/items and returns them upon the driver's exit from the Site. Other legal but Site-prohibited items can be declared and held at 2377 Stevens Drive and at Site barricades.*

- Propellant Actuated or Powder Actuated Devices, commonly referred to as nail guns and their actuators (commonly .22 cal. blank shells) are considered tools and do not require a *Prohibited/Controlled Article Pass*.

- Information System Security Officers are authorized to possess and use flash drives (e.g., thumb drives, memory sticks, USB flash drives) in rooms where classified information is processed for testing of classified information systems; however, a second appropriately cleared and knowledgeable individual must be present when such testing is being performed.

Appendix B. Prohibited/Controlled Article Pass Request Instructions

Block	Requested Information
Name of Bearer	Name of the person to whom the pass is to be issued. **NOTE:** *If pass request is for items used by multiple personnel, e.g., pool cellular telephones, pool cameras, etc., provide name of individual submitting the request. Indicate in the request a "Bearer Pass" is required.*
HID	Bearer's Hanford Identification number. **NOTE:** *If pass request is for items used by multiple personnel, e.g., pool cellular telephones, pool cameras, etc., no HID is needed.*
Contractor	Name of the contractor.
Expiration Date	Passes are issued for a specific time period – typically not more than one year. If the pass is for a subcontractor or vendor, the requester should indicate an appropriate date of expiration, not to exceed the contract completion date, and should not exceed the expiration on the bearer's badge.
Manager Name	Typed name of requesting manager.
Property Items	List of specific prohibited/controlled articles the bearer is authorized to possess or move. **NOTE:** *Passes are **not** issued for privately owned controlled articles.*
Frequency of Use	Expected frequency of need to have the prohibited/controlled article(s) onsite or to pass through Patrol checkpoints (e.g., daily, weekly, etc.).
Security Area(s) and Limitations	List of security areas to which the pass authorizes the bearer to possess prohibited/controlled articles. Limitations associated with use of the pass are also identified in this section. For example a pass may indicate "Hanford Site," yet exclude specific facilities, e.g., PNNL facilities.
Work Related Justification	Brief description of the following: 1. The bearer's need to possess or move prohibited/controlled article(s). Be specific – generalities such as "job requires it" or "program support" will not be accepted. 2. Bearer's job title and work location.