

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 1 of 35
------------------------------------	--

INTEC	Management Control Procedure	For Additional Info: <a href="http://EDMS">http://EDMS</a>	Effective Date: 06/23/14
-------	------------------------------	---	--------------------------

Manual: INTEC FSV4

**USE TYPE 3**

Change Number: 342341

\*The current revision can be verified on EDMS.

## CONTENTS

1.	PURPOSE .....	2
2.	SCOPE AND APPLICABILITY .....	2
3.	PREREQUISITES .....	2
4.	INSTRUCTIONS.....	2
4.1	Escorted Access (see def.) .....	2
4.2	Access Program .....	3
4.3	Review of Security Force Member Acceptability .....	8
4.4	Security Training Program Responsibilities .....	9
4.5	Deficient Performance of Security Personnel.....	11
4.6	Terminating Unescorted Access .....	11
4.7	MVDS Vehicle Access Authorization .....	12
4.8	Safeguard Event Reports.....	12
4.9	Key Control.....	14
4.10	Security Audits.....	16
5.	RECORDS .....	17
6.	DEFINITIONS.....	18
7.	REFERENCES .....	20
8.	APPENDICES .....	21
	Appendix A, Reporting of Safeguards Events.....	22
	Appendix B, Safeguards Event Matrix .....	24
	Appendix C, Background Investigation File .....	27
	Appendix D, Security Responsibilities and Administrative Operations.....	30
	Appendix E, Security Training Program .....	35

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 2 of 35
------------------------------------	--

## 1. PURPOSE

To provide physical security administrative instruction for the Ft St. Vrain (FSV) Independent Spent Fuel Storage Installation (ISFSI) to ensure a secure facility.

## 2. SCOPE AND APPLICABILITY

This procedure applies to all personnel who are required to perform duties as specified herein.

Unless specified otherwise, the Facility Safety Officer (FSO) is responsible to ensure performance of each procedure step. The FSO is designated by name on the appropriate department Organization Chart. Approved alternates are designated in the Security Implementation Plan.

## 3. PREREQUISITES

Nuclear Regulatory Commission (NRC or Commission) approved Physical Protection Plan.

## 4. INSTRUCTIONS

**NOTE 1:** *In the event of a declared emergency condition or a drill in which the Commission is participating, all access controls for emergency personnel, vehicles, material and equipment entering the Protected Area (PA) may be suspended.*

**NOTE 2:** *Personnel who have been denied unescorted access to the PA (or access has been revoked) as a result of a valid failure to meet screening requirements will not be granted access to the PA. This requirement specifically applies to cases of "for cause" termination/denial/revocation (such as, unfavorable conditions).*

### 4.1 Escorted Access (see def.)

**NOTE:** *An individual with unescorted access may escort not more than 10 visitors at a time.*

4.1.1 Complete Form FSV-039, Escorted Visitor Access Authorization, for personnel who require escorted access to the PA in non-emergency conditions (see def.).

4.1.1.1 Verify individual has not been denied unescorted access to the PA.

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 3 of 35
------------------------------------	--

4.1.1.2 Indicate areas to which the individual is authorized access (i.e. Protected Area, Charge Face, and/or Vital Area/Alarm Station).

4.1.2 Authorize escorted access for not more than 31 days.

4.1.3 Maintain written access authorizations at the access control point(s).

4.1.4 Security Force: Review daily for expired forms.

4.1.4.1 Forward expired forms to FSO.

**NOTE:** *In the event an individual is terminated for cause, the individual's access authorization is revoked and the individual's entry devices retrieved before or simultaneously with notifying the individual of the termination.*

4.1.5 Terminate escorted access as follows:

4.1.5.1 Record access termination and incorporate appropriate documentation of termination action in individual's file.

## **4.2 Unescorted Access Program**

### **4.2.1 Background Investigation Criteria**

**NOTE 1:** *Contract Security Agency, licensee personnel or other contract personnel may perform all or part of any background investigation conducted on an individual. Fingerprints are submitted to the NRC for the FBI criminal history check. The DOE-ID reviewing official determines whether an individual may be granted unescorted access to Safeguards Information (SGI) and the Protected Area (PA).*

**NOTE 2:** *Unescorted access to SGI and the PA is limited to individuals with an active DOE "L" or "Q" clearance or individuals who have completed the access authorization process described below. The FSO determines which specific individuals, approved by the DOE-ID reviewing official, are allowed unescorted access to SGI and the PA. Fort St. Vrain has no "temporary" unescorted access program.*

## FSV SECURITY ADMINISTRATION

Identifier: MCP-325

Revision\*: 8

Page: 4 of 35

**NOTE 3:** *Access to personal, confidential information obtained during the background investigation, including information stored in electronic format, is limited to regulatory agency (for example, NRC), licensee (DOE-ID), and their contractors, subcontractors, or vendors who have a “need to know” the information.*

- 4.2.1.1 Verify the individual(s) granting access and/or performing background investigations described above have met the background investigation requirements described in Step 4.2.1.3.
- 4.2.1.2 Obtain written consent of the individual applying for unescorted access authorization to obtain personal information necessary to perform the background investigation.
  - 4.2.1.2.1 Ensure Form FSV-051, “Unescorted Access Background Investigation Checklist for Non-Security Force Personnel,” is completed for non-security force personnel who do not possess a DOE “L” or “Q” clearance.
  - 4.2.1.2.2 Complete Form FSV-012, “Security Force Member Acceptability Review,” per Section 4.3 for security force personnel.
- 4.2.1.3 Verify the individual possesses a DOE “L” or “Q” clearance or the following background investigation elements have been completed:
  - A. Verification of employment with each employer for the most recent year from the date of application
  - B. Verification of employment with an employer of the longest duration during any calendar month for the remaining next most recent two years
  - C. Review of criminal history records obtained from local criminal justice resources for an applicant with all residences of record for the 3 years preceding unescorted access authorization (if available)
  - D. Full credit history review

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 5 of 35
------------------------------------	--

- E. Review of official identification (for example, driver's license, passport, government identification, State, Province or country of birth issued certificate of birth). If used, each page of the passport containing data is photocopied in a clear and legible manner and a photocopy is mailed to the commission
  - F. Interview with not less than two character references, developed by the investigator
  - G. FBI fingerprint criminal history check
  - H. Confirmation of eligibility for employment through the regulations of the Bureau of Citizenship and Immigration Services
  - I. Verification, to the extent possible, of the accuracy of the provided social security number and/or alien registration number (as applicable)
  - J. Confirmation of the character of military service for the past 3 years (if applicable)
  - K. Verification of academic enrollment and attendance in lieu of employment for the past 5 years (if applicable).
- 4.2.1.4 Verify *update background investigations* (see definition) are completed for persons without a DOE "L" or "Q" access authorization who are applying for reinstatement of unescorted access authorization.
- 4.2.1.5 Verify *background reinvestigations* (see definition) are completed for persons without a DOE "L" or "Q" access authorization at intervals not to exceed 5 years.

#### 4.2.2 Unescorted Access Authorization

**NOTE 1:** *With the exception of Commission (see def.) representatives as described below, personnel who are not members of the security force, approved by the DOE-ID reviewing official for unescorted access to SGI and the PA, are authorized unescorted access to SGI and the PA based upon their need for that access as determined by the FSO, or designee.*

**NOTE 2:** *Commission representatives are granted unescorted access authorization upon written request of the Commission. NRC personnel remain subject to applicable training or Radiation Protection (RP) and security access control requirements.*

- 4.2.2.1 Review personal history information (for example, personal history questionnaire, job application, and so forth) and other information obtained in Step 4.2.1.
- 4.2.2.2 Verify the background investigation supports a positive finding of trustworthiness and reliability by one of the following methods:
  - A. The individual possesses an active DOE “L” or “Q” clearance
  - B. Security force member acceptability review (Form FSV-012) has been completed
  - C. Unescorted access background investigation checklist for non-security force personnel (Form FSV-051) has been completed.
- 4.2.2.3 Ensure all non-security force personnel have a legitimate need for access to the PA.
- 4.2.2.4 Establish other, non-security criteria as a basis for granting unescorted access. These criteria may include RP or other training and may be applied as appropriate to each situation or condition of the ISFSI.
- 4.2.2.5 Verify individual has not previously been denied unescorted access to the PA.
- 4.2.2.6 Verify the individual has been approved for unescorted access to SGI and the PA by the DOE-ID reviewing official.

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 7 of 35
------------------------------------	--

**NOTE:** *Form FSV-011, “Unescorted Access Data Sheet,” meets the intent of the file described below.*

4.2.2.7 Develop a file for all personnel (Security, Non Security and Commission Representatives) granted unescorted access, which shall include the following items:

- A. Full name
- B. Social security number (passport or alien registration number if not a U.S. citizen)
- C. Employer's name and address at the time access was granted or denied
- D. Start and end dates of each period of unescorted access
- E. Reason for denying or terminating the individual's access. Refer to Step 4.2.1, “Background Investigation Criteria,” for criteria to deny access.
- F. Reason for which access is requested.

**NOTE:** *Each individual whose employment is or will be adversely affected as a direct result of the denial or revocation of unescorted access will have the opportunity to provide additional information.*

4.2.2.8 IF access is denied, THEN inform the individual, in writing, the basis for denial or revocation.

**NOTE:** *The determination of this review is final. Access will not be granted until after a successful appeal.*

4.2.2.9 Individual Denied Access: Provide additional information for ISFSI Manager review.

4.2.2.10 Complete Form FSV-011, “Unescorted Access Data Sheet,” for access authorization.

- 4.2.2.10.1 Indicate areas to which the individual is authorized access (i.e. Protected Area, Charge Face, and/or Vital Area/Alarm Station).

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 8 of 35
------------------------------------	--

- 4.2.2.11 Evaluate training criteria against current ISFSI procedures for applicability.
  - 4.2.2.12 IF access is denied,  
THEN attach supporting documentation as appropriate.
  - 4.2.2.13 Forward one copy of the Unescorted Access Data Sheet (Form FSV-011) to the Access Control Point(s). This copy may be used as the access authorization document until the access list has been revised, published, and distributed.
  - 4.2.2.14 Establish a Background Investigation File for each individual investigated per Appendix C.
- NOTE:** *Pen and ink changes to the list may be made by the FSO or designee if required.*
- 4.2.2.15 Update and re-approve unescorted access list at least monthly or as needed depending on MVDS activity.
    - 4.2.2.15.1 Include a list of individuals denied unescorted access to the ISFSI on the unescorted access list.
  - 4.2.2.16 Security Force: File Unescorted Access Data Sheets and/or unescorted access lists, as appropriate, in the Post Status Book.

### **4.3 Review of Security Force Member Acceptability**

- 4.3.1 Review each Background Investigation file and document each individual's acceptability before granting a member of the security force unescorted access.
- 4.3.2 Consider information obtained during background investigation and psychological evaluation when determining *security officer* (see def.) acceptability. This information must be reviewed for potentially disqualifying information using the guidelines specified below:
  - A. Willful omission or falsification of material information submitted in support of employment or request for unescorted access authorization
  - B. Illegal use or possession of a controlled substance or abuse of alcohol without adequate evidence of rehabilitation

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 9 of 35
------------------------------------	--

- C. A criminal history without adequate evidence of rehabilitation, which establishes untrustworthiness or unreliability
- D. History of mental illness or emotional instability that may cause a significant defect in the individual's judgment or reliability
- E. Any evidence of coercion, influence, or pressure that may be applied by outside sources to compel an individual to commit any act of sabotage or other act that would adversely reflect upon the individual's trustworthiness or reliability
- F. Evidence that the individual has committed or attempted to commit, or aided or abetted another who committed or attempted to commit, any act of sabotage or other act that would pose a threat or reflect adversely upon that individual's trustworthiness or reliability
- G. A psychological evaluation that indicates an individual is a risk in terms of trustworthiness or reliability
  - Any other information that Psychological exams for mental fitness are conducted initially and every 5 years thereafter.
- H. would adversely reflect upon the reliability and trustworthiness of the individual as it relates to the individual being permitted unescorted access.

4.3.3 Verify the following:

- 4.3.3.1 Evidence the individual is at least 21 years of age.
- 4.3.3.2 Documentation of High School diploma or equivalent.

4.3.4 Complete the Security Force Member Acceptability Review Form, Form FSV-012.

#### **4.4 Security Training Program Responsibilities**

- 4.4.1 Supervise and administer Security Training Program. (See Appendix E, "Security Training Program.")
  - 4.4.1.1 Ensure that all members of security force are trained and qualified to perform security duties as outlined in the Security Training and Qualification Plan (STQP).
  - 4.4.1.2 Ensure that security force trainees complete required training before assuming their duties.

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 10 of 35
------------------------------------	---

- 4.4.1.3 Ensure that prior to assignment to the security force, that trainees are trained to perform tasks and duties as described in the STQP on Form FSV-019, “Security Training Record.”
  - 4.4.1.4 Document and attest to the qualifications and requalifications of each security force member on Form FSV-020, “Security Qualification Record.”
  - 4.4.1.5 Designate in writing, the ISFSI Security Instructor(s).
    - 4.4.1.5.1 Ensure the Security Instructor(s) possess(es) sufficient skills, abilities and knowledge of the ISFSI and ISFSI security operations.
  - 4.4.1.6 Ensure training or orientation is made available to the local law enforcement agency (LLEA) personnel (response force) required to perform their function.
  - 4.4.1.7 Ensure WCC Operators are trained on the requirements of the FSV Physical Protection Plan (PPP), as applicable, for FSV alarm monitoring and LLEA response notifications.
- 4.4.2 Security Force Members: Attend and ensure the following training elements are met:
- A. Examination(s) at initial hire, to ensure mental and physical fitness to perform security duties required in the STQP, by a licensed physician and psychologist
  - B. Demonstration of the required knowledge, skill and ability in accordance with the specified standards for each task as defined in the STQP, applicable procedures, and lesson training plans
  - C. Re-qualification at least once every twelve months, not to exceed thirteen (13) months (395 days total allowable with no further extensions), to perform security tasks identified by the STQP
- NOTE:** *Requirements for Security Officer physical fitness are contained in Security Contractor procedures.*
- D. Re-examination for mental fitness by a licensed psychologist, to meet the examination requirements of the STQP.
- NOTE:** *The Security Contractor provides drug and alcohol screening on-demand as needed.*

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 11 of 35
------------------------------------	---

#### 4.5 Deficient Performance of Security Personnel

**NOTE 1:** *The following step will be taken should a security officer be found deficient in job performance.*

**NOTE 2:** *In the event retraining and requalification are required, the individual may not perform those duties until retraining and re-qualifications have been completed.*

- 4.5.1 Determine if individual shows trending towards specific problems or *demonstrates* (see def.) a significant lack of ability. Conduct or direct retraining and requalification on a specific *task(s)* (see def.) as required.

#### 4.6 Terminating Unescorted Access

- 4.6.1 Receive notification that unescorted access is no longer required or must be withdrawn.

- 4.6.1.1 Establish if the access termination is for cause and take all necessary actions to immediately deny access in accordance with the PPP.

- 4.6.1.1.1 IF unescorted access is terminated “for cause” (unfavorable conditions),  
THEN refer to Step 4.2.2 for additional actions.

- 4.6.1.2 Retrieve Unescorted Access Data Sheet (Form FSV-011) from individual's file.

- 4.6.1.3 Complete the Access Termination fields at bottom of Form FSV-011 and attach supporting documentation, as needed.

- 4.6.1.4 Notify Alarm Station Operator to update the access list or all copies of the Data Sheet in the Post Status Book.

- 4.6.1.5 Process completed Unescorted Access Data Sheet in accordance with Section 5.

- 4.6.2 Security Officer (SO): Update the Access List or Unescorted Access Data Sheet as directed by the FSO.

- 4.6.2.1 SO: If applicable, forward the Unescorted Access Data Sheet to the FSO.

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 12 of 35
------------------------------------	---

#### 4.7 MVDS Vehicle Access Authorization

**NOTE 1:** *This step is only required for vehicles that are capable of legal motor operations on public highways. Forklifts and similar equipment will still be searched, but their presence does not require any specific authorization.*

**NOTE 2:** *Vehicles used primarily for the conveyance of individuals are not permitted within the IC except under emergency conditions. LLEA and emergency vehicles are exempt from vehicle access requirements during emergencies.*

4.7.1 Receive notification that a vehicle will require access to the MVDS.

4.7.1.1 Complete the MVDS Vehicle Access Authorization form (Form FSV-048).

4.7.1.2 Forward original or copy to Access Control Point for use as the access authorization document.

4.7.2 Security Force: File, as appropriate, for use as the access authorization document in Post Status Book.

4.7.2.1 Review daily for expired forms.

4.7.2.2 Forward expired forms to FSO.

#### 4.8 Safeguard Event Reports

4.8.1 Alarm Station Operator (ASO): Upon receiving a report of a potential Safeguard Event, perform the applicable tasks outlined in MCP-324, “FSV Physical Security.”

4.8.2 ASO: Use Appendix A, Reporting of Safeguards Events, and Appendix B, Safeguards Event Matrix, to determine event category.

4.8.2.1 IF event is NOT a 24-hour or 1-hour event category, THEN when time permits, complete a Security Incident Report (SIR) (Form FSV-046 or 046A).

4.8.2.2 IF event is in the 24-hour logable event category, THEN perform the following:

4.8.2.2.1 SO: Complete Form FSV-040, Safeguards Event Log.

4.8.2.2.2 SO: Notify FSO (or EC on back shifts) within 12 hours.

4.8.2.3 Emergency Coordinator/ASO: IF event is in the 1-hour event report category, THEN perform the following:

4.8.2.3.1 Record the following information for the NRC:

- A. Time event began or was discovered
- B. Full description of event
- C. Compensatory measures imposed
- D. Consequences of event (if known).

4.8.2.3.2 Ensure the FSO is informed of the event.

4.8.2.3.3 FSO: Submit written report to Commission within 30 days of 1-hour report and include the following:

- A. Date and time of event
- B. Location of event
- C. Type of security force onsite
- D. Number and type of personnel involved
- E. Method of discovery
- F. Procedural errors involved, if applicable
- G. Immediate actions taken in response to event
- H. Corrective actions taken or planned
- I. Law enforcement agencies contacted
- J. Description of media interest and press release
- K. Indication of previous similar events
- L. Knowledgeable contact.

4.8.2.3.4 For system failures, include the following:

- A. Description of failed equipment
- B. Apparent cause of failure
- C. Status of equipment before event
- D. Secondary functions affected

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 14 of 35
------------------------------------	---

- E. Effect on site safety
- F. Unusual conditions that may have contributed to the failure, such as environmental extremes.

4.8.2.3.5 For threat incidents, include the following:

- A. Number of perpetrators
- B. Type of threat, such as bomb, extortion, etc.
- C. Means of threat communication
- D. Text of threat
- E. Mode of operation
- F. Clear photocopy of letter and envelope.

#### 4.9 Key Control

4.9.1 Determine *security related keys/cores* (see def.) to be controlled by the ASO that are used to control access to the Alarm Station, MVDS facility, and other areas.

**NOTE:** *All active security keys are inventoried or accounted for on a daily basis.*

4.9.2 Direct control and accountability of security keys, locks, cores, combinations, and related access control equipment used to secure protected areas and Safeguards Information. (This will minimize the possibility of compromise, and ensure a prompt change whenever there is evidence that the access control may have been compromised.) Ensure keys, locks, cores, combinations and related access control equipment meets 10 CFR 73.2 and Regulatory Guide 5.65.

4.9.2.1 Conduct a physical inventory of security locks, cores, and keys used in the protection of the ISFSI at least once every 12 months, not to exceed 13 months (395 days total allowable with no further extensions) (see Form FSV-015, “Key/Core Inventory Record”).

4.9.2.2 Maintain inventory of all security locks, cores, keys, and combinations that might be used to compromise the integrity of the security system in a *security storage container* (see def.).

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 15 of 35
------------------------------------	---

4.9.2.3 Ensure security keys, locks, and cores that have not been placed in service are stored in a security storage container.

4.9.2.4 Ensure the following items are issued only to individuals authorized by the FSO:

A. Combinations

B. Keys for locks used to secure gates or doors into protected areas for access to designated security controlled equipment.

4.9.2.5 FSO: Ensure keys, locks, cores and combinations to which an employee was authorized access be changed upon termination of the employee.

**NOTE:** *This requirement applies to DOE-ID, Contractor, and Subcontractor employees.*

4.9.2.5.1 Complete the actual change within 48 hours of unfavorable termination.

4.9.2.5.2 Complete the actual change within 5 days of favorable termination.

4.9.2.5.3 If a control key is compromised, implement compensatory measures for (a) degraded barrier(s) per MCP-324 until all affected security locks can be re-cored.

4.9.2.6 Ensure combinations of security locks or padlocks and access codes are changed under the following conditions:

A. When an area, system, security container or repository to be controlled by the lock is first placed into use

B. When a person knowing the combination no longer requires it as the result of reassignment of duties or termination of employment

C. When the combination or access code may have been compromised.

4.9.2.7 Ensure cores are changed out if a core key or lock is lost or compromised.

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 16 of 35
------------------------------------	---

4.9.2.8 Ensure security lock combinations are stored in a security storage container. This will normally be the container located in the administration building.

4.9.3 FSO or Designee: Ensure security locks, keys, access codes, and combinations used to control access to the protected area, security systems or security storage containers are rotated or changed at least once every 12 months, not to exceed 13 months (395 days total allowable with no further extensions).

4.9.4 ASO: Maintain active security keys in a *locked* (see def.) container in the Alarm Station when not in use, and ensure their return or transfer at the end of each shift.

**NOTE:** *Keys to the MVDS PA and Alarm Station are issued only to a member of the security force or key control personnel.*

4.9.4.1 Ensure security related keys shall only be issued to personnel authorized in writing by the FSO as approved recipients.

4.9.4.2 Maintain a record each time a security related key is issued, returned or transferred listing pertinent information on the Security Key Issue Log (Form FSV-041).

#### **4.10 Security Audits**

4.10.1 FSO: Schedule audits of the Physical Protection Plan implementation at least once every 24 months.

4.10.1.1 Ensure individuals performing audits are independent of the management and implementation responsibilities for the Physical Protection Plan.

4.10.1.2 Ensure an audit (at least once every 24 months) includes an evaluation of the effectiveness of the Physical Protection systems and a review of the LLEA commitments.

4.10.1.3 Ensure an audit (at least once every 24 months) includes an evaluation of the security officer training program effectiveness.

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 17 of 35
------------------------------------	---

- 4.10.1.4 Ensure an audit (at least once every 24 months) includes all program elements of the access authorization program.
  - 4.10.1.4.1 Ensure this portion of the audit is performed by individual(s) knowledgeable and practiced in access authorization program performance objectives.
- 4.10.1.5 Ensure audit reports are maintained as records for three years from the audit date.

**5. RECORDS**

- 5.1 FSO: Ensure personal, confidential information obtained during the background investigation is stored in a fashion (for example, locked cabinets or password protected files) which prevents unauthorized access to and modification of that information.

Record Description
Security Implementation Plans
Physical Protection Plan, Security Training and Qualification Plan, & Safeguards Contingency Plan
Security Administrative Procedures (i.e. Management Control Procedures)
Written Local Law Enforcement Agency Agreements
Unescorted Access Data Sheets (Form FSV-011)
Security Force Member Acceptability Review (Form FSV-012), maintained as part of the Security Force Member Suitability file
Escorted Visitor Access Authorization (Form FSV-039)
MVDS Vehicle Access Authorization (Form FSV-048)
Safeguards Event Log (Form FSV-040)
Security Incident Report (Form FSV-046 or -046A)
Security Key Issue Log (Form FSV-041), maintained with daily security logs described in MCP-324
Key/Core Inventory Record (Form FSV-015)
Background Investigation File (Appendix J), maintained as part of the Security Force Member Suitability file – including information stored in electronic format

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 18 of 35
------------------------------------	---

Record Description
Security Training Records (Form FSV-019), maintained as part of the Security Force Member Suitability file
Security Qualification Records (Form FSV-020), maintained as part of the Security Force Member Suitability file

**NOTE:** *Records management requirements are described in MCP-557, “Managing Records.” See Records Schedule Matrix – NRC Record Center ([NRC Schedule Matrix](#)) for information on Uniform File Code, Disposition Authority, and Retention Period.*

## 6. DEFINITIONS

**NOTE:** *The definitions in this procedure are specific to procedures and communications relating to the security program and security system at the ISFSI. The definitions in this section are not all inclusive and are supplemented by definitions in other security procedures.*

*Access Authorization.* An administrative process for determining that a person, vehicle or material has a legitimate reason for entering the Alarm Station or MVDS.

*Authorized Individual.* Any individual, including an employee, consultant, or an agent of DOE who has been designated in writing to have responsibility for, surveillance of, or control over spent fuel; to have unescorted access to areas where spent fuel is used or stored; or to have met the requirements for possessing Safeguards Information.

*Background reinvestigation.* A periodic review of criminal history and credit history records for potentially disqualifying information.

*Certification.* Verification by the Facility Safety Officer or designee that a member of the security force has successfully completed his/her training.

*Commission.* The United States Nuclear Regulatory Commission or its duly authorized representatives.

*Conditions.* Those events, equipment, or workstation effects that members of the security force experience while performing a given task. The environment surrounding the performance of a task.

*Controlled Area (CA).* That area immediately surrounding the ISFSI for which DOE exercises authority over its use and within which ISFSI operations are performed.

*Demonstrate.* The ability to qualify in a task through the use of written, hands on, verbal, or performance-oriented tests or any combination thereof.

## FSV SECURITY ADMINISTRATION

Identifier: MCP-325

Revision\*: 8

Page: 19 of 35

*Facility.* The equipment, structures, building, and property within the Controlled Area.

*Lock.* In the case of vaults or vault type rooms, “Lock” means a three position, manipulation resistant, dial type, built-in combination lock or combination padlock or any manipulation resistant, electro-mechanical device that provides the same functions as a built-in combination lock or combination padlock, which can be operated remotely or by the “reading” or insertion of information, which can be uniquely characterized, and which allows operation of the device. In the case of fences, walls, and buildings, “Lock” means an integral door lock or padlock which provides protection equivalent to a six-tumbler cylinder lock.

*Qualification.* Demonstrated successful performance of a given task by a member of the security force meeting the minimum standards and under the stated conditions for that task.

*Safeguards Contingency Plan (SCP).* The safeguards event contingency plan established as Appendix C to the ISFSI Physical Protection Plan by which standards the security force responds to emergencies.

*Safeguards Information.* Information that discloses equipment, procedures, communications, or response plans used to protect certain nuclear material or facilities.

*Security Force.* The onsite, shift-to-shift contingent of security officers trained and qualified in security duties.

*Security Management.* Persons responsible for security at the policy and general management level. The Facility Safety Officer holds this position at the ISFSI.

*Security Officer.* An individual, not necessarily uniformed or armed, whose primary duty is the protection of the ISFSI spent fuel against radiological sabotage. Except for the Alarm Station Operator, security officers may perform other non-security-related duties pertaining to the operation of the ISFSI.

*Security Related Keys/Cores.* Those specifically designated keys and lock cores controlled by the security force that are used to control access to the Alarm Station, MVDS, and other areas as determined by the Facility Safety Officer.

*Security Storage Container.* Any of the following repositories:

For storage in a building located within a protected or controlled access area, a steel filing cabinet equipped with a steel locking bar and a three position, changeable combination, General Services Administration (GSA) approved padlock.

**FSV SECURITY ADMINISTRATION**

Identifier: MCP-325

Revision\*: 8

Page: 20 of 35

A security filing cabinet that bears a Test Certification Label on the side of the locking drawer, or interior plate, and is marked, “General Services Administration Approved Security Container” on the exterior of the top drawer or door.

A bank safety deposit box.

Other repositories, which in the judgment of the Commission, would provide comparable physical protection.

*Security Supervision.* Persons, not necessarily uniformed or armed, whose primary duties are supervision and direction of security at the day-to-day operating level. This function is performed by the Alarm Station Operator.

*Security Training and Qualification Plan (STQP).* The training plan established as Appendix B to the ISFSI Physical Protection Plan by which standards security force members are trained.

*Site.* The land owned by DOE on which the ISFSI Compound and Alarm Station is located. Refer to the ISFSI Safety Analysis Report (ISFSI SAR) for exact acreage.

*Standards.* Those measurable and/or observable characteristics of a task that tell how well it is being, or has been, performed. Standards may include time constraints.

*Task.* A task is normally a highly specific action performed by a single individual that has a definite beginning and end. A task must be measurable so that a proficient observer can observe the performance of the task or the product produced by the task, and be able to determine the extent to which the task has been properly performed.

*Update Background Investigation.* An investigation conducted for individuals requesting reinstatement of unescorted access whose previous unescorted access authorization was terminated (under favorable conditions) less than 3 years previous to the date of application. The following elements are included: verification of identity, verification of employment or unemployment history since last unescorted access authorization, credit history check, verification of character and reputation with at least two developed references, criminal history check, evaluation of trustworthiness and reliability.

## **7. REFERENCES**

10 CFR 72.180, “Physical Protection Plan”

10 CFR 72.186, “Change to Physical Security and Safeguards Contingency Plans”

10 CFR 73.21, “Requirements for the Protection of Safeguards Information”

10 CFR 73.71, “Reporting of Safeguards Events”

NUREG-0794, “Protection of Unclassified Safeguards Information”

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 21 of 35
------------------------------------	---

NUREG-1304, “Reporting of Safeguards Events”

NUREG-1497, “Interim Licensing Criteria for Physical Protection of Certain Storage of Spent Fuel”

Regulatory Guide 5.65, Vital Area Access Controls, Protection of Physical Security Equipment, and Key and Lock Controls

Regulatory Guide 5.62, “Reporting of Safeguards Events”

ISFSI Physical Protection Plan and Appendices

Colorado House Bill 91-1014

NRC Access Authorization Order (EA-03-097)

## **8. APPENDIXES**

Appendix A, Reporting of Safeguards Events

Appendix B, Safeguards Event Matrix

Appendix C, Background Investigation File

Appendix D, Security Responsibilities and Administrative Operations

Appendix E, Security Training Program

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 22 of 35
------------------------------------	---

## Appendix A

### Reporting of Safeguards Events

#### 1-Hour Reports

The following events affecting the physical security of the ISFSI will be telephonically reported to the NRC Operations Center at (301)816-5100 or (301)951-0550. The on-duty Emergency Coordinator is responsible to ensure the notification is completed within 1 hour of the event declaration. Notification will normally be completed by the INL Warning Communication Center. Notification can be made via commercial telephonic or dedicated telephonic services, or any other method that will ensure report is made within 1 hour. This report will be followed within 30 days with a written report as provided for in 10 CFR 73.71(a)(4), Regulatory Guide 5.62 and NUREG 1304. Additional guidance is provided in Appendix B, Safeguards Event Matrix.

- A. Threatened, attempted or actual:
1. Theft or Unlawful diversion of SNM, or
  2. Interruption of normal operation of the ISFSI through the unauthorized use of or tampering with its fuel handling machinery and components, or controls, including the Security System, or
  3. Significant physical damage to the ISFSI or spent fuel carriers, or
  4. Actual entry of unauthorized person into a protected area, controlled access area or transport, or
  5. Actual or attempted introduction of contraband into a protected area, controlled access area or transport, or
  6. Uncompensated failure, degradation, or discovered vulnerability in the safeguards system that could allow unauthorized or undetected access to a protected area, controlled access area or transport. Acceptable compensatory measures and times are available in the PPP and MCP-324, "FSV Physical Security Procedure." For events where the PPP and MCP-324 are silent, compensatory measures will be in place within 10 minutes of event discovery.

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 23 of 35
------------------------------------	---

24-Hour/Quarterly Log Reports

- A. The following events affecting the physical security of the ISFSI shall be entered on a log within 24 hours of discovery, see example (Form FSV-040), Safeguards Event Log. Compensated failure, degradation, or discovered vulnerability in a safeguards system that if uncompensated could have allowed unauthorized or undetected access to a protected area, controlled access area or transport.
1. Any other threatened, attempted, or committed act not previously defined in Appendix G of 10 CFR 73 that has the potential for reducing the effectiveness of the safeguards system below that committed to in the PPP or the actual condition of such reduction in effectiveness.

<p><b>FSV SECURITY ADMINISTRATION</b></p>	<p>Identifier: MCP-325                  Revision*: 8                  Page: 24 of 35</p>
---	--

**Appendix B**

**Safeguards Event Matrix**

CATEGORY	SUBCATEGORY	DESCRIPTION	1 HOUR	24 HOUR	SIR ONLY
Alcohol/Drugs		Security degradations caused by the use of alcohol or drugs or the discovery of alcohol or drugs within the AS or MVDS PA	XX		Immediately report occurrence to the Facility Safety Officer.
Firearms or Contraband		Events involving the discovery of firearms, ammunition or contraband in the PA Intentional Introduction or significant threat Unintentional introduction	XX	XX	
Hardware System	<b>(This category is not reportable if the failure or degradation is planned due to maintenance or similar circumstances and compensatory measures are in place prior to the failure, degradation or removal from service.)</b>				
	CCTV Failure	Mechanical failure of CCTV hardware or components. Uncompensated. Compensated.	XX	XX	
	Communications	Interruption or degradation of communications to onsite and/or offsite locations including telephone or radio malfunction or interference. Uncompensated. Compensated.	XX	XX	
	Computer	Failure of the alarm processing unit. Uncompensated Compensated.	XX	XX	
	Door	Failure of the door alarm and/or other hardware such as latches, locksets or hinges. Uncompensated. Compensated.	XX	XX	
	Other Failures	All other component failure not categorized in other hardware system categories. This includes discoveries of uncompensated barrier penetrations or barrier design flaws. Uncompensated. Compensated.	XX	XX	
	False Alarms	Detection system events involving <u>False or nuisance</u> alarms. These alarms are the result of environmental conditions or unknown causes.  <u>Less</u> than four alarms in 60 minute period.  Four (4) or more alarms in a 60 minute period. Multiple alarms cause significant degradation of system capability. Uncompensated. Compensated.	XX	XX	XX

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 25 of 35
------------------------------------	---

CATEGORY	SUBCATEGORY	DESCRIPTION	1 HOUR	24 HOUR	SIR ONLY
	Detection System	Failure of the detection system, including alarms, due to component malfunction. This includes intermittent failures where they system fails to function properly but can be restored to use without immediate repair. This includes events where the system is found defective or did not function properly during testing. Uncompensated Compensated Falls testing/Uncompensated Falls testing/Compensated Falls testing while compensated	XX	XX	XX
	Power/Lighting	Loss of power that affects the functioning of security equipment or the loss of lighting other than momentary (less than 60 seconds) or insufficient lighting due to other causes (i.e., burned out bulbs.) Uncompensated Compensated Momentary	XX	XX	XX
Hoax		Events that resulted in unsubstantiated bomb or extortion threats. Media is aware of event. Media is unaware.	XX	XX	
Human Error	Access Control and Authorization	Events caused by incorrect access authorization information, incomplete screening records, or incorrect evaluation of psychological tests.		XX	
	Escort Errors	Events caused by individuals who become separated from their escort. Intentional/threat Intentional/no threat Unintentional/Promptly corrected	XX	XX	XX
	Non-Performance of Guard Duty	Members of the security force who neglected to properly perform an assigned function such as a required search, patrol, test or left their assigned post uncompensated. Drugs/Alcohol involved No drug/alcohol involvement Uncompensated Compensated	XX	XX	
	Non-Security Force Error	Human error events on the part of personnel, other than security force members not in other subcategories. Intentional/threat Intentional/no threat Unintentional	XX	XX	XX
	Other Security Force Error	Human error events caused by security force members that are not in other subcategories. Includes compromise of keys and failure to return keys at end of shift. Intentional/threat Intentional/no threat Unintentional	XX	XX	XX

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 26 of 35
------------------------------------	---

CATEGORY	SUBCATEGORY	DESCRIPTION	1 HOUR	24 HOUR	SIR ONLY
	Safeguards Information	Events associated with the loss, theft, improper handling, marking, and storage of documents containing Safeguards information. Significant threat Insignificant threat Improperly marked as Safeguards	XX	XX	XX
	Unsecured Door	Doors which are found to be unsecured with no compensatory officer posted are assumed to be the result of personnel error unless determined to be caused by component failure (latch, lock, strike). Unauthorized Entry Made No Unauthorized Entry Made	XX	XX	
Miscellaneous Event	Arson	Intentional acts involving incendiary materials resulting in damage to property, equipment or other assets.	XX		
	Bomb Device	Concerned with the discovery or credible threat of explosives or incendiary devices.	XX		
	Civil Disturbance/Demonstration	Events concerning demonstrations.	XX		
	Intrusion	Actual or attempted intrusions of the MVDS or AS.	XX		
	Missing SNM	Events in which SNM is found to be missing.	XX		
	Theft of SNM	Events in which SNM is found to be stolen.	XX		
	Compensatory Measure Failure	A failed compensatory measure such as an inattentive officer or equipment that fails after being successfully placed in service as a compensatory measure. Uncompensated Compensated	XX	XX	
	Transportation	SNM was misrouted or involved in an accident while being transported.	XX		
	Vandalism	Destruction or attempted destruction of property, parts, and equipment which does not directly cause a radioactive release.	XX		
	Minimum Number of Security Personnel Unavailable	Events where the minimum number of security personnel are unavailable for duty. Uncompensated Compensated	XX	XX	

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 27 of 35
------------------------------------	---

## Appendix C

### Background Investigation File

Each Background Investigation file shall incorporate the following elements:

#### **Employment History**

Except as noted, employment history must be obtained, on a best effort basis, for the past 3 years through contacts with previous employers by obtaining the following information. If the entire 3-year period cannot be verified, access may be granted after a shorter period of time of not less than 2 years has been verified.

1. Verification of all claimed period of employment of 30 days or more
2. Disciplinary history
3. Reasons for termination and eligibility for rehire
4. Any other information that would adversely reflect upon the reliability and trustworthiness of the individual
5. Activities during interruptions of employment in excess of 30 days must be verified.

#### **Education History**

High School or General Education Diploma must be verified regardless of time.

#### **Criminal History**

A criminal files check of each state of residence in the previous 3 years. This may be accomplished via state, country or local records on a documented best effort basis or through the submittal of fingerprints to the FBI through the Colorado Bureau of Investigation in accordance with Colorado law (Colorado Revised Statutes 91-1014).

#### **Full Credit History**

Documentation of credit history report (for example, copy of on-line or written report from credit reporting agency).

#### **Military Service**

Military service performed within the previous 3 years (claimed or developed) must be verified by receipt of a DD214 or other acceptable records. Foreign military service within the previous 3 years is verified on a best effort basis.

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: <b>28</b> of 35
------------------------------------	--

### **Character and Reputation**

The applicant's reputation for emotional stability, reliability, and trustworthiness must be examined through contact with two references supplied by the applicant and at least two additional references (not related to the applicant) developed during the investigation. It is not necessary that the reference's (individually or collectively) association with, or knowledge of, the applicant for unescorted access cover the entire 3-year retrospective period. Emphasis must be placed on:

1. Identified psychological problems
2. Criminal history (no felony convictions involving the use of a weapon or that reflects on the individual's reliability)
3. Illegal use or possession of a controlled substance
4. Abuse of alcohol
5. Susceptibility to coercion
6. Any other conduct relating to an applicant's trustworthiness or reliability to discharge job duties.

### **Verification of Identity**

Identify must be verified through such means as:

1. Photographs
2. Birth certificate
3. Comparison of applicant's physical characteristics with employment, education, military, or other records
4. Employer or character references who have a personal acquaintance with the applicant.

Reliability and stability must be determined by the result of a reliable written personality test. The results of such test must be evaluated by a qualified and licensed psychologist or psychiatrist, along with a personal interview to discuss the test results. If the results of the written test or procedure identify any psychological abnormalities that may indicate emotional instability, unreliability, or untrustworthiness, or the results need further clarification, upon the request of the FSO, another written test may be conducted and the results re-evaluated by a qualified and licensed psychologist or psychiatrist.

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: <b>29</b> of 35
------------------------------------	--

In addition to the above requirements, security force personnel shall meet the suitability requirements of the ISFSI Security Training and Qualification Plan.

With the exception of photocopied or faxed replies to requests for information, all documentation developed or received in the course of the investigation shall meet one of the following:

- A. Original documents
- B. Certified or notarized copy of the original
- C. A copy of the document annotated with or accompanied by a signed statement from the investigator identifying how the document was verified
- D. Original copies of investigator's telephonic inquiries, which include the name of the individual providing the information, the actual information, and the name of the investigator.

In addition to the above requirements, each file shall include as a separate item the information required by Section 4.3 (the Unescorted Access Data Sheet) of this procedure.

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 30 of 35
------------------------------------	---

## Appendix D

### Security Responsibilities and Administrative Operations

#### Personnel Responsibilities

A Management System has been established to provide for the development, revision, implementation, and enforcement of security procedures. The functional responsibilities and “Security Chain of Command” are addressed below:

The ISFSI Management Department Manager, or equivalent M&I Contractor position: Provides support at the Senior Management Level for the FSV ISFSI and has authority and responsibility to ensure continued safety and overall management of the ISFSI.

ISFSI Manager: Assumes administrative responsibility for overall operations management of the ISFSI.

Facility Safety Officer (FSO): Reports directly to the ISFSI Manager and is responsible for all day to day security operations at the ISFSI including:

- A. Directing administrative and regulatory implementation for installation security
- B. Ensuring minimum security staffing per PLN-176, Step 3.2.10, is met at all times.
- C. Coordinating and planning with offsite response force activities with the LLEA point-of-contact and emergency response
- D. In addition, the FSO is responsible for safety, quality, radiation control, and emergency response activities at the ISFSI.

Alarm Station Operator (ASO): The alarm station is normally continuously staffed by the ASO who acts as senior on-shift security position. Duties include:

- A. Monitoring and directing the physical security activities of the security force

**NOTE:** *The ASO may transfer alarm annunciation system monitoring duties to the WCC CAS operator if it becomes necessary to leave the Alarm Station. This relief is intended to be “temporary” in nature for non-emergency situations.*

- B. Monitoring the alarm annunciation system and remote assessment equipment (CCTV System), and initiating appropriate response activities
- C. Advising the FSO and ISFSI operations staff of ongoing security conditions

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 31 of 35
------------------------------------	---

- D. Ensuring security procedures and instructions enforcement
- E. Ensuring personnel accountability is conducted during emergency situations.
- F. In the event the patrol fails or is unable to perform his/her duties, the ASO will contact a backup security force member to report for duty and continue surveillance of the MVDS.

Security Force: Assumes responsibility for the physical protection of the ISFSI. Duties include:

- A. Patrol duty
- B. Performing detection, assessment, and response functions as defined in security instructions/procedures
- C. Conducting access control, identification verification, and escort duty as needed
- D. Testing alarms, barriers, and security equipment as required by security procedures
- E. Acting in a compensatory measure capacity, as needed
- F. Conducting emergency accountability
- G. In the event the ASO fails or is unable to perform his or her duties, a remaining Security Force member assumes the duties and responsibilities of the ASO, and contacts a backup security force member to report for duty, if necessary.

Secondary Alarm Station (WCC CAS) Operator: is responsible for:

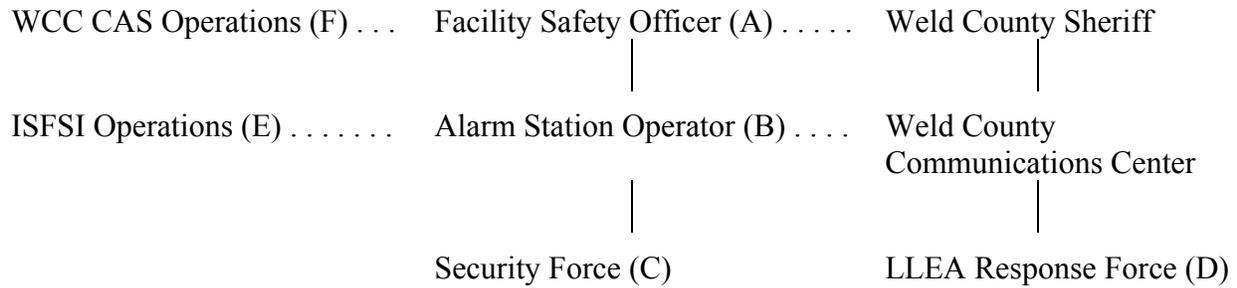
**NOTE:** *The WCC is continuously staffed and is capable of video assessment, receiving FSV alarm indications, and contacting the FSV LLEA as required.*

- A. Monitoring alarm annunciation if requested by the FSV ASO, or on-duty EC
- B. Making required emergency response notifications
- C. Monitoring, acknowledging, and (when appropriate) responding to alarm indications.

Response Force: Composed of LLEA personnel - prevents or impedes attempted acts of radiological sabotage of spent fuel.

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 32 of 35
------------------------------------	---

**Security Organization Chain Of Command**



**NOTE:** *Dotted lines indicate communications.*

- A. FSO is responsible for coordination and planning with offsite response forces, and the INL’s Warning Communications Center (WCC); and directing administrative and regulatory responsibility for installation security
- B. ASO is responsible for monitoring the alarm annunciation system and initiating appropriate response activities, including notifying the INL WCC. Directing the activities of the security force
- C. Security force is responsible for patrols, compensatory measures and detection and response functions. This function normally consists of at least one (1) armed, non-dedicated individual per shift
- D. Weld County Sheriff Department (LLEA) has committed to respond to the ISFSI in a timely manner (consistent with State and local statutes) of a request for assistance. The LLEA, upon arrival, will assume responsibility for assessing and dealing with the situation
- E. The ASO and ISFSI Operations are responsible for keeping each other advised on security matters
- F. The Warning Communications Center (WCC) CAS Operator is responsible for notifications and backup monitoring for the FSV Alarm Station when required.

**Approval Authority**

Approval for the use of the Physical Protection Plan and its implementing procedures are by written authorization of the ISFSI Manager or designee. change tracking number, revision number, and effective date of the security procedures is located on the first page of each procedure.

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 33 of 35
------------------------------------	---

### **Procedure Conflicts and Revisions**

In the event of a conflict between two procedures and in the absence of definite Commission guidance, the PPP shall always be the deciding document. If the PPP is silent on the issue in conflict, the most conservative of the two procedures shall be followed.

The FSO ensures necessary changes are made to procedures. Clarifications or enhancements may be provided by temporary instructions maintained in the Post Status Book.

### **FSV Security Forms**

Forms used in the security program are approved for use by the ISFSI Manager or designee.

ISFSI security forms include a controlled form number, revision number, and issue date.

### **Plan, Procedure, and Forms Control**

The INL Security Classified Document Control Center controls Physical Protection Plan and implementing procedure (containing Safeguards Information) history files in accordance with Quality and Security/Safeguards protection requirements. Plans and procedure originals are maintained in secure storage and copies issued as required. Only current copies are issued for use. The FSO shall ensure one copy of the Physical Protection Plan and implementing procedures will be located in the alarm station.

The INTEC Document Control Center controls the security form and implementing procedure (not containing Safeguards Information) history files in accordance with Quality and Security protection requirements.

### **Security Record Quality**

All records generated by the Security Personnel shall be typed or printed in black ink, and records generated by non-security personnel should be typed or printed in black ink whenever practical.

The FSO is responsible for ensuring that records are legible, complete, and are traceable to the items or activities involved. Copies of quality records sent to the off-site records retention location must be validated as complete and correct. Corrections are made by lining out the incorrect information (single line) making the correction and initialing and dating the correction. The use of white out or correction tape is prohibited.

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 34 of 35
------------------------------------	---

### **Authorized Designees**

Any security related duty of the FSO may be delegated to an authorized designee. Authorized designees are appointed in writing. This written authorization may be incorporated into the Security Implementation Plan. The FSO retains responsibility for the actions of the designees.

The FSV ASO or the WCC CAS Operator may call for LLEA Assistance independent of higher authority.

### **Security Implementation Plan (SIP)**

The FSO, or designee ensures an SIP is published, at least monthly, establishing security patrol criteria, call-out lists, emergency and non-emergency telephone numbers, and a test schedule for security related equipment as described in the ISFSI PPP. The unescorted access list is normally issued as an attachment to the SIP. If the unescorted access list is issued separately, the SIP may be published quarterly.

### **Post Status Books**

Post Status Books reside in the Alarm Station, the MVDS, and/or other areas deemed appropriate, and contain the following; at a minimum:

- A. Current implementation plan
- B. Current unescorted access list
- C. Copy of valid Unescorted Access Data Sheet(s) (may be discarded once an individual has been added to the Authorized Access List)
- D. Copy of Visitor Access Authorizations
- E. Copy of valid MVDS Vehicle Access Authorizations
- F. Media/public call referral list for rumor control
- G. Special instructions and information that are short term in nature are not required to be added to approved procedures or the Implementation Plan. Such instructions and information are reissued or deleted as appropriate after 30 days and are marked with an expiration or review date before being placed in the Post Status Book.

The Post Status Book is examined at the start of each shift by the individual assuming the post. Each Post Status Book is routinely reviewed for complete, accurate, and up-to-date information by the FSO.

<b>FSV SECURITY ADMINISTRATION</b>	Identifier: MCP-325 Revision*: 8 Page: 35 of 35
------------------------------------	---

## Appendix E

### Security Training Program

#### Ft St Vrain ISFSI Security Training Program

Training Waivers: No portion of the ISFSI training program may be waived.

Course Description: The training program consists of:

- A. Initial Class Room Training
- B. Initial Practical Training
- C. Initial Qualification Tasking
- D. Annual Refresher Training, if applicable
- E. Annual Requalification Tasking
- F. Training on the use of hand-held or portable fire extinguishers.

Length of Training: The minimum length of each portion of the training program is determined by the instructor, based on the size of the class and student aptitude.

Program Content: The Security Training Program consists of the ISFSI Security Procedures, ISFSI Security Lesson Plans (created by the security subcontractor, or other vendor or supplier, and approved by the FSO), and Practical Training. This program is designed to develop an understanding of the ISFSI Security System and the proper use of the procedures that pertain to the security force member's duties and responsibilities.

Evaluation: Tasks, Conditions & Standards

- A. Prior to assignment to the security force, each individual must successfully qualify by demonstrating proficiency under the conditions specified and in accordance with the indicated standards for the applicable tasks
- B. Individual tasks may be performed for qualification or requalification in actual or simulated situations or conditions
- C. For requalification, routine on-the-job performance of appropriate tasks will suffice when completed to the specified standards
- D. Successful completion of a task must be verified and certified by the Facility Safety Officer or designee.