

Idaho National Laboratory

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier:	RD-1002
	Revision:	7
	Effective Date:	03/14/2016

Page: 1 of 36

Subcontractors	Program Requirements Document	eCR Number: 637744
----------------	-------------------------------	--------------------

Manual: INL Subcontractors Requirements

1. PURPOSE

Safeguards and Security (S&S) requirements are established and maintained for subcontractors working at the Idaho National Laboratory (INL). These S&S requirements ensure that appropriate measures are in place to provide protection and accountability for personnel. S&S is also required to protect U.S. government and INL Contractor owned classified and controlled unclassified information, nuclear materials, and computer systems from theft, diversion, sabotage, espionage, or other hostile acts.

2. APPLICABILITY

This document applies to all INL subcontractors and sub-tier contractors working at the INL. Subcontractors may impose stricter requirements upon their employees, and the means of implementation may vary as determined and enforced by the subcontractor; however, compliance with the requirements of this document is mandatory.

Subcontractor S&S requirements may also be contained in the Special Conditions and associated technical documents of the subcontract.

3. REQUIREMENTS**3.1 General Security Requirements**

NOTE: *The contractor is not responsible for delays that occur as a result of a subcontractor employee's failure to comply with the security requirements detailed herein.*

- 3.1.1 The subcontractor shall be responsible for "flowing-down" to all lower-tier subcontractors, unions, and suppliers all pertinent security requirements.
- 3.1.2 All personnel granted access to INL shall comply with all DOE and contractor security regulations and requirements.
- 3.1.3 The subcontractor shall report all abnormal or suspicious activities to the Contractor Point of Contact (POC), or Warning Communication Center (WCC) (526-1515) if the Contractor POC is not available.

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	
	Revision: 7	
	Effective Date: 03/14/2016	Page: 2 of 36

3.2 INL Access Control and Badging

3.2.1 Each subcontractor employee requesting access to INL shall:

- Be 18 years or older
- Be a U.S. citizen
- Receive an initial briefing before receiving an INL security badge
- Report to and obtain a badge from the contractor security office located at an access control point.
- All sub-contractors are required to wear their assigned INL identification badge while on INL premises, property and facilities. Exceptions can only be made when it is not deemed safe to wear the badge during special work situations. In this special situation, the sub-contractor should keep the badge on their person at all times or secured in a location that prevents loss or theft.

3.2.2 In order to have uncleared access to INL, subcontractor employees shall have successfully completed a suitability screening for employment check.

3.2.3 Form 472.70 , “INL Employment Suitability Questionnaires Identification Request Form, and Form 470.01 “Identification Request Form ,” shall be obtained from the contractor security office or by visiting the following link:
https://inlportal.inl.gov/portal/server.pt/community/procurement/346/documents_and_forms

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	
	Revision: 7	
	Effective Date: 03/14/2016	Page: 3 of 36

NOTE: *Failure to return the required forms in a timely manner will result in access being denied.*

3.2.4 When the subcontractor conducts the suitability check, the subcontractor shall establish the job qualifications and suitability of prospective employees prior to their employment through the use of typical personnel investigations in accordance with 48 CFR 970.2201(b)(1)(ii).

3.2.4.1 Personnel investigations shall include:

- Credit check
- Verification of a high school education, or a degree or diploma from an institution of higher learning within the last five years
- Contacts with listed personal references
- Contacts with listed employers for the past three years
- Local law enforcement checks
- Confirmation of any military experience.

3.2.4.2 The employee's job qualifications and suitability shall be established before:

- The employee reports to INL
- The employee is issued a security badge
- A request is made to DOE for a security clearance.

3.2.4.3 If requested the results of the pre-employment/suitability personnel investigation shall be made available to the contractor for eligibility verification for issue of an uncleared picture badge.

3.2.5 When a clearance is required the responsible contractor conducts the required background check. The subcontractor employee shall obtain an appropriate badge before beginning employment at INL.

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	
	Revision: 7	
	Effective Date: 03/14/2016	Page: 4 of 36

3.2.6 Subcontractor drivers making deliveries shall be 18 years or older and possess a valid driver's license with picture identification compliant with the Real ID Act.

3.2.7 All subcontractors who are not U.S. citizens shall be identified and processed in accordance with DOE requirements through the INL Foreign Visits and Assignments office.

3.3 INL Access Control Points and Procedures

NOTE 1: *Additional subcontractor site security access requirements, if any, will be designated in the subcontract Special Conditions.*

NOTE 2: *Specific controls for governing personnel access are established at INL. Officially designated INL access control points have been established. There are four guard access control points (guard gates) that control access to INL site facilities.*

3.3.1 When obtaining access to INL site facilities, subcontractor personnel shall use ONLY the following designated access control points:

- The primary entrance to INL at East Portland between Highway 20/26 and Jefferson Boulevard (Gate 1)
- Lincoln Boulevard between Test Area North (TAN) and Naval Reactor Facility (NRF), located immediately south of the junction with U.S. Highway 33 (Gate 4)
- Taylor Boulevard, located approximately 1.3 miles from the entrance to Materials and Fuels Complex (MFC) at U.S. Highway 20 (Gate 2)
- North Van Buren located approximately 0.3 miles north of the junction with U.S. Highway 20/26 (Gate 3).

3.3.2 When obtaining initial access to INL Idaho Falls facilities, subcontractor personnel shall use ONLY the following designated access control point:

- Willow Creek Building (WCB) at 1955 Fremont Avenue.

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	
	Revision: 7	
	Effective Date: 03/14/2016	Page: 5 of 36

NOTE: *Any subcontractor employee who does not have a valid INL security badge will be directed to an access control point or the contractor security office for issuance of a badge. If the individual is working for a valid subcontractor and has forgotten his/her badge, the individual will be directed to an access control point or the contractor security office and issued a one day temporary “forgotten” badge.*

- 3.3.3 All vehicles used for subcontractor purposes shall be clearly marked with the subcontractor's company name in **one-inch-high letters** (minimum) on each side of the vehicle.
- 3.3.4 Upon arrival at a contractor facility, subcontractor personnel shall submit all vehicles and hand-carried articles for warrantless search and inspection.
- 3.3.4.1 During vehicle searches, all occupants shall exit from the vehicle and open all receptacles such as:
- Glove box
 - Hood
 - Trunk
 - Toolboxes
 - Briefcases
 - Lunch boxes.
- 3.3.4.2 The occupants shall step away from the vehicle until the search and inspection is completed.
- 3.3.4.3 The occupants shall NOT proceed until completion of the search and inspection.
- 3.3.5 Subcontractors shall NOT control access to an INL facility.
- 3.3.6 Badged subcontractors can allow other badged persons including other badged subcontractors to “piggyback” into specific INL facilities. The person who opened the door must ensure everyone they let in has a valid badge or pass and are authorized access to that area. If they have any doubt they must not allow them access, instead they will close the door and ask the person to card in. Subcontractors will contact the TPOC

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	
	Revision: 7	
	Effective Date: 03/14/2016	Page: 6 of 36

with any questions about whether the facility you are working at makes this allowance.

3.4 Security Clearance

NOTE: *The subcontract Special Conditions contract or Technical Point of Contact (TPOC) will identify whether or not subcontractor employees require a security clearance. Uncleared subcontractor employees will be allowed unescorted access to property protection areas (PPA), providing they have an INL picture badge and have completed all access and training requirements.*

3.4.1 Prior to badging , all personnel shall obtain:

- QL00IGET – INL General Employee Access
- QLSECBRF – INL Security Briefing
- QLCNTINT – Counterintelligence (0TRN1372)
- ONCURVWR – Controlled Unclassified Information (Z735)
- INL Environmental Management System (00INL935)
- Z414 Comprehensive Security Briefing and AN5 Annual Security Briefing for cleared employees or Z415 Initial Security and Counterintelligence Briefing and AN8 Annual Security Briefing for un-cleared employees.

3.4.2 If the justification for a clearance has been approved by Personnel Security, subcontractor personnel shall complete and submit form SF-86, Questionnaire for National Security Positions, DOE F206.4 Information Sheet For Sponsorship of HSPD-12 Credential and complete the identify proofing fingerprint process by electronic copy. This process will be completed as follows.

NOTE: *In order to obtain a security clearance, the program requesting clearances for subcontractors is required to provide justification..*

3.4.2.1 Complete the online clearance forms, and then return the required hard copy forms or documentation to INL Personnel Security within 30 days. The individual receiving the SF-86 form must complete and submit the form to Personnel Security for review within 30 days from the date

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	
	Revision: 7	
	Effective Date: 03/14/2016	Page: 7 of 36

the e-mail containing the link to the form is sent to the employee.

3.4.2.2 The SF-86 form must be submitted to DOE no later than 14 calendar days from the date the form was certified in the e-QIP system.

3.4.2.3 When an access authorization (clearance) has been granted by DOE, the subcontractor must complete a security briefing and Standard Form 312, on-line training Z414 and AN8 before an "L" or "Q" security badge can be issued.

3.4.2.4 As long as a clearance is active, the subcontractor shall complete a security refresher briefing online (AN5 Annual Security Briefing) approximately every 12 months.

3.4.3 Each subcontractor employee who will act as an escort for other subcontractor personnel shall complete, Z414, ZVISITOR, and QLSECBRF Qualification Training.

NOTE: *The subcontract Special Conditions will identify under what circumstances, if any, escort requirements may be involved.*

NOTE: *There are no escort requirements for PPA areas in REC facilities. Any safety escorts are under the TPOC jurisdiction.*

3.4.4 Subcontractors shall NOT escort non-U.S. Citizens.

NOTE: There are no escort requirements for PPA areas in REC facilities. Any safety escorts are under the TPOC jurisdiction.

3.5 Control and Surrender of Badges

3.5.1 The subcontractor shall ensure that requests for badge transfers are properly executed during the course of work on the subcontract and that all badges are surrendered upon completion of the subcontract.

3.5.2 Within 24 hours of permanently transferring a subcontractor employee to another subcontract with the same subcontractor, the subcontractor shall notify TPOC and SA of the transfer request.

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	
	Revision: 7	
	Effective Date: 03/14/2016	Page: 8 of 36

- 3.5.3 When a subcontractor employee completes the subcontract work, excluding transfers (see Step 3.5.2), the subcontractor shall comply with all exit requirements as follows.
- 3.5.3.1 The employee shall surrender his/her badge.
- NOTE:** *The badge may be surrendered at the contractor's main security office on East Portland or WCB.*
- 3.5.3.2 An employee holding a security clearance shall sign a Security Termination Statement, DOE Form F5631.29 the day of the employee's termination.
- 3.5.4 Subcontractor employees not currently working at INL or not assigned to a current subcontract shall immediately surrender their security badges to contractor security and notify the TPOC.
- 3.5.5 Upon notification of termination "**for cause**," the employee shall be escorted by the subcontractor until the employee departs from the INL and surrenders their badge at a badging office or security post.
- 3.5.6 At the conclusion of the project and prior to requesting final payment, the subcontractor shall notify the subcontract administrator (SA) that all security badges have been either reassigned (to another subcontract) or returned.

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	
	Revision: 7	
	Effective Date: 03/14/2016	Page: 9 of 36

NOTE: *If all security badges have been transferred (to another subcontract) or surrendered, Physical Security will issue a release form to the SA. This release form will be attached to the final payment request. The payment will then be processed. If all badges are not accounted for, the subcontractor will be issued a list of unaccounted for badges from the SA. Once all issues are resolved, a release form will be issued to the subcontractor and attached to the final payment request.*

- 3.5.7 All sub-contractors are required to immediately report a lost or stolen badge to the Warning Communications Center (526-1515).

3.6 Illegal Drugs and Controlled Substances

NOTE: *Through the Drug Free Work Place program, employees may be screened based on reasonable suspicion, accident, or incident. The contractor reserves the right to require a urine drug screen or a blood alcohol screen based on reasonable suspicion of illegal substance use; abuse of legal substances; or involvement in an accident or incident resulting in personal injury, death, or property damage.*

- 3.6.1 Any personnel under the subcontractor (including lower tier contractors and vendors) who become aware of, or have knowledge of, the illegal use or possession of drugs or controlled substances by any individual shall immediately report that information to their supervisor, superintendent, or manager.
- 3.6.2 The subcontractor shall immediately report information of illegal use or possession of drugs or controlled substances to the Contractor Point of Contact.
- 3.6.3 The subcontractor's supervisor, superintendent, or manager shall immediately prevent access to classified matter by implicated individual(s) and or remove the individual(s) from any security area.
- 3.6.4 If the implicated individual(s) cannot immediately and clearly establish that the drug or controlled substance in question was legally obtained or used, the subcontractor's supervisor, superintendent, or manager shall escort the individual(s) to the contractor's security office.

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	
	Revision: 7	
	Effective Date: 03/14/2016	Page: 10 of 36

NOTE 1: *Proof of legal purchase may consist of written evidence that the controlled substance was prescribed or administered by a licensed physician or was legally purchased over the counter.*

NOTE 2: If it is determined the individual is in lawful possession of the controlled substance, the subcontractor's supervisor, superintendent, or manager shall initiate a fitness for duty evaluation to ensure the individual may continue working while taking the medication.

NOTE 3: *When the implicated individual(s) arrive at the security office, their security badge(s) will be confiscated and the individual(s) will be informed of what further action will be taken by the contractor.*

3.7 Prohibited Activities

3.7.1 Subcontractor personnel shall not participate in any form of hunting or fishing activities within INL boundaries.

3.7.2 Subcontractor personnel shall comply with all INL over-flight requirements.

3.7.2.1 All proposed flights over any portion of INL by any type of aircraft at altitudes currently prohibited by the Federal Aviation Administration shall be approved in advance by DOE-ID Safeguards and Security.

3.7.2.2 All INL overflights must meet the requirements of MCP-516, "Notification of INL Overflight."

NOTE: *Sub-contractors wishing to conduct overflight(s) of INL facilities need to obtain permission from the Area Physical Security Officer before conducting Overflights of INL facilities for the purpose of taking photos, video, or other activities. See INL General Physical Security Plan, PLN-1466 for details.*

3.8 Prohibited and Controlled Items/Articles

3.8.1 Employees shall not - bring prohibited items/articles to the site with the intent of storing them at a designated INL entrance.

Idaho National Laboratory

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	
	Revision: 7	
	Effective Date: 03/14/2016	Page: 11 of 36

NOTE: *All personnel and vehicles entering and leaving INL properly are subject to search conducted by INL Security personnel.*

NOTE: *INL Security personnel will periodically make unannounced property compliance checks. This will include random personnel and vehicle property compliance searches.*

3.8.2 Prohibited items/articles include:

- Alcoholic beverages, Illegal drugs
- Firearms (including hunting rifles), ammunition, other weapons
- Explosives
- Non-badged people (i.e., family, friends, babies)
- Pets (except service animals such as seeing eye dogs)
- Knives with blades greater than 4 inches.
- Mace, pepper or bear spray.

NOTE: *Any individual attempting to access the INL Site who has in his/her possession any of the prohibited items listed in Step 3.8.2 above will be turned away at established entrances to the INL property. Accommodations for storage or attendance of prohibited items will be the responsibility of the individual carrier and will not be afforded by the INL under any circumstance. Weapons cannot be checked in at the INL Site, Idaho Falls or RWMC facilities. "NO EXCEPTIONS".*

3.9 Transmitting Devices

3.9.1 Before using any wireless transmitting, excluding cell phone type devices, at INL facilities, the contractor POC shall be notified so that approval may be obtained from the Office of Spectrum Management, 6-7421.

3.9.2 The subcontractor shall supply copies of current FCC allocations to the Office of Spectrum Management.

3.9.3 All transmitting radio equipment shall be limited to 30 watts maximum power output.

3.9.4 A copy of a user permit and FCC license shall be in the possession of each user.

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	
	Revision: 7	
	Effective Date: 03/14/2016	Page: 12 of 36

3.9.5 The subcontractor shall obtain a new approval for any change in FCC licensing.

NOTE: *Prior approval of two-way radio use at a different government site is not transferable to the INL. These permits must be updated annually.*

3.9.6 For all Security Areas at the INL, it is prohibited to use any device having or suspected to have the ability to collect data wirelessly, record audio, record video, transmit over a wireless apparatus, or take pictures. If such devices are deemed mission essential, requirements in LWP-11303 must be followed for approval.

3.9.7 Sub-contractors are not allowed to covertly record any conversations on INL premises, either by audio or video means.

NOTE: *Failure of the subcontractor to comply with INL requirements for use of transmitting devices may result in default termination of the subcontract and/or removal from the contractor proposers' list for a minimum period of one year.*

3.10 Controlled Unclassified Information (CUI)

NOTE 1: *The subcontract Special Conditions will identify whether or not the subcontract contains documents designated as controlled unclassified information.*

NOTE 2: *Drawings and documents that have been designated and stamped as controlled unclassified information are subject to the provisions of Section 148 of the Atomic Energy Act of 1954, as amended. Any person who makes unauthorized disclosure of this information is subject to both criminal and civil penalties.*

3.10.1 The subcontractor shall comply with the controlled unclassified information guidelines of Section 148 of the Atomic Energy Act of 1954, as amended.

3.10.2 Controlled unclassified information shall be protected against unauthorized disclosure.

3.10.3 Each person who receives, acquires, or produces controlled unclassified information shall take reasonable and prudent steps to ensure that it is protected from unauthorized disclosure.

3.10.4 Only U.S. citizens who have an established need-to-know in the performance of official duties shall be allowed access to controlled unclassified information.

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	
	Revision: 7	
	Effective Date: 03/14/2016	Page: 13 of 36

- 3.10.5 Access by non-U.S. citizens shall only be permitted when it is in conjunction with established cooperative agreements, treaties, mutual defense acts, or DOE contracts.
- 3.10.6 To prevent unauthorized access, removal, or copying of controlled unclassified information, such information shall remain under the control of the responsible person.
- 3.10.7 When controlled unclassified information is outside of an access-controlled facility, the information shall be stored in a locked desk, file cabinet, or office.
- 3.10.8 Storage inside access controlled facilities should be out of sight, such as in a desk, file cabinet, or credenza.

3.11 External Transmission or Reproduction of Documents, Information and Photographs

- 3.11.1 Documents that are identified as possibly containing controlled unclassified information shall only be transmitted outside an authorized place of use or storage by the INL mail service, U.S. mail, or an individual with authorized access.
- 3.11.2 Documents shall be packaged to preclude disclosure of the presence of controlled unclassified information.
- 3.11.3 Packages to be mailed shall be marked with both a recipient address and return address.
- 3.11.4 Controlled unclassified information may only be discussed or transmitted over unprotected telephone or telecommunication circuits, or processed or produced on an automatic data processing system if it complies with the guidelines of the Office of Management and Budget (OMB) circular A-71 for the protection of controlled unclassified information.
- 3.11.5 Controlled unclassified information shall be reproduced only when necessary to carry out official duties.
- 3.11.6 Reproduced controlled unclassified information shall be properly marked.
- 3.11.7 Requests for release of controlled unclassified information to sources without a need-to-know shall be referred to the contractor security office.

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	
	Revision: 7	
	Effective Date: 03/14/2016	Page: 14 of 36

NOTE: *Subcontractor failure to comply with the following disposal requirements will result in the contractor withholding final payment until such time as the subcontractor complies.*

- 3.11.8 When controlled unclassified information is no longer needed or the subcontract work is completed and accepted, the subcontractor shall properly dispose of the information.
- 3.11.8.1 For offsite disposal, the subcontractor shall verify in writing to the SA that all subcontractor documents and other materials that contained controlled unclassified information have been disposed of by methods that ensure complete destruction or otherwise preclude retrieval.
- 3.11.8.2 For onsite disposal, the subcontractor shall submit all subcontractor documents and other materials containing controlled unclassified information to the SA for disposal.
- 3.11.9 Prior to taking photographs of INL facilities, including projects, the individual must receive authorization from the INL Point of Contact and Area Physical Security Officer.
- 3.11.10 Sub-contractors shall not use any personal electronic device to store or transmit CUI. Only government issued thumb drives or external storage devices may be used to house CUI. Additionally, sub-contract personnel are not allowed to connect personally owned electronic devices to a government computer due to the threat of introducing a virus inside the INL Computer Network. Examples of these devices include, but are not limited to personal cell phones, personal thumb drives, lap top computers, or iPods, etc.

3.12 Additional Requirements

- 3.12.1 All INL sub-contractors are responsible to read and adhere to the INL General Physical Security Plan, PLN-1466. (See attachment in Appendix A)
- 3.12.2 All INL sub-contractors that handle CUI information in the course of their assigned duties should read and adhere to Lab Wide Procedure, LWP-11202, "Controlled Unclassified Information Program."

4. DEFINITIONS

For definitions of terms used throughout the INL Subcontractors Requirements Manual, refer to LST-359.

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	
	Revision: 7	
	Effective Date: 03/14/2016	Page: 15 of 36

5. REFERENCES

5.1 Source Documents

48 CFR 970.2201(b)(1)(ii), Basic Labor Policies

Section 148 of the Atomic Energy Act of 1954, as amended

Office of Management and Budget (OMB) circular A-71

5.2 Related Documents

RD-5001, "Training and Indoctrination"

SF-86, "Questionnaire for Sensitive Positions"

DOE Form F5631.29, "Security Termination Statement"

DOE Form 206.4, "Information Sheet for Sponsorship of HSPD-12 Credential"

PLN-1466, "INL General Physical Security Plan"

LWP-11202, "Controlled Unclassified Information Plan"

6. APPENDIXES

A. PLN-1466, "INL General Physical Security Plan"

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002
	Revision: 7
	Effective Date: 03/14/2016
Page: 16 of 36	

APPENDIX A.

Document ID: PLN-1466
Revision ID: 15
Effective Date: 11/20/2014

Plan

**INL General Physical
Security Plan**



The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance.

Idaho National Laboratory

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002
	Revision: 7
	Effective Date: 03/14/2016

Idaho National Laboratory

INL GENERAL PHYSICAL SECURITY PLAN	Identifier: PLN-1466
	Revision: 15
	Effective Date: 11/20/14

Physical Security	Plan	eCR Number: 627235
-------------------	------	--------------------

Manual: 11B – S&S Protection Program Operations

REVISION LOG

Rev.	Date	Affected Pages	Revision Description
4	05/12/08	Page 4, para 5	Corrected error in reference to AN8 and Z415
		Page 3	Step – 6.3 added
		Page 11	References updated
		Page 12	Records Disposition Authority Updated
5	04/02/09	All	See ECR-568624
6	10/13/09	Page 6	See eCR-574503
7	12/21/09	Pages 5 - 7	Updated Visitor Request Process General formatting
8	02 Mar 10	Pages 9, 10, 13, 14	Updated prohibited articles paragraph to reflect current laboratory policy. Added paragraphs to address new DOE M 470.4-2A requirements regarding motorized gate controllers and as part of the implementation plan power supply elements
9	02/10/11	New Section 19	Added the process for assessing site Trespassing signs.
10	03/10/11	Page 10	Rev 10 Sec 12 due to an inactive document is being referenced.
11	04/05/11	Page 10	Rev 11 Sec 12 is referencing the new LWP-11303
12	08/25/11	Page 8	Added paragraph 9, regarding INL Tours
13	06/21/12	All	Changes throughout the document.
14	07/17/13	All	Update references, added verbiage to describe General Access Area. Changes throughout the document.
15	11/20/14	Page 6, para 7.2.1	REAL ID compliance

CONTENTS

1. PURPOSE.....3

Idaho National Laboratory

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	Page: 18 of 36
	Revision: 7	
	Effective Date: 03/14/2016	

Form 412.09 (Rev. 10)

Idaho National Laboratory

INL GENERAL PHYSICAL SECURITY PLAN	Identifier: PLN-1466	Page: 2 of 20
	Revision: 15	
	Effective Date: 11/20/14	

- 2. SCOPE AND APPLICABILITY3
- 3. SECURITY ADMINISTRATION3
- 4. PERSONNEL SECURITY4
- 5. SECURITY AWARENESS4
- 6. ACCESS4
- 7. VISITOR ACCESS (U.S. Citizen)5
- 8. VISITOR ACCESS (Non - U.S. Citizen)8
- 9. VISITORS ATTENDING SPECIAL EVENTS8
- 10. TOURS9
- 11. EMPLOYEE ACCESS9
- 12. ESCORT REQUIREMENTS10
- 13. INSPECTION PROCEDURES10
- 14. CAMERA AND RECORDING DEVICE USE POLICY12
- 15. SPECIAL NUCLEAR MATERIAL (SNM) STORAGE15
- 16. MOTORIZED GATE CONTROLLERS15
- 17. POWER SUPPLY ELEMENTS15
- 18. SECURITY KEYS15
- 19. CONTROLLED UNCLASSIFIED INFORMATION16
- 20. CONSTRUCTION SECURITY PROCEDURES17
- 21. TRESPASSING SIGNS17
- 22. DEFINITIONS17
- 23. REFERENCES19
- 24. RECORDS20

Idaho National Laboratory

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	Page: 19 of 36
	Revision: 7	
	Effective Date: 03/14/2016	

Form 412.09 (Rev. 10)

Idaho National Laboratory

INL GENERAL PHYSICAL SECURITY PLAN	Identifier: PLN-1466	Page: 3 of 20
	Revision: 15	
	Effective Date: 11/20/14	

1. PURPOSE

- 1.1 This plan outlines the general security requirements for all Idaho National Laboratory (INL) areas and buildings within a *General Access Area* (see def.) (GAA) or *Property Protection Area* (see def.) (PPA). Those areas or buildings protecting classified material and/or *Special Nuclear Material* (see def.) (SNM), Categories I, II, or III have additional requirements which are outlined in individual security plans available to personnel with a *need-to-know* (see def.).
- 1.2 The Laboratory Protection organization establishes protection requirements for special nuclear material (SNM), classified and sensitive material, government property, and personnel from theft and/or diversion sabotage, espionage, or other hostile acts. These requirements comply with the PLN-11000, "Site Safeguards and Security Plan" (SSSP), PLN-11002, "Site Security Plan" (SSP), U.S. Department of Energy (DOE) directives, DOE threat guidance, specific physical security plans, and laboratory policy.

2. SCOPE AND APPLICABILITY

- 2.1 This plan applies to all INL contractor employees, *subcontractors* (see def.), construction personnel, visitors, INL *foreign national* (see def.) employees, and academic personnel accessing or performing activities within a GAA or PPA. These general security requirements must be adhered to and communicated to all employees and subcontractors by their management/technical contacts.
- 2.2 Failure to conduct work in accordance with this plan constitutes a potential *security incident* (see def.) and may result in the issuance of *security infraction* (see def.), cancellation of approvals to perform work, prosecution for violation of federal law, and/or disciplinary action.

NOTE: *This plan does not apply to NRC-licensed facilities.*

3. SECURITY ADMINISTRATION

- 3.1 The Laboratory Protection Director and designated representatives will advise and counsel program and/or operations management regarding security measures necessary to meet DOE requirements and current threat guidance.
- 3.2 Managers will ensure their programs and personnel are in compliance with all applicable security requirements.
- 3.3 Program/Facility Managers will notify the appropriate Physical Security Officer (PSO) in advance of disruptions to security systems or equipment due to scheduled outages, maintenance, or construction.

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	Page: 20 of 36
	Revision: 7	
	Effective Date: 03/14/2016	

Form 412.09 (Rev. 10)

Idaho National Laboratory

INL GENERAL PHYSICAL SECURITY PLAN	Identifier: PLN-1466	Page: 4 of 20
	Revision: 15	
	Effective Date: 11/20/14	

3.4 Each building or program is assigned a PSO who ensures facility security interests are adequately protected in accordance with applicable DOE orders or guidance via approved security plans. The PSO functions as a primary point-of-contact for safeguards and security of the INL facilities.

4. PERSONNEL SECURITY

4.1 Employees and U.S. citizen subcontractor employees will be issued a badge reflecting their clearance level. The required clearance level will be determined by the employee’s manager or the organization requesting the subcontractor’s services, and the level of classified matter or SNM the individual is required to access.

5. SECURITY AWARENESS

5.1 All personnel/subcontractors working at the INL are required by DOE orders and guidance, to complete the initial and/or refresher security briefings prior to assuming their duties. Managers will ensure all personnel receive the following INL Security Briefings (see LWP-11106, “INL Security Awareness Briefings”).

- 0000Z415, Initial Security Briefing (included in the New Hire Orientation Training)
- 0000AN8, Annual Security Refresher Briefing for Uncleared Employees
- 0000AN5, Annual Security Refresher Briefing for Cleared Employees

6. ACCESS

6.1 General access onto INL Property Protection Areas (PPAs), which are non-security areas is controlled utilizing issued badges and passes for the protection of government interest and employees. All visitors and employees must have in their possession a valid badge or pass and a need to perform official government business before access is afforded (reference LWP-11301, “INL Access Control”) onto the INL.

6.2 A General Access Area (GAA) is an area established allowing access into designated areas having minimum-security requirements as prescribed by specific signage posted at the entrance into any GAA. GAA designated areas are accessible to all personnel including the public as described on the posted signage. Signage will list at a minimum the requirements described in 41 CFR Part 102-74 Subpart C, which at a minimum will include hours open to the public, prohibited activities, and prohibited articles.

6.3 GAAs existing in proximity to a PPA or other security area(s) must have defined barriers established to ensure separation between the GAA and any other security

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	Page: 21 of 36
	Revision: 7	
	Effective Date: 03/14/2016	

Form 412.09 (Rev. 10)

Idaho National Laboratory

INL GENERAL PHYSICAL SECURITY PLAN	Identifier: PLN-1466	Page: 5 of 20
	Revision: 15	
	Effective Date: 11/20/14	

area ensuring the public does not gain access to areas other than those defined as the GAA.

7. VISITOR ACCESS (U.S. Citizen)

7.1 All visits to INL facilities must be for *official business* (see def) purposes. Access requirements are outlined in LWP-11301.

NOTE 1: *The term visitor applies to those individuals who require access for less than 30 days. If access is required longer than 30 days the individual is not considered a visitor and must contact Personnel Security for further guidance. Continued renewal of a visit request and pass is generally not an accepted practice.*

NOTE 2: *Visitor request and visitor pass (see def.) is not required for person outside Research and Education (REC) buildings, i.e. lawn care, snow removal, etc.*

7.2 Visitor access is facilitated through submittal of Form 472.24, "Visitor Notification. These requests are submitted by their *host* (see def) prior to their arrival at the INL. At least 24 hours notification is preferable as same day submittal delays the overall approval process. The form is electronically submitted and routed to the affected area PSO for review and approval. Once the visitor notification form is approved the following occurs:

7.2.1 The Visitor Pass is issued by a Protective Force Officer, Personnel Security department representative, or other authorized individual at an authorized issuance location. Issuance locations are located at the Willow Creek Building (WCB), Materials and Fuels Complex (MFC), Gate 1 and when applicable, Special Manufacturing Capability (SMC) visitors only. All visitors, to include delivery drives accessing the INL must validate their identity using picture identification. The picture identification must be compliant with the REAL ID act.

7.2.2 State driver's license used to validate identification must be listed as compliant on the following web site, "<https://www.dhs.gov/secure-drivers-licenses>." One of the following may be used to validate identification if the visitors driver's license is not REAL ID compliant:

- U.S. Passport or U.S. Passport Card
- Military ID card or Military Dependent's ID card
- HSPD-12 credential or Common Access Card (CAC)
- Permanent Resident Card or Alien Registration Receipt Card (Form I-551)
- Foreign Passport that contains a temporary I-551 stamp or temporary I-551 printed notation on a machine-readable immigrant visa

Idaho National Laboratory

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	Page: 22 of 36
	Revision: 7	
	Effective Date: 03/14/2016	

Form 412.09 (Rev. 10)

Idaho National Laboratory

INL GENERAL PHYSICAL SECURITY PLAN	Identifier: PLN-1466	Page: 6 of 20
	Revision: 15	
	Effective Date: 11/20/14	

- Employment Authorization Document that contains a photograph (Form I-766)
- The above documents are the primary identification methods, in special cases the list on the Department of Homeland Security (DHS) Form I-9, "Employment Eligibility Verification" can be used to establish identity with management approval.

7.2.3 Visitors not having REAL ID compliant driver's license or one of the 6 alternative means of identification will be referred to the PSO for final access authorization disposition.

7.2.4 Visitors will not be allowed access under any circumstances if they do not have a REAL ID or acceptable alternate means of identification approved by the PSO.

7.2.5 Delivery drivers will not be allowed access under any circumstances if they do not have a REAL ID or acceptable alternate means of identification approved by the PSO. A delivery will not be made and the delivery driver will be sent away if a PSO and logistics representable cannot be located if the delivery driver does not have a REAL ID.

NOTE 1: *The requirement for a REAL ID applies to any occupant of a vehicle.*

NOTE 2: *Persons without a valid REAL ID cannot be escorted in lieu of not having the identification. Persons without a valid REAL ID will not be allowed access onto the INL.*

7.2.6 Hosts of visitors having DOE or other agency Homeland Security Presidential Directory -12 (HSPD-12) badges should submit a visitor notification (Form 472.24).

7.3 Visitors traveling to the site must be issued a visitor pass at an issuance location (WCB, MFC, and Gate 1) before proceeding to other facilities within the site boundaries. For example, visitors must be issued a visitor pass at WCB, MFC, or Gate 1 before proceeding to the Advanced Test Reactor-Complex (ATR-Complex) or Idaho Nuclear Technology and Engineering Center (INTEC).

7.4 All visitors are required to wear the HSPD-12 badge, INL-issued Local Site Specific Only (LSSO) badges, or INL visitor pass on their outer clothing between their neck and waistline at all times while within the INL boundaries, unless health or safety regulations prohibit, such as working in radiological areas or around certain machinery.

7.5 Visitors having HSPD-12 badges may be required to sign a visitor log when accessing designated PPA. Visitor's logs shall be used for accountability of personnel within an area, building, or room is required.

Idaho National Laboratory

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	Page: 23 of 36
	Revision: 7	
	Effective Date: 03/14/2016	

Form 412.09 (Rev. 10)

Idaho National Laboratory

INL GENERAL PHYSICAL SECURITY PLAN	Identifier: PLN-1466	Page: 7 of 20
	Revision: 15	
	Effective Date: 11/20/14	

- 7.6 Visitors with a visitor pass must complete and sign Form 473.01, "Visitor Traffic Log," upon initial entry and exit as required by the building or area. *Escort* (see def.) requirements for visitors are outlined in Paragraph 10.
- 7.7 Once visitor traffic logs are completed, program/building personnel shall ensure all fields are completed. The traffic logs are then inspected for accuracy by program/building personnel and sent to the affected individuals for review and approval.
- 7.8 INL personnel may request to see another person's identification badge or pass at any time within INL boundary. Any refusal or evasion to show the identification badge/pass may result in disciplinary action. In areas where keycard badges are used for access control, personnel must inspect the badge of any individual to which they grant access. This is commonly referred to as "piggybacking."
- 7.9 The visitor's host is responsible to:
- 7.10 Ensure visitors listed on the visit request follow all INL procedures during the visit, to include but not limited to, safety, security, emergency and work-related procedures.
- 7.11 Ensure visitors listed on the visit request complete required training prior to the visit.

NOTE: *Training questions should be addressed through your training coordinator or the Training Hotline at 526-1016 for assistance.*

- 7.11.1 Ensure visitors listed on the visit request who will be provided access to classified information has the appropriate access authorization/clearance level and a "need-to-know." Clearance status must be validated through the Personnel Security department. The visitor should present a valid DOE security badge indicating the appropriate access authorization level prior to access of any classified information. If necessary, the visitor can initiate verification/transfer of clearance through his/her respective personnel security office by submitting DOE F 5631.20, "Request for Visit or Access Approval" prior to the visit.

7.11.1.1 Using Generic Keycard Access:

- 7.11.1.1.1 Generic Keycard Access is available for REC TOWN facilities only and site locations with the approval of building the facility manager and responsible PSO.

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	Page: 24 of 36
	Revision: 7	
	Effective Date: 03/14/2016	

INL GENERAL PHYSICAL SECURITY PLAN	Identifier: PLN-1466	Page: 8 of 20
	Revision: 15	
	Effective Date: 11/20/14	

- 7.11.1.1.2 Additional training requirements may apply and it is the Host's responsibility to ensure all training requirements are accomplished.
- 7.11.1.1.3 Each host is responsible for the accountability of any issued keycard(s) by signing for the keycard(s), thereby attesting to the receipt of such controlled keycard access. Keycards shall be return at the point of origin i.e. WCB guard desk, at the end of the visit.
- 7.11.1.1.4 Normal keycard access will be valid for normal business hours (6:00 AM to 6:30 PM) Monday thru Friday. The facility PSO is required to approve requests for weekends and backshift hours based on warranted justification.

8. VISITOR ACCESS (Non - U.S. Citizen)

- 8.1 Non-U.S. citizen visitors must be approved in advance by the Foreign Visits and Assignments Office and will be issued a non-U.S. citizen badge or visitor pass. Foreign national security plans specify access controls and escort requirements (see LWP-11102, "Unclassified Foreign Visits and Assignments").

9. VISITORS ATTENDING SPECIAL EVENTS

- 9.1 This section is intended for pre-planned, INL sponsored and approved special events only; it is not to be used for casual or routine access for vendors, caterers or media.
- 9.2 Approved visitors participating in INL sanctioned special events are allowed access to defined INL facilities for the purpose of attending and/or participating in these events. These events are typically awards, recognition of services ceremonies, or other activities not considered "**official business**" but are recognized as a valuable tool to enhance employee and public relations. Every special event must be requested in collaboration with the responsible PSO.
- 9.3 Battelle Energy Alliance (BEA) Leadership Management Team (LMT) has directed specific areas/rooms within the Engineering Research Office Building (EROB), INL Research Center, (IRC), and Willow Creek Building (WCB) be made "Open to the Public" to include non-U.S. citizens for special events. These activities shall be escorted by appropriate BEA personnel.
- 9.4 Since these events do not share information or technologies; non-U.S. citizens will be allowed to attend without complying with the requirements of the

Idaho National Laboratory

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	Page: 25 of 36
	Revision: 7	
	Effective Date: 03/14/2016	

Form 412.09 (Rev. 10)

Idaho National Laboratory

INL GENERAL PHYSICAL SECURITY PLAN	Identifier: PLN-1466	Page: 9 of 20
	Revision: 15	
	Effective Date: 11/20/14	

“Unclassified Foreign Visits and Assignments Program” through the Foreign Visits and Assignments Office.

- 9.5 All visitors participating in the event must be badged with a special events pass (obtained from the PSO). All visitors must print their name and sign the appropriate traffic log.
- 9.6 Issuance of visitor passes and escorting requirements for approved special event is described in LWP-11301 or the physical security plan if written for the event. Refer to these documents as applicable for details and the process regarding access authorization and badging of visitors attending special events.
- 9.7 The PSO shall follow the requirements in LWP-11301 regarding access authorization.
- 9.8 If the threat condition is raised to SECON 2, High Condition (Orange), all non-U.S. Citizens visitors attending these events will be required to comply with requirements of the, “Unclassified Foreign Visits and Assignments Program” additional paperwork for access.

10. TOURS

- 10.1 Tours at the INL are organized and managed by the Communications and Government Affairs organization.
- 10.2 The Communications and Government Affairs shall not issue a tour pass to any person not having meeting the requirements of the REAL ID act (see paragraphs 7.2.1, 7.2.2 and 7.2.3).
- 10.3 Using a graded approach, a baseline tour escort ratio shall be established by the building area management and the PSO, and communicated to the tour Communications and Government Affairs office. This ratio is depending on the tour location, activity within the PPA that the tour is taking place, and the span of control required to maintain accountability and control of the tour group. The PSO and/or building management shall communicate necessary changes if activity or conditions warrant a change in the visitor to escort ratio to the Communications and Government Affairs office.
- 10.4 Tour members are issued a special numbered “Tour Pass” for the duration of the tour.

11. EMPLOYEE ACCESS

- 11.1 All INL personnel and visitors are required to wear DOE standard badge, INL-issued LSSO badges, or INL visitor pass on their outer clothing between their neck and waistline at all times while within the INL facilities or areas unless

Idaho National Laboratory

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	Page: 26 of 36
	Revision: 7	
	Effective Date: 03/14/2016	

Form 412.09 (Rev. 10)

Idaho National Laboratory

INL GENERAL PHYSICAL SECURITY PLAN	Identifier: PLN-1466	Page: 10 of 20
	Revision: 15	
	Effective Date: 11/20/14	

health or safety regulations prohibit, such as working radiological areas or around certain machinery.

- 11.2 Employees who arrive at a facility without an identification badge or pass are required to obtain a temporary “forgotten pass” denoting the proper access authorization. A forgotten pass may be obtained at any staffed guard post. Lost passes must immediately be reported to the Warning Communications Center (WCC) at 526-1515.

NOTE 1: *Employees will not be issued a generic keycard pass in place of a forgotten or lost pass at the Research and Education Campus (REC) facilities.*

NOTE 2: *Subcontractors may not control access into INL Facilities.*

- 11.3 Employees may not have personal services conducted in any INL facility or parking lot, such as oil changes or windshield repair, because of environmental, safety, and liability concerns.

NOTE: *Local Site Specific Only (LSSO) badges issued by other DOE Sites are not considered a DOE Standard Badge and shall not be recognized at the INL.*

12. ESCORT REQUIREMENTS

- 12.1 Hosts of visitors are responsible to ensure visitors are properly trained for unescorted access if needed, or that visitors are properly escorted by an authorized individual if the visitor’s training is not current. Escort requirements apply to visitors, INL employees, and subcontractors who do not have unescorted access. Security areas may have additional escort requirements outlined in the area-specific physical security plans or as directed by security area manager and PSO. The escort ratio is depending on location, activity within the PPA, and the span of control required maintaining accountability and control of the individual(s) involved.

13. INSPECTION PROCEDURES

- 13.1 Prior to, and as a condition of entry and exit, all packages, boxes, briefcases, and similar articles and containers carried by or in the possession of any individual entering the site are subject to inspection. Each inspection will include a thorough check of all compartments, sections, and any other parts of the article necessary to determine whether or not it contains prohibited items such as firearms, explosives, incendiary devices, or other items capable of causing personal injury or property damage. After passing a completed inspection and meeting all requirements, the individual will be allowed to enter the area with the package.

Idaho National Laboratory

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	Page: 27 of 36
	Revision: 7	
	Effective Date: 03/14/2016	

Form 412.09 (Rev. 10)

Idaho National Laboratory

INL GENERAL PHYSICAL SECURITY PLAN	Identifier: PLN-1466	Page: 11 of 20
	Revision: 15	
	Effective Date: 11/20/14	

- 13.2 It is the responsibility of all employees entering INL facilities to know and understand what constitutes a prohibited item and to ensure they are not introduced into INL building.
- 13.3 All vehicles entering fenced areas at the INL site must have government license plates, be placarded with the company name in 2" tall or greater letters, or otherwise approved by the responsible PSO.
- 13.4 LWP-11303, "Introducing Electronic Devices into Security Areas," provides guidance regarding introduction of controlled articles into the INL.
- 13.5 Prohibited article signs are posted at entrances of the INL.
- 13.6 Prohibited articles include weapons (e.g. hunting rifles, hunting knives, boot knives, switchblades or any knives longer than 8" when opened), alcohol, illegal drugs, and/or explosive devices. Accommodations for temporary storage of prohibited items are the responsibility of the individual and will not be provided within the boundaries of the INL.
- 13.7 Individuals attempting to access the INL through Gates 1, 3, and 4 may not temporarily leave items such as those in Paragraph 13.6 above on INL property; i.e. adjacent to these gates.
- 13.8 If a prohibited article is not declared by a vehicle driver or is not discovered at the INL entry gate (Gates 1, 3, 4), but is subsequently found at a building/area access control point, the vehicle and driver shall be immediately escorted off INL property.
- 13.9 Service animals will be afforded access with advance approval by the appropriate PSO. Families and/or visitors may be allowed access by following the requirements in LWP-11301 and this plan.
- 13.10 All individuals are subject to warrantless search while at the INL. Failure or refusal on the part of any person to comply with any search requirements will result in denial of access.
- 13.11 Failure to comply with a random inspection can result in confiscation of packages, removal from the INL, and reported to a PSO for further investigation. PSOs shall report any anomalies to access control requirements to the INL Incidents of Security Concern (IOSC) investigators. Employees who refuse a random inspection may receive disciplinary action up to and including termination. Non-employees may be barred from future visits to the INL.

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	Page: 28 of 36
	Revision: 7	
	Effective Date: 03/14/2016	

Form 412.09 (Rev. 10)

INL GENERAL PHYSICAL SECURITY PLAN	Identifier: PLN-1466	Page: 12 of 20
	Revision: 15	
	Effective Date: 11/20/14	

14. CAMERA AND RECORDING DEVICE USE POLICY

- 14.1 This policy addresses the increased need to utilize cameras, video recording devices, and audio recording devices in the performance of the laboratory’s day-to-day mission within property protection areas.
- 14.2 The term camera includes any type of device having the ability to take a moving or still picture or store the picture or video in any format.
- 14.3 All pictures and video leaving the INL must be reviewed and approved by an appropriate Derivative Classifier (DC), except as noted in section 13.9. Pictures or videos should be limited to digital format so that they can be easily reviewed before use or release. If however non-digital devices are used to take pictures, arrangements shall be made with the INL Video Photography organization to develop the camera or video film and ensure a subsequent review by a DC.
- 14.4 Camera or video devices operating within the boundaries of the laboratory property, either leased or owned, which are used for or have the potential to provide surveillance (inadvertent or otherwise) must be coordinated through and managed by the affected area PSO. In many cases, approval will be in the format of an approved physical security plan. Within the laboratory, it is prohibited to record activities of persons without their notification or consent. When there is a need for property or assets protection surveillance, provide a written request stating the dates and justification for the surveillance to the affected area PSO. The PSO will then route this request to the appropriate approval authorities.
 - 14.4.1 Cameras used for “Covert” (hidden) surveillance are NOT permitted on INL property without special permission from DOE. Cameras used for “Overt” (visible) surveillance of property and asset protection are permitted.
 - 14.4.2 Cameras must be installed for area surveillance and not for individual (personnel, visitors, etc.) surveillance.
 - 14.4.3 Covert recording of any conversation is strictly prohibited.
- 14.5 There is always a concern regarding the content of a picture(s) or video because they may contain classified information, controlled unclassified information such as Official Use Only (OUO), Personally Identifiable Information (PII), sensitive information, or information that would not reflect positively on laboratory operations. Because of this concern, the use of a camera, video recorder, or other picture taking device within the INL Property Protection Areas (PPAs) is discouraged unless it is for official government use.

Idaho National Laboratory

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	Page: 29 of 36
	Revision: 7	
	Effective Date: 03/14/2016	

Form 412.09 (Rev. 10)

Idaho National Laboratory

INL GENERAL PHYSICAL SECURITY PLAN	Identifier: PLN-1466	Page: 13 of 20
	Revision: 15	
	Effective Date: 11/20/14	

14.6 A Controlled Article Permit is not required when taking pictures or video within a PPA. However, if a picture or video is to be used outside the laboratory, a representative from the classification office must review the picture(s) or video.

14.7 If a camera or video equipment must be used within a security area, (limited area or higher) the controlled article permit process described in LWP-11303 must be followed.

14.8 Web or Internet Protocol (IP) cameras within personal work areas, which are not within a security area, do not require PSO approval. The requirements for these devices and their use within facilities are outlined in LWP-11303.

14.9 Media events hosted by the Communications and Public Affairs (C&PA) Department may be exempt from the requirement to have all pictures or videos reviewed if the following requirements are met:

14.9.1 The photographs or videos were taken in one of the following approved locations:

14.9.1.1 Research and Education Campus

- A. The main lobby area of the WCB, EROB, or IRC facilities
- B. In front of in-town office buildings
- C. Unclassified Conference Rooms
- D. Executive office areas
- E. Some other in-town areas may be allowed on a case-by-case basis depending upon the area and the activities that are taking place.

NOTE 1: *Approval of such requests shall be coordinated with the facility PSO in advance.*

NOTE 2: *Personnel and/or hosts are responsible for the effective protection of CUI.*

14.9.1.2 Central Facility Area (CFA) - area not within a fenced facility

- A. In front of site-wide complex buildings
- B. Unclassified Conference Rooms

Idaho National Laboratory

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	Page: 30 of 36
	Revision: 7	
	Effective Date: 03/14/2016	

Form 412.09 (Rev. 10)

Idaho National Laboratory

INL GENERAL PHYSICAL SECURITY PLAN	Identifier: PLN-1466	Page: 14 of 20
	Revision: 15	
	Effective Date: 11/20/14	

- C. Some additional CFA areas may be allowed on a case-by-case basis depending upon the area and the activities that are taking place.

NOTE: *Approval of such requests shall be coordinated with the building/area PSO in advance.*

- 14.9.1.3 Pictures or videos will not be taken within the Critical Infrastructure Test Range Complex (CITRC) and the National Security Test Range (NSTR) without the approval of the program manager, principal investigator, or PSO.

- 14.9.2 Fenced Areas (MFC, INTEC, ATR-Complex, Radioactive Waste Management Complex (RWMC) and SMC).

- 14.9.2.1 The only pre-approved areas for taking un-reviewed photographs are outside of the fence looking into the area. This should only be done after verifying with the area PSO that no sensitive security operations are underway that could be observed.

- 14.9.2.2 Other exterior building shots may be allowed inside the fenced area on a case-by-case basis depending upon the area and the activities that are taking place.

NOTE 1: *Approval of such requests shall be coordinated with the area PSO in advance.*

NOTE 2: *If the above requirements are not met, Media events are required to have all pictures or videos reviewed.*

- 14.9.3 A walk-down of the area to be utilized will be conducted by Communications and Government Affairs personnel and/or the facility PSO or Classification Office immediately prior to the event to ensure there is nothing in the area being used or in the background that should not be released to the general public. Conference rooms should also be inspected prior to the event to ensure no sensitive information has been left in the conference room by prior users.
- 14.9.4 Members of the Communications and Government Affairs staff will be in attendance at all times while photographs or videotaping is being conducted. They will ensure that no classified, controlled unclassified, company proprietary information, etc., is discussed or photographed. Members of the public relations staff must immediately contact the Office of Classification if they have any doubts about the material being considered for *public release* (see def.).

Idaho National Laboratory

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	Page: 31 of 36
	Revision: 7	
	Effective Date: 03/14/2016	

Form 412.09 (Rev. 10)

Idaho National Laboratory

INL GENERAL PHYSICAL SECURITY PLAN	Identifier: PLN-1466	Page: 15 of 20
	Revision: 15	
	Effective Date: 11/20/14	

15. SPECIAL NUCLEAR MATERIAL (SNM) STORAGE

- 15.1 Category IV quantities of SNM must be stored in a locked area within a PPA at a minimum. Nuclear Material Custodians (NMCs) are responsible for controlled access to Category IV SNM storage areas, and access must be restricted to authorized individuals. Protection requirements for Category I, II, & III SNM are described in the SSP, SSSP, or the applicable physical security plan.

NOTE: *Category IV SNM must be protected with Level III locks and keys or equivalent devices as approved by the area PSO.*

16. MOTORIZED GATE CONTROLLERS

- 16.1 Controls for motorized gates, used for vehicle entry control points, are protected using a graded approach. Protection requirements are described in detail within MCP-228, "Physical Security Protection."

17. POWER SUPPLY ELEMENTS

- 17.1 Power supply elements, located or operating within the confines of the INL, are protected from malicious physical attacks based upon a graded approach. Protection requirements are described in detail within MCP-228.

18. SECURITY KEYS

- 18.1 All installation of locks and the issuance of security keys to employees must be requested through the INL Request for Services and coordinated through the Area PSO. Guidelines and procedures for the use of security keys are outlined in LWP-11301.
- 18.2 Loss of a Level I or II security key requires replacement of all locks utilizing that series of key. A loss of a Level III key may require the replacement of all locks utilizing that series of key. Final determination is made by the PSO based on what the lock is protecting and how many keys have been previously lost. The organization of the key custodian who lost the key is responsible for the cost of installing new locks.
- 18.3 Replacement of lost Level IV keys or locks shall be replaced at the discretion of the PSO and Facility Managers.
- 18.4 Security locks and combinations must be changed immediately whenever they have, or are suspected of having been compromised.
- 18.5 When a Level I, II, or III key is no longer required, the key must be transferred or returned to the area PSO. Form 473.75, "Security Key or Lock Receipt," is completed by the PSO upon receipt, issuance, or transfer of keys.

Idaho National Laboratory

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002
	Revision: 7
	Effective Date: 03/14/2016 Page: 32 of 36

Form 412.09 (Rev. 10)

Idaho National Laboratory

INL GENERAL PHYSICAL SECURITY PLAN	Identifier: PLN-1466
	Revision: 15
	Effective Date: 11/20/14 Page: 16 of 20

- 18.6 Any employee who loses a security key must submit a lost key report Form 473.76, "Report of Lost or Stolen Security Key" to the area PSO as soon as possible.
- 18.7 All custodians of a security key are required to conduct an annual (for Level II and III) and semi-annual (Level I) physical inventory and resolve any discrepancies.
- 18.8 When a key custodian terminates employment or no longer requires their security/controlled key, the employee must contact the area PSO to arrange transfer or return of the key. Keys that are not controlled by Security must be returned to the employee's manager when they are no longer needed or when the employee terminates employment.
- 18.9 Managers are responsible to ensure that unoccupied facilities and buildings are locked whenever possible.
- 18.10 Managers shall ensure Level I, II, III & IV cores and locks are removed from facilities or buildings being vacated, put into cold storage, or being Decommissioned and Demolished, and said keys & cores are returned to the affected area PSO.

19. CONTROLLED UNCLASSIFIED INFORMATION

- 19.1 All controlled unclassified information, such as Unclassified Controlled Nuclear Information (UCNI), Official Use Only (OUO) information, Navy Nuclear Propulsion Information (NNPI), and Export Controlled Information (ECI) will be appropriately identified, marked, and protected in accordance with federal laws, regulations, orders, and company policy (see LWP-11202, "Controlled Unclassified Information Program").
- 19.2 Controlled unclassified information can be destroyed by shredding, boxing and sending it to the INL land fill per LWP-11204, "Destruction/Disposal of Controlled Unclassified Media.", or disposing in an approved CUI receptacle. Shredding must be a minimum of 1/4" strips. Any questions regarding destruction of controlled unclassified information can be directed to the INL *Operations Security* (see def) (OPSEC) Coordinator.
- 19.3 All computer systems, including those used to process or store controlled unclassified information must be appropriately identified and protected in accordance with LWP-1303, "Information Cyber Security Policy." The type of information processed on the computer, including sensitive information, must be identified on Form 565.06, "Hardware Registration." All computer systems should be configured to preclude uncontrolled, unauthorized access. Appropriate controls include requiring passwords for all users of the system, screen savers

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	Page: 33 of 36
	Revision: 7	
	Effective Date: 03/14/2016	

Form 412.09 (Rev. 10)

Idaho National Laboratory		
INL GENERAL PHYSICAL SECURITY PLAN	Identifier: PLN-1466	Page: 17 of 20
	Revision: 15	
	Effective Date: 11/20/14	

with passwords enabled, and not allowing the use of shared files or web pages unless explicitly approved.

20. CONSTRUCTION SECURITY PROCEDURES

- 20.1 Prior to disruptions of security systems due to scheduled outages, maintenance, or construction, project/program managers or Facility System Engineers will notify the area PSO.
- 20.2 Prior to initiating any changes in security arrangements or any alterations in security areas/equipment or configuration, project/program managers will coordinate with area PSO.
- 20.3 The responsible area PSO will participate in the review of conceptual, preliminary, and final design of construction projects as required by MCP-7001, "Management of Capital Asset Projects."

21. TRESPASSING SIGNS

- 21.1 Site Boundary Trespassing Signs
 - 21.1.1 The INL site boundary area is marked with trespassing signs along its boundary. These signs indicate access beyond these signs requires following normal INL access requirements as listed within this document. Detailed maintenance requirements are described in detail within MCP-228.
- 21.2 Facility Trespassing Signs
 - 21.2.1 Facility building and or barrier (fences) signs indicate access beyond that point requires individuals to follow normal INL access requirements as listed within this document. Detailed maintenance requirements are described in detail within MCP-228.

22. DEFINITIONS

Authorized individual - A person endorsed by the cognizant area manager to have unescorted access to that area, and empowered to perform their designated job duties in that area.

Controlled Unclassified Information (CUI) - Information for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security or governmental interests. National security interests are those unclassified matters that relate to the national defense or foreign relations of the U.S. Government. Governmental interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agriculture, technological, and law-enforcement

Idaho National Laboratory

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	Page: 34 of 36
	Revision: 7	
	Effective Date: 03/14/2016	

Form 412.09 (Rev. 10)

Idaho National Laboratory

INL GENERAL PHYSICAL SECURITY PLAN	Identifier: PLN-1466	Page: 18 of 20
	Revision: 15	
	Effective Date: 11/20/14	

information, as well as the privacy or confidentiality of personal or commercial proprietary information provided the U.S. Government by its citizens.

Escort - An authorized individual assigned the responsibility to accompany persons who lack a need-to-know, access authorization, appropriate training, or who have not been granted unescorted access by security.

Foreign National - Any person who is not a U.S. citizen or a U.S. national, including foreign corporations (i.e., a corporation not incorporated in the United States), international organizations, foreign governments, and any agency or subdivision of foreign governments (e.g., diplomatic missions).

General Access Area - A security area established allowing access into designated areas having minimum-security requirements as prescribed by specific signage posted at the entrance to the GAA. GAA designated areas are accessible to all personnel including the public as described on the posted signage.

Host - An authorized individual assigned the responsibility for the safety, security and welfare of the assigned visitor.

Infraction - Documentation of administrative and/or disciplinary actions assigned to an individual taken in response to an incident of security concern.

Need-to-Know - A determination made by a possessor of classified information SNM, or sensitive information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge of, or possession of the classified information SNM, in or CUI order to perform tasks or services essential to the fulfillment of an official United States Government program (DOE O 472.2, "Personnel Security").

Official Business - A non-INL individual reporting to the INL in an capacity of having INL work interactions with employees and/or management.

Operations Security (OPSEC) - A process designed to disrupt or defeat the ability of foreign intelligence or other adversaries to exploit sensitive Departmental activities or information and to prevent the inadvertent disclosure of such information.

Property Protection Area (PPA) - A facility where a special standard of protection must be applied. Such a facility may have: property of significant monetary value (> \$5,000,000); nuclear materials requiring safeguards controls or special accounting procedures; significance to DOE program continuity; national security consideration; or potential adverse impact upon the public health and safety.

Public Release - Release of material to the general public for widespread dissemination.

Idaho National Laboratory

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002	Page: 35 of 36
	Revision: 7	
	Effective Date: 03/14/2016	

Form 412.09 (Rev. 10)

Idaho National Laboratory

INL GENERAL PHYSICAL SECURITY PLAN	Identifier: PLN-1466	Page: 19 of 20
	Revision: 15	
	Effective Date: 11/20/14	

Security Incident - An adverse event that results in attempted, suspected, or actual compromise of classified information, or waste, fraud, abuse, loss, or damage of Government property.

Special Nuclear Material (SNM) - Plutonium, Uranium-233, Uranium enriched in the isotope 235, and any other material which, pursuant to Section 51 of the Atomic Energy Action of 1954, as amended, has been determined to be special nuclear material, but does not include source material; it also includes any material artificially enriched by any of the foregoing, not including source material.

Subcontractor - A supplier, distributor, vendor, or firm that furnishes supplies or services to or for a prime contractor or another subcontractor, who enters into a contract with a prime contractor.

Visitor Pass - Temporary identification issued to authorize visitors that is blue in color, has an INL logo at the bottom and has an embedded watermark of the INL log at the bottom of the pass to prevent copying.

23. REFERENCES

41 CFR Part 102-74 Subpart C

565.06, "Hardware Registration"

472.24, "Visitor Notification"

473.01, "Visitor Traffic Log"

473.75, "Security Key or Lock Receipt"

473.76, "Report of Lost or Stolen Security Key"

DOE O 472.2 "Personnel Security"

DOE F 5631.20, "Request for Visit or Access Approval"

LWP-11106, "INL Security Awareness Briefings"

LWP-11301, "INL Access Control"

LWP-11303, "Introducing Electronic Devices into Security Areas"

LWP-11102, "Unclassified Foreign Visits and Assignments"

LWP-11202, "Controlled Unclassified Information Program"

LWP-11204, "Destruction/Disposal of Controlled Unclassified Media"

Idaho National Laboratory

SAFEGUARDS AND SECURITY REQUIREMENTS	Identifier: RD-1002
	Revision: 7
	Effective Date: 03/14/2016 Page: 36 of 36

Form 412.09 (Rev. 10)

Idaho National Laboratory

INL GENERAL PHYSICAL SECURITY PLAN	Identifier: PLN-1466
	Revision: 15
	Effective Date: 11/20/14 Page: 20 of 20

LWP-1303, "Information Cyber Security Procedure"

MCP-7001, "Management of Capital Asset Projects"

MCP-228, "Physical Security Protection"

PLN-11000, "Site Safeguards and Security Plan"

PLN-11002, "Site Security Plan"

24. RECORDS

NOTE: *LWP-1202, "Records Management," the INL Records Schedule Matrix, and associated record types list(s) provide current information on the retention, quality assurance, and/or destruction moratorium requirements for these records Contact a Records Coordinator for assistance if needed.*