CRD M 470.4-2A, (Supplemented Rev. 0) Title: PHYSICAL PROTECTION

Applicable Contract (s): RCC X, OccMed X, PRC X, MSC X, Other TOC, ATL, JTS

Section A – Headquarters CRD: DOE M 470.4-2A, Attachment 1 (Hard copy attached)

Section B – General Clarifications:

All requirements contained in DOE M 470.4-2A, Physical Protection, Attachment 1, dated 7-23-09, apply to contractors who are responsible for operating and/or administering the Department of Energy (DOE) [including the National Nuclear Security Administration (NNSA)], Physical Protection Programs for protecting safeguards and security (SAS) interests. The requirements in DOE M 470.4-2A, Physical Protection, Attachment 1 must be assigned to all subcontractors who have responsibilities for operating, administering, and/or protecting DOE SAS interests.

Regardless of the performer of the work, the contractor is responsible for compliance with these requirements. All requirements contained in DOE M 470.4-2A, Physical Protection, Attachment 1 apply to Site/facility management contractors with responsibility for SAS interests at DOE and NNSA facilities. These requirements must be flowed down to all subcontractors with specific responsibilities for operating, administering, and/or protecting DOE SAS interests. For all other subcontracts, the contractor is responsible for flowing down these requirements to subcontracts at any tier to the extent necessary to ensure the contractor’s compliance with the requirements. In doing so, the contractor must not unnecessarily or imprudently flow down requirements to subcontracts. That is, the contractor will (1) ensure that it and its subcontractors comply with these requirements to the extent necessary to ensure the contractor’s compliance and (2) only incur costs that would be incurred by a prudent person in the conduct of competitive business.

A violation of the provisions of this directive to the safeguards or security of Restricted Data or other classified information may result in a civil penalty pursuant to subsection a. of section 234B, of the Atomic Energy Act of 1954 (42 U.S.C. 228b). The procedures for the assessment of civil penalties are set forth in Title 10, Code of Federal Regulations, Part 824, Procedural Rules for Assessment of Civil Penalties for Classified Information Security Violations, (10 CFR Part 824).

Section C – Specific Clarifications: None

Section D – General Supplemental Requirements:

The contractor shall comply with DOE M 470.4-2A, Physical Protection, Attachment 1. In addition, the provisions of this SCRD apply, to the extent required by law and/or contract and implemented by the Contracting Officer, to RL contractors and subcontractors located on and off the Hanford Site who possess government property as defined in this directive. In situations where there is discrepancy between requirements identified in DOE M 470.4-2A, Physical Protection, Attachment 1, or other DOE directives and Site specific requirements identified in this SCRD, the SCRD will take precedence.

DEFINITION OF TERMS

The following is a list of terms used throughout this document.

a. Accessible Inventory. Determined by a vulnerability/risk analysis committee using a baseline definition of the total inventory of radionuclides that is accessible to a potential saboteur.

b. Administrative Controls. The management procedures and constraints, operational procedures, accountability procedures, training, and supplemental controls established to provide an acceptable
level of protection for departmental assets (e.g., where daytime access is controlled by means other than locks, automated access control devices, receptionists or protective force personnel).

c. **Asset.** Information, material, facilities, property and people supporting DOE.

d. **Asset Owner.** The organization/person to which an asset is consigned for use/care.

e. **Asset Protection Agreement.** The document (Attachment 6.2) developed by the asset owner, as a result of the asset protection review, that reflects assets needing protection and how the assets are to be protected.

f. **Asset Protection Review.** A process, resulting in an Asset Protection Agreement, which identifies the assets, threat(s), minimum protection requirements, and strategic business impact(s), which result from loss of use of those assets, increased protection measures required to mitigate strategic business impact(s), documentation and approval requirements, and method for increased risk acceptance and approval. The asset owner or designee performs the asset protection review with assistance from his/her Security organization. When the asset is located offsite, threat guidance may be obtained from local intelligence and law enforcement agencies.

g. **Asset Protection Template.** Identifies assets and the DOE approved baseline protection methods (Attachment 6.1). The template incorporates the DOE minimum protection requirements.

h. **Controlled-Use Information.** Information on which regulations and/or controls are placed that limit availability, access, and/or dissemination. Includes Official Use Only (OUO), Unclassified Controlled Nuclear Information (UCNI), Export Controlled Information (ECI), Applied Technology (AT), and Naval Nuclear Propulsion Information (NNPI).

i. **Credible Sources.** Person/persons, police reports/investigation report(s) or similar sources with first hand or equivalent substantiated information regarding the behavior of an individual requiring access to the Hanford Site.

j. **Disqualifying Behavior.** Any threat of violence, violent or illegal behavior. See VI (b).

k. **Equipment.** For property management purposes, any item of government property having a unit acquisition cost of $5K or more and having the potential for maintaining its integrity (i.e., not expendable due to use) as an item.

l. **Facility.** An educational institution, manufacturing plant, laboratory, office building, or complex of buildings located on the same site that is operated and protected as one unit by the Department or its contractor(s).

m. **Government Property.** All land, buildings, structures (real property) and movable equipment and supplies that are owned, rented, or leased by the U.S. Government or contractors from commercial sources and subject to the administrative custody or jurisdiction of the Department.

n. **Hanford Site.** For the purpose of this SCRD, the Hanford Site encompasses all DOE and contractor facilities located on the Hanford Site, and offices in the Tri-Cities area housing DOE property, unless designated otherwise by contract.

o. **Public Access Area.** A specifically demarcated area in which business activities may occur between Hanford Site employees and certain segments of the general public without the constraints of a security area. A public access area shall be a building or portion of a building that does not contain or allow access to any controlled-use information, classified information, and/or SNM. Hanford Site Public Access Areas are equivalent to a General Access Area as described in DOE M 470.4-2A.

p. **Sensitive Property.** Those items, regardless of value, that require special control and accountability because of susceptibility to unusual rates of loss, theft, or misuse, or due to national security and export control considerations. Items include, but are not limited to, weapons, ammunition, explosives,
classified property, laptops, computers, personal digital assistants, other information technology equipment and removable components with memory capability that contain controlled-use information.

q. **Strategic Business Impact.** For the purpose of this SCRD, this term refers to the importance of an asset relative to the work being performed, as determined by the asset owner/sponsor. Assets shall be reviewed and a determination made as to what the business impact will be, should the asset not be available for use. Alternative ways of doing business may offset or reduce the impact of non-availability of the asset. Mitigating factors may include access to another asset to perform the work, a spare asset that could be put into use, or other alternatives. An asset may have low property value, which requires minimum protection, yet have a strategic business impact; in such a case, the asset owner/sponsor may want to increase protection above the minimum requirements. Costs for increased protection, above the minimum requirements, shall be the responsibility of the asset owner/sponsor.

r. **Visitor.** A person not employed on the Hanford Site who is granted access to the Hanford Site for discussions with RL and/or RL contractor employees on project-related matters, employment interviews, or authorized tours.

I. **CONTRACTOR SAFEGUARDS AND SECURITY OFFICES SHALL:**

a. Provide Safeguards and Security (SAS) guidance and direction to contractor programs for the protection of DOE interests at the Hanford Site.

b. Support the responsible contractor program or facility as required with SAS expertise for the planning, scheduling, oversight, and participation in security assessments as follows:

1. Establish team(s) to perform security assessments of credible threat targets based on the requirements of DOE O 470.3B, *Graded Security Protection (GSP) Policy (U)*, and DOE M 470.4-1 Change 1, *Safeguards and Security Program Planning and Management*.

2. Recommend security enhancements or mitigation options as required to the responsible program or facility.

3. Review and revalidate the Site threat levels and protection effectiveness at frequencies consistent with governing DOE Orders/Directives.

4. Coordinate with Emergency Preparedness and other Site organizations as requested to identify and assess quantities of hazardous materials at the Hanford Site.

II. **CONTRACTOR PROGRAM/PROJECT MANAGEMENT OFFICES SHALL:**

a. Provide oversight of activities within facilities.

b. Participate in hazards assessments for facilities requiring security assessments.

c. Participate with contractor SAS organizations in selecting the appropriate prevention and mitigation option(s) and facilitate implementation.

III. **CONTRACTORS AND SUBCONTRACTORS SHALL:**

a. Document, as part of the Hanford Site Safeguards and Security Plan (SSSP), or as part of their contractor/organizational security directives, as applicable, procedures for implementing an asset protection program and access control measures in accordance with the contents of this SCRD and appropriate DOE Orders/Directives.

b. Conduct hazard and vulnerability assessments as required. To ensure consistency in assessments, the Site Services and Infrastructure (SSI) contractor or its designated subcontractor will lead assessment team efforts with involvement of the contractor responsible for affected facilities.

c. Provide oversight of contractor asset protection programs and coordinate protection program planning.
with asset owners.

IV. ASSET OWNERS OR DESIGNATED SECURITY FOCAL POINTS SHALL:

a. Asset owners/designated security focal point(s) are responsible for coordinating all security concerns relative to the facility, organization, program or project with their Security organization. Additional responsibilities shall include:
   1. Posting required signs
   2. Managing facility lock and key and automated access control system programs in accordance with the responsible contractor security policies and procedures
   3. Ensuring all security requirements/procedures are met as outlined in their contractor security procedures
   4. Ensuring that all facility occupants and/or organization/project members are knowledgeable of their security responsibilities
   5. Maintaining necessary security reference materials as directed by the responsible contractor Security organization
   6. Providing adequate visitor control measures
   7. Ensuring adequate protection measures and access control procedures are implemented and maintained

V. LEVELS OF PROTECTION:

a. Protection levels shall be determined using a low, medium, and high protection designation strategy for each type asset. The asset owner shall determine, using the Asset Protection Agreement, which protection requirements to use for assets based on requirements listed in the Asset Protection Template (Attachment 6.1), applicable Orders/Directives/Contractor Requirements Documents, and technical advice from his/her Security organization. The asset owner, along with his/her contractor Security organization, shall also determine if more or less protection is required than specified in the template. In lieu of an Asset Protection Agreement, a facility security plan may be developed at the discretion of the responsible contractor Security organization. Security plans shall be developed in accordance with requirements identified in DOE M 470.4-1, Change 1, Safeguards and Security Program Planning and Management.

b. Low-Level Protection requirements apply to non-sensitive DOE information, capital property, precious metals (where the value does not exceed $100K), Category IV D/E SNM and Category IVE source and other nuclear material, and other assets identified through asset protection reviews as requiring special protection.

c. Medium-Level Protection requirements apply to information designated as controlled-use, precious metals valued at greater than $100K, firearms, Category IV B/C SNM and processes considered unique where the loss of information/material would have detrimental effects on the DOE Hanford Site mission.

   NOTE: Controlled-use information identified as OUO may be protected in accordance with low-level protection requirements upon approval of the responsible contractor Security organization.

d. High-Level Protection requirements apply to classified matter, classified information systems (IS), classified conference rooms, Category III SNM, and assets identified through asset protection reviews as requiring this level of protection. Measures identified for the protection of classified matter must implement the minimum requirements of DOE Orders/Directives.
VI. HANFORD SITE ACCESS ELIGIBILITY

a. GENERAL CONTENT

1. Access to the Hanford Site is based on support of a DOE contract or sub-contract, official business with RL and/or RL contractor(s)/subcontractor(s), and/or sponsorship by an RL contractor/subcontractor employee. Access to the Hanford Site requires compliance with all applicable DOE, DOE-RL, and DOE contractor/subcontractor policies and directives established for the security of employees and visitors, protection of all government and contractor/ subcontractor property, and protection of DOE SAS interests. Failure to uphold the security of personnel, property, or SAS interests may be cause for being denied access to the Hanford Site.

2. Access to the Hanford Site may be denied based on derogatory information received by DOE or a Hanford contractor/subcontractor. Access denial to the Hanford Site will be based on credible sources regarding disqualifying behavior that meets the criteria described in this SCRD.

3. Pre-employment checks will be completed to determine suitability for employment on DOE contracts for all employees issued a DOE Personal Identity Verification (PIV) security badge (i.e., USAccess Credential), or the Green Hanford Local Site Specific Only (LSSO) security badge. Results of pre-employment checks or similar checks conducted by a DOE contractor/subcontractor may be used to determine eligibility for access to the Hanford Site. Information from other credible sources about Hanford Site contractor/subcontractor employees or visitors may likewise be used to determine eligibility for access to the Hanford Site. The following elements are standards/areas that should be evaluated before allowing employment on DOE contracts:
   - Criminal background check
   - Personal reference checks
   - Credit history check
   - Employment verification/history check
   - Education verification
   - Driving report (if applicable/required)
   - Credit Check (only for positions governed under Washington State law, RCW 19.182.020)

   Individuals issued the black Hanford LSSO security badge follow the pre-employment standards and procedures set by their employers and/or any appropriate federal or state agencies or regulatory bodies. However, access to the Hanford Badge Request System (BRS) or the Personnel Security Clearance Records Plus (PSCR+) system will only be authorized for individuals having a security clearance or who have undergone a satisfactory PIV and/or a pre-employment background check as described above. In addition, only PIV and/or green badge holders are authorized to host/sponsor visitors and guests onto the Hanford Site.

4. The RL Manager has the final authority for determining access to the Hanford Site, and as such may approve, disapprove, suspend, or modify, any and all actions related to Site access. The RL Director of Security and Emergency Services (SES) is delegated the authority for determining Hanford Site access eligibility.

b. CRITERIA

The following behavior or incidents may be a basis for denying an individual Hanford Site access:

1. Violent behavior occurring on or off the Hanford Site, including but not limited to murder, attempted
murder, battery, rape, and robbery;
2. Communicating threats of harm to an individual in the workplace;
3. Conflicts with supervisors or other employees creating a fear or threat of harm;
4. Bringing a weapon to the workplace;
5. Intimidating, belligerent, harassing, bullying, or other aggressive behavior creating a threat or fear of harm in the workplace.

c. DETERMINATION PROCESS

1. MSA serves as the focal point for administering and managing the Hanford access denial program under the oversight of RL SES. The MSA will maintain the access denial database, enter and remove individuals from access denial in accordance with the below criteria, review and process requests and/or appeals relating to access denial and coordinate determination decisions with appropriate legal counsel and RL SES.

2. Upon receipt of potentially disqualifying information involving a Hanford site employee, the contractor will make a determination as to whether the individual should be denied site access. If, upon reviewing all relevant information, the contractor determines that site access denial is appropriate, it shall inform RL Security and Emergency Services (SES) in writing by email within 48 hours of receipt of potentially disqualifying information. Contractor should place MSA Security on copy coverage. Depending upon the circumstances, immediate suspension of access may be necessary. Contractor should contact MSA Security for immediate suspension if warranted. A follow up letter must be sent to SES, and must include the relevant facts and the rationale for site access denial.

3. SES will review the information and approve or disprove the Site access denial. SES will inform the contractor of its decision in writing within seven (7) calendar days of receipt of Site access denial request. SES should place MSA Security on copy coverage.

4. If SES concurs with the Site access denial, the contractor shall inform the individual of his or her Site access denial in writing. The notification will include the basis for the denial and information as to how the individual may request reinstatement after at least 180 days have passed. When describing the reinstatement process, the notification should include a list of the mitigating factors listed in the Review of Access Denial section, as well as examples of relevant documentation that should be submitted if the individual hopes to reverse the Site access denial decision. The notification must explain the appeal should be made to the Director of Security of the applicable contractor, and provide an address.

5. If a contractor receives a request for reinstatement, the contractor must review all relevant information and make a determination within 30 calendar days of receipt of the request. The contractor then must forward the request, information from any sources used in its determination and its written determination to SES for final review and approval.

6. Based on the contractor’s rationale and any additional information submitted by the individual, SES will make a final determination. SES will not conduct additional research or meet with the individual in making its decision, but it may consult with DOE Office of Chief Counsel. SES will inform the contractor of its binding decision in writing within 15 calendar days of receiving the request.

7. The contractor shall inform the individual of the determination in writing, including a copy of SES’s decision letter.
d. REVIEW OF ACCESS DENIAL

In the event that an individual requests review of his or her Site access denial, the following mitigating factors shall be considered by the contractor and SES:

1. Seriousness of behavior;
2. Recentness of behavior;
3. Whether the individual was pressured or coerced into committing the act and information demonstrating those pressures are no longer present in the person’s life;
4. Evidence that the individual did not commit the offense;
5. Evidence of successful rehabilitation, including but not limited to the passage of time without recurrence; remorse or restitution; job training or higher education; good employment record; constructive community involvement; or successful completion of counseling or rehabilitation, including anger management.

Special circumstances

- In the event that a contractor has reason to believe that an employee should be denied Site access based on behavior that is not listed in the Criteria section (VI.b.), the contractor may submit a request to SES. The request must include a detailed description of the relevant behavior and an explanation as to why it warrants access denial. If SES agrees, the individual will be placed on the Site access denial list and receive the same notification and opportunity to appeal provided in the Determination Process section (VI.c.).
- In the event that an individual has agreed not to enter the Hanford Site per a legal settlement or other agreement, such agreements should be documented and included in the Site access denial database (in redacted version if required per the agreement).
- Each contractor will conduct a review of its access denial list every two (2) years and remove individuals who are no longer a security or safety threat.

e. RECORDS OF SITE ACCESS ELIGIBILITY DETERMINATIONS

1. Data, including names and detailed explanation for access denial, shall be maintained by MSA and available for review by SES, other contractors, and others who have a need to know and who meet the requirements established by the Privacy Act.
2. An individual may request and attain his or her Site access denial information through a request under the Freedom of Information Act or Privacy Act.

VII. ACCESS CONTROL:

a. Access control includes the process of limiting access to information, facilities, resources, or designated security areas. Measures used to ensure an effective access control program may include: hardware and software features, physical controls (e.g., lock and key, receptionist, automated access control system), operating and administrative procedures (e.g., signs, employee challenge system), and various combinations of these.

b. Personnel with read/write access to the PSCR+ badging database must have an access authorization (security clearance) equal to or higher than the security clearances of those personnel contained in the database. Read/write access is defined as the ability to manipulate programming code or alter existing data fields which would allow a single person to issue, or cause to be issued, an undetected false credential allowing unauthorized access to Hanford limited areas (LAs) or protected areas (PAs).

c. Security badges shall be worn in all Hanford Site facilities, with the exception of public access areas,
**Contractor Requirements Document (CRD) (Supplemented) Form**

including those located in the Tri-Cities, WA.

d. Security badges shall be worn between the neck and the waist on the front of the body. Security badges shall be worn on the outermost garment, unless dictated otherwise by safety requirements.

e. Access control shall be provided according to the Asset Protection Template (Attachment 6.1). The number of frequently used entrances to a facility shall be limited. The host is responsible for assisting visitors requiring entry into a facility.

f. Automated access control systems, when used for access to LAs or higher level security areas, must, as a minimum, verify the following: valid USAccess Credential or DOE Standard badge (i.e., validity of the badge is matched between the badge identification number read by the system and valid personal identification number (PIN)).

g. If the asset owner, in conjunction with the responsible contractor Security organization, after completion of the asset protection review, determines that administrative controls are adequate for access control, the asset owner shall consider protection of certain assets by locking internal office doors, use of PC lockdown devices, storing assets in a storage container, etc. Facilities shall be locked at all times, unless pre-approved by asset owners in conjunction with the affected contractor Security organization, or in consideration of special operational requirements as documented in an approved Asset Protection Agreement. Additionally:

1. Specific facility check procedures shall be established (e.g., end of shift lock up).

2. A sign shall be installed at the main entrance indicating entry/access requirements and/or instructions. When access points and the perimeters of fenced areas are sufficiently posted with signs, individual facilities within the fenced areas do not require signs unless the access requirements for the facility are more restrictive than those for the area in which the facility is located, or additional signs are required by DOE Directives.

3. When administrative controls are used as an access control measure, certain types of low-level assets (Category IV D SNM, precious metals) shall be secured as required in applicable DOE Orders/Directives and/or as approved by RL SES.

4. All unoccupied facilities shall be locked.

5. Personnel issuing Site-wide access media, i.e., visitor and temporary security badges via the automated BRS, must have a security clearance or have undergone a satisfactory pre-employment background check meeting the specifications outlined in Section VI, paragraph a. 3.

h. If the responsible contractor Security organization, after completion of the asset protection review or as the result of performance testing, determines that administrative controls are not adequate or are not being effectively employed, physical access control systems shall be implemented (e.g., receptionist, lock and key, automated access control systems).

i. At property protection areas (PPAs) or LAs where access is controlled through the use of automated access control systems (e.g., OMNILOCK, proximity card, etc.), the personnel access practice of “vouching” or “piggybacking” is permitted. “Vouching” or “piggybacking” is the practice of allowing access to another individual through a controlled door to which you have access after visually verifying the security badge and, in the case of LAs, security clearance and authorization to enter of the individual being permitted access.

**VIII. VISITOR CONTROL:**

a. Visits to the Hanford Site are authorized under the following conditions:

1. Visit is compatible with mission or public relations activities.
2. Visit has an official relationship to programs conducted at Hanford.
3. Visit will create no interruption of work or significant risk to the visitor.

b. Visitors to Hanford Site facilities will be badged according to procedures developed by the responsible contractor Security organization with RL review and approval. Standard visitor badge procedures shall be consistent for all LAs and PPAs. In leased/private facilities (Tri-Cities, WA, etc.), a Building Specific badge (BSB) may be issued to a U.S. citizen visitor who arrives at the facility on official business, without processing through a badging office. Hosts of visitors shall:
   1. Determine the minimum host/visitor and security requirements.
   2. Know the work location of the visitor and the work being performed.
   3. Ensure the visitor is provided appropriate training on policies and procedures, including safety and security requirements and emergency preparedness information.
   4. Determine the need for escorted or unescorted access with due consideration of the visitors familiarity with the Hanford Site and visit destination.

c. Escorts shall be provided for visitors entering areas where they do not have authorization for unescorted access. Escorts shall maintain visual surveillance of escorted visitors at all times. A ratio of one (1) escort per five (5) visitors shall be maintained unless otherwise authorized by the responsible contractor Security organization due to special operational considerations.

d. Foreign National visitors require special approvals and escorting for access. Refer to DOE O 142.3, *Unclassified Foreign Visits and Assignments Program*, and the appropriate contractor security procedures for specific requirements.

e. Visitor logs are not required for PPAs.

f. Hanford employees may approve/authorize a Hanford security badge, including visitor and Site tour badges. Contractors may designate employees who can authorize security badges; however, the background investigation provisions referenced in Section VI, paragraph a. 3, apply.

**NOTE:** All Hanford Site tours will be approved and conducted in accordance with the SECON Hanford Site Tour and Visit Approval Matrix (Attachment 6.3).

For all tours/visits that do not directly support the mission of the Hanford Site, contractors will complete a *Visit/Tour Approval Request* form, RL-698 (Attachment 6.4), and submit the form to the RL SES Tour Security POC for information. This form is *not required* for tours/visits that are in direct support of the DOE or contractor's mission at the Hanford Site.

g. Visitors (from the general public sector) to public access areas are not required to wear/possess a security badge, nor be escorted. In addition, visitors must be informed of any special instructions pertaining to security areas located adjacent to/within the public access area.

h. Visits for other than official purposes (e.g., social functions), shall be made in accordance with contractor policies and procedures and approved by the cognizant contractor Security organization, and RL SES. Security badges shall be worn by visitors except children age five (5) and under.

**IX. PHYSICAL PROTECTION OF FACILITIES:**

a. DOE and Government contractor operations are conducted in government, leased, and private facilities;

b. A graded approach to protection application shall be used in developing protection strategies; consider: the function performed, type of information/material stored; value, attractiveness, and portability of property in the facility; local threat; resources available for response/assessment; and cost of protection
application. The safety of employees and the public and strategic business impact associated with loss of assets are key factors in development of a protection strategy.

c. To arrive at an asset protection strategy, the asset owner, in conjunction with his/her Security organization, shall perform an asset protection review using Attachments 6.1 and 6.2 or equivalent format. The review, as documented in the Asset Protection Agreement, shall identify threat(s) to the asset, asset value, any unacceptable risks involved with the protection strategy, concurrence of the appropriate Security organization, and signature of the person responsible for the asset protection strategy (asset owner).

d. When determining the physical security requirements of assets, the following shall be considered:
   1. Value of the asset(s)
   2. Portability
   3. Attractiveness
   4. The applicable/credible threat (against the assets located in the area)
   5. A review of any property losses and/or adverse security trends associated with the assets

e. The completed Asset Protection Agreement, Attachment 6.2, shall be used as the approved security plan for Hanford Site facilities meeting the asset protection requirements. For those facilities which do not meet the minimum protection requirements identified in the Asset Protection Template (Attachment 6.1), the Asset Protection Agreement must be approved by RL SES with the concurrence of the appropriate RL Program Office.

f. A single Asset Protection Agreement may be established for asset owners who co-locate within a multi-contractor or multi-organization occupied facility. The Asset Protection Agreement must be negotiated, concurred in, and approved by all the appropriate contractor asset owners and Security organization points of contact. Additionally, multiple facilities performing similar functions may be incorporated into a single Asset Protection Agreement.

g. The designated security focal point/asset owner shall ensure the minimum physical security requirements are met for each facility/asset. Minimum requirements will be established per the Asset Protection Template (Attachment 6.1) and applicable DOE Orders/Directives. Generic requirements for all levels of physical protection in security areas follow:
   1. Signs shall be posted as follows:
      i. Around the perimeter and at the main entrances to each facility or security area, as stated in the Asset Protection Agreement, which prohibit trespassing, list prohibited articles, and advise personnel that vehicles and hand carried items are subject to search.
      ii. At government-owned facilities, the standard DOE “Atomic Energy Act, No Trespassing” sign will be used.
      iii. At government-leased facilities, contractor Security organizations shall consult with their Office of Legal Counsel for the posting of locally developed “No Trespassing” signs. These signs will contain language that complies with the required DOE wording.
      iv. At the Hanford Site and security area perimeters, "No Trespassing" signs shall be placed at all gates and access points and along fence lines at 500-foot intervals where terrain does not present a visual obstruction. Where terrain is a problem, signs should be posted at shorter distances and in locations which provide the best visibility.
Contractor Requirements Document (CRD)  
(Supplemented) Form

v. “No Trespassing” signs should be posted as close to eye level as possible, but not less than four (4) or more than six (6) feet above ground level.

vi. When access points and the perimeter of fenced areas are sufficiently posted with signs, then facilities within the area do not require signs unless the access requirements are more restrictive than the area itself.

vii. The Hanford Site perimeter, to include the Columbia River shoreline, will be posted with the standard DOE "Atomic Energy Act, No Trespassing" sign. The bank of the river shall be posted above the high water mark, which is considered the Site boundary, from the old Hanford power lines, south to Horn Rapids Road. The river shoreline is considered the Site boundary north of the power lines to the Vernita Bridge.

e. Warning signs and/or notices must be posted at entrances to areas under electronic surveillance advising that physical protection surveillance equipment is in use.

2. Unoccupied/abandoned facilities shall be locked at all times with limited distribution of building keys.

3. Security area boundary doors (i.e., exterior doors) shall be constructed in compliance with criteria established in applicable DOE Orders/Directives.

4. Locking devices must meet the requirements outlined in the Asset Protection Template (Attachment 6.1). Although locking hardware (i.e., bolts, latches, and strike plates) are not specified, the hardware used must be substantial enough to show signs of forced entry.

i. The use of locking hardware that would allow for the undetected manipulation ("jimmying") of the bolt is unacceptable.

ii. Locking devices and/or hardware from which the retaining screws can be removed from outside the security area without detection will not be used.

5. Door hinges must be substantial enough to show signs of forced entry.

6. Windows must be lockable from inside the facility. Locking hardware for windows must be substantial enough to show signs of forced entry.

h. Personnel in possession of a USAccess Credential, DOE Standard, Hanford Site Specific, or Temporary security badge are authorized to transport government property, excluding prohibited and controlled articles.

i. All personnel are responsible for ensuring adequate protection is provided for government property assigned for use in the performance of job duties.

j. All personnel are responsible for ensuring only properly badged, authorized individuals are present and permitted access to work locations (e.g., employee challenge).

k. All personnel are responsible for ensuring facilities are properly secured in accordance with asset protection requirements.

l. Facilities or areas within a facility designated a “Public Access Area” shall meet the following criteria:

NOTE: Public access areas are not authorized north of the WYE Barricade (exception: RL approved Manhattan Project B Reactor Tour Program).

1. At close of business or as indicated in an approved Asset Protection Agreement, the access control afforded to public access areas will, as a minimum, be the same as required for low-level assets as described in the Asset Protection Template (Attachment 6.1).
2. During normal business hours, entry points used for access shall be kept to a minimum.

3. The area should be generally used by non-Hanford personnel and/or the work or service provided by the facility must pertain to the public (e.g., OccMed Facilities, Volpentest HAMMER Law Enforcement & Security Training Center/Hanford Patrol Training Academy, etc.).

4. Public access areas may not contain any equipment, processes or material, the loss of which would cause unacceptable impact to the DOE, the contractor, national security or health and safety of the public.

5. Controlled-use information, equipment to reproduce controlled-use information, classified security interests, or SNM may not be used or stored within public access areas.

6. Signs shall be posted that clearly demarcate the public access area.

7. Signs shall be posted advising visitors of any special instructions pertaining to security areas located adjacent to/within a public access area.

8. Security areas (to include PPAs) adjacent to public access areas must have the appropriate measures in place that preclude unauthorized access.

9. Electronic communications equipment that can access controlled-use information, (e.g., Hanford Local Area Network) shall not be available to visitors.

10. Visitors to public access areas do not require an escort.

11. Security badges are not required within public access areas.

12. A detailed description of public access areas and application of the above criteria must be included within the Asset Protection Agreement.

X. LOCK AND KEY CONTROL

a. A lock and key program must be established to ensure control and protection of SNM, government property, and classified matter. There is no requirement to install door locks on interior offices requiring only low-level security protection; however, at the discretion of facility managers and/or asset owners, in conjunction with the responsible contractor Security organization, interior locks may be installed. If interior locks are installed, a system for issuance, accountability, and key control shall be maintained and shall be based on a graded approach.

b. Security keys and locks are divided into four (4) levels, Levels I through IV (Attachment 6.5). Based on site analysis, line management must determine the appropriate key and lock level for application to the site.

Level I

1. Level I security locks and keys must be used in the protection of Category I quantities of SNM, Category II quantities of SNM that credibly roll-up to a Category I quantity, and Top Secret and/or Secret classified matter (Attachment 6.5). Security key blanks must be restricted/proprietary; specifically, the blank must be unique to the site (e.g., does not use a commercially-available master key blank). Security locations such as vaults, vault-type rooms, material access areas, SCIFs, and exclusion areas where there is direct access to Top Secret and/or Secret documents require Level I security locks and keys. All unassigned Level I security keys and uninstalled cores must be under direct control of an authorized person or stored in a GSA-approved security container (repository) or vault-type room.

2. Level I security locks and keys, once put in service inside a PA or LA, excluding those issued to protective force personnel, must not leave the PA or LA without authorization by the responsible contractor Security organization. Assembled Level I security locks (excluding X-07, X-08, X-09
combination locks) or uninstalled cores and Level I security keys must remain under the direct control of an authorized person or must be stored in a GSA-approved security container or a vault-type room when not in use for the protection of the above assets (e.g., locksmith service work).

3. Level I security locks or keys reported missing or discovered missing or in any way tampered with must be reported as an Incident of Security Concern. These types of security incidents must be reported as an Impact Measurement Index (IMI) 3.4 event as identified in DOE M 470.4-1, Change 1, Safeguards and Security Program Planning and Management. Immediate notification must be made to RL SES and compensatory measures must be immediately initiated. If the key cannot be located within 24 hours, the affected lock(s) must be changed.

4. Any installation, replacement, or maintenance activities associated with Level I security locks must be documented to include the name of the person who performed the activity.

5. The number of Level I security keys must be kept to an operational minimum.

6. All parts of broken Level I security keys must be recovered. If the functional part of the key (the blade) is lost or not retrievable, it must be considered a lost/missing key.

7. Obsolete, damaged, or inoperative Level I security keys must be destroyed and such destruction recorded. Keys must be destroyed in a manner authorized by the responsible contractor Security organization.

8. Fabrication, issuance and return of Level I security keys must be documented.

9. Compensatory measures must be initiated whenever a Level I lock is missing (e.g., padlock) or malfunctions (e.g., X-07, X-08, X-09 combination lock), or a Level I security key is lost or stolen.

**Level II**

10. Level II security locks and keys are typically used for building doors, entry control points, gates in PA fences, exclusion area doors or other barriers or containers protecting Category II and Category III SNM (does not apply to hold-up or sludge) as well as providing direct access to classified matter, at the Confidential level. All unassigned Level II security keys and uninstalled cores must be under direct control of an authorized person or stored in a GSA-approved security container or vault-type room. Incidents involving Level II security keys must be reported as an IMI-3.4 event as identified in DOE M 470.4-1, Safeguards and Security Program Planning and Management. Immediate notification must be made to RL SES and compensatory measures must be immediately initiated. If the key cannot be located within 24 hours, the affected lock(s) must be changed.

11. The number of Level II security keys must be kept to an operational minimum.

12. Level II security keys, excluding those issued to protective force and fire department personnel, once put into service must not leave the facility without authorization by the responsible contractor Security organization.

13. All parts of broken Level II security keys must be recovered. If the functional part of the key (the blade) is lost or not retrievable, it must be considered a lost/missing key.

14. Obsolete, damaged, or inoperative Level II security keys must be destroyed and such destruction recorded. Keys must be destroyed in a manner authorized by the responsible contractor Security organization.

15. Fabrication, issuance and return of Level II security keys must be documented.

**Level III**

16. Level III security locks and keys are typically on limited area doors, weapons/ammunition storage facilities, gates in LA boundary fences, and buildings/storage areas for the protection of government
property. Level III security locks and keys must be used for the inside doors of buildings or office areas
where Section A, Chapter II, paragraph 2, Classified Matter in Use, of DOE M 470.4-4A, Information Security, is applicable. Incidents involving Level III security keys must be reported as
an IMI-4.15 event as identified in DOE M 470.4-1, Safeguards and Security Program Planning and Management. Immediate notification must be made to RL SES and compensatory measures must
be immediately initiated. If the key cannot be located within 24 hours, the affected lock(s) must be changed.

NOTE: Keys to buildings/storage areas used for the protection of government property may be
designated as Level III or Level IV at the discretion of the responsible contractor Security organization.

17. All parts of broken Level III security keys must be recovered. If the functional part of the key (the blade) is lost or not retrievable, it must be reported to the responsible contractor Security organization.

18. Obsolete, damaged, or inoperative Level III security keys must be destroyed and such destruction recorded. Keys must be destroyed in a manner authorized by the responsible contractor Security organization.

19. Fabrication, issuance and return of Level III security keys must be documented.

20. Site specific procedures must be developed for control and accountability of Level III security keys and be approved by the responsible contractor Security organization.

Level IV

21. Level IV locks and keys are typically used for offices where there is no open storage of classified matter and no classified matter in use. Desk, office, and vehicle keys are considered administrative and have no control and accountability requirements.

c. Inventories must be conducted to ensure an accurate and up-to-date accountability of level I, II, and III security keys, key rings, and uninstallation pinned cores. Keys must be categorized according to the asset being protected and an inventory and accountability system must be implemented.


e. Security locks on security containers, vaults, and vault-type rooms used for the protection of high value assets (e.g., classified matter, weapons and ammunition, Category I and II SNM) placed into service after 7-14-94 must have a lock that meets Federal Specification FF-L-2740A, “Locks, Combination,” or a lock or access control system approved by RL-SES.

f. If a combination lock fails on any General Services Administration-(GSA-)approved security container or vault door, it must be repaired or replaced with a lock that meets Federal Specification FF-L-2740A, “Locks, Combination,” before being used to protect classified matter or Categories I and II SNM. These failures must be documented on Form 89, Maintenance Record for Security Containers/Vault Doors, and filed for future reference to assist in resolving the problem prior to future procurement of combination locks (i.e., failed in the open or closed position and the reason for the failure).


h. Security key padlocks must meet the following specifications:

Contractor Requirements Document (CRD)  
(Supplemented) Form

- Lock bars must be 1 ¼ inches (31.75mm) by 3/16 inch (4.76mm), or equivalent, in cross section and constructed of material hardened to Rockwell C59 to C63 standards.

- Hasps and yokes on repositories containing classified matter must be constructed of material hardened to Rockwell C59 to C63 standards; be at least ¼ inch (6.35mm) in diameter or equivalent cross section; a

i. Panic hardware or emergency exit mechanisms used on emergency doors located in security areas must be operable only from inside the perimeter and must meet all applicable Life Safety Codes.

j. Keys, restricted keyway blanks, and key cutting codes must be protected in a graded fashion. Consideration must be given to the safeguards and security interest being protected, the identified threat, existing barriers, and other protection measures afforded to the asset.

k. Security keys include mechanical keys, proximity cards, and access codes. Security keys do not include administrative or privacy lock keys to factory installed file cabinet locks, desk locks, toolboxes, etc. Access codes must be protected from compromise.

l. Security key stock must be stored in a manner to prevent loss, theft, or unauthorized use. Personnel responsible for the control and issuance of locking systems and/or security keys must maintain an access authorization (security clearance) commensurate with that required for access to the asset(s) to which the key(s) provides direct access.

m. The organization responsible for the pinning and cutting of Levels I, II, and III security locks and keys must report to the responsible contractor Security organization.

n. The pinning and cutting of Levels I, II, and III security locks and keys must be done within a Limited Area or have equivalent type protection measures.

o. Level I, II or III Grand Master, master, sub-master, and control keys must be considered and analyzed in the vulnerability assessment process of the Site Safeguards and Security Plan (SSSP) or Site Security Plan (SSP).

p. An inventory system must be implemented to ensure the accountability of Levels I, II, and III security keys, and key rings. Each accountable key and key core must have a unique identifying number placed on it. Key cores with a unique identifying number will replace key cores without numbers as they are removed from service. Key cores will only be prepinned for the number required to fulfill the identified need. An inventory of prepinned cores will not be maintained for convenience.

1. Fabrication, issuance, return, and destruction of Levels I, II, and III security keys must be documented. Grand master security keys must be kept to an operational minimum and under strict control. Duplicate and replacement keys must not have the same key number assigned as the key being replaced or duplicated. The inventory record must identify the specific duplicate and replacement keys. If replaced, the disposition of the key being replaced must be identified.

2. Inventories must include keys in possession of key holders, issuance stock, keys assigned to key rings/key cabinets and accountable key cores with unique identifying numbers. Key rings must have a unique identifying number placed on the ring. Key rings should be of the tamper indicating type. Individual locks, keyways and pinned cores without unique identifying numbers are not required to be inventoried. The inventory system must:
   - document each person issued a Level I security key and the individual who issued the key;
   - document the location of the keys;
   - support the 100 percent inventory of Level I security keys that must be performed on a semi-annual basis by the responsible organization; and,
Contractor Requirements Document (CRD)  
(Supplemented) Form

- provide support in inventorying of Level I security keys not assigned to an individual (e.g., key rings, key cabinets, and keys issued on a temporary basis) that must be performed daily.

q. An annual inventory must be conducted to account for all Level II and III keys.

r. Contractors should implement a training plan for key custodians and anyone having responsibility for a security key to ensure they understand their responsibilities for security key control and accountability.

s. Contractors must have documented plans for key turn-in when personnel or programs are terminating or moving from one program to another.

XI. PROHIBITED AND CONTROLLED ARTICLES:

a. The following prohibited articles are not permitted to be introduced onto the Hanford Site or in Site-associated facilities without the specific authorization of the RL Director, Security and Emergency Services Division:

1. **Weapon**: Any firearm, dagger, sword, knife, or other cutting or stabbing instrument, club, or any weapon capable of producing bodily harm in a manner, under circumstances, and at a time/place that shows intent to intimidate another or warrants an alarm for the safety of other persons. Dangerous weapons include, but are not limited to: knives with blades that are automatically released by a spring mechanism, or that opens/falls/ejects by gravity, or by outward, downward, or centrifugal thrust or movement; Knives, folding or straight blade, with a blade exceeding four (4) inches in length (to include swords, machetes, hatchets, axes, razors and similar cutting devices); sling shot; bow and arrows/cross bows; blow guns; metal knuckles; nun-chu-ka sticks; throwing stars; and air guns (RCW 9.41.250).

2. **Ammunition**: As associated with small arms, ammunition is the assembled cartridge, including primer, powder, case and projectile.

3. **Explosives**: Materials that either detonate or explode.

4. **Incendiary devices**: Any material, substance, device, or combination thereof, which is capable of supplying the initial ignition or fuel for a fire/explosive and is designed for willful destruction.

5. **Controlled substances**: Drugs whose availability is restricted; any one of a number of drugs or other substances that are strictly regulated or outlawed because of their potential for abuse or addiction. Such drugs include those classified as narcotics, stimulants, depressants, hallucinogens, and cannabis. (NOTE: Prescription medication in appropriate or dispensed containers, or controlled substances obtained and used legally under appropriate Federal/State licensing for work related purposes (e.g., research) are not prohibited. These include a drug or other substance or immediate precursor included in Schedules I-V of USC 802(6) Part B).

6. **Drug paraphernalia**: All equipment, products, and materials of any kind that are used or designed for use in introducing a controlled substance into the human body (not including prescription drugs).

7. **Alcoholic beverages**: Any intoxicating beverage or liquor containing alcohol, including "near" or "non-alcoholic" beers and wines and some energy drinks. (NOTE: Alcoholic beverages are not prohibited if used at officially sanctioned events in accordance with contractor policies and procedures in locations designated as public access areas.)

8. The following exceptions apply:
   
i. Knives with a blade exceeding four (4) inches in length in possession of employees that are recognized as a tool designed for use in the performance of contract work are not prohibited.
   
ii. Knives readily recognized as kitchen cutlery (i.e., carving knives, steak knives, etc.) are not
## Contractor Requirements Document (CRD)  
### (Supplemented) Form

<table>
<thead>
<tr>
<th>Contracted Requirements Document (CRD)</th>
</tr>
</thead>
</table>

- prohibited. However, such knives found in locations inconsistent with their use, (e.g., vehicle glove box), with blades exceeding four (4) inches, are prohibited.

- The following controlled articles, in addition to the above listed prohibited articles, are not permitted in LAs, PAs, Material Access Areas (MAAs) or Exclusion Areas (EAs) without the specific authorization of the contractor Director, Safeguards and Security or their designee.

1. Recording equipment (audio, video, optical, or data).
2. Portable electronic equipment with a data exchange port capable of being connected to devices (e.g., laptop computers, Palm Pilots, MP3 players, iPods, etc.).

**NOTE:** Portable electronic devices are prohibited in rooms where classified computer systems are located, or where classified discussions are held. Such items can not be authorized into such areas.

3. Cellular telephones.
4. Radio frequency transmitting equipment.
5. Other items prohibited by law.

- Authorization to possess controlled articles in LAs, PAs, MAAs or EAs requires that:
  1. The equipment is government owned or leased.
  2. Possession of the item is “mission essential”.
  3. A documented risk analysis has been performed, identifying vulnerabilities inherent to the characteristics and operation of the device along with defined countermeasures.
  4. Authorization for use of controlled articles in one security area does not apply to all other security areas.

- In addition to the items above, personal protective sprays (e.g., mace, pepper spray, etc.), are not permitted in PAs.

### XII. HANFORD SITE TOURS

All Hanford Site tours will be approved and conducted in accordance with the SECON Hanford Site Tour and Visit Approval Matrix (Attachment 6.3).

For all tours/visits that do not directly support the mission of the Hanford Site, contractors will complete a Visit/Tour Approval Request form, RL-698 (Attachment 6.4), and submit the form to the RL SES Tour Security POC for information. This form is not required for tours/visits that are in direct support of the DOE or contractor's mission at the Hanford Site; for such tours/visits contractors are referred to Section VIII of this SCRD for visitor control requirements.

### XIII. DEVIATIONS:

Any deviations to the medium and high security requirements as outlined in this SCRD must be documented and submitted to RL SES through the appropriate Program Office, in accordance with DOE M 470.4-1, Change 1, Safeguards and Security Program Planning and Management.

### XIV. RADIOLOGICAL/TOXICOLOGICAL SABOTAGE PROTECTION METHODOLOGY:

- The purpose of the radiological/toxicological sabotage protection program is to identify any sabotage threats that meet the Security Protection Level 2 (SPL-2) criteria as defined in DOE O 470.3B, *Graded Security Protection (GSP) Policy (U)*

- If any SPL-2 threats are identified, the responsible contractor Security organization will determine if a
Contractor Requirements Document (CRD)  
(Supplemented) Form

security assessment is required in accordance with DOE M 470.4-1 Change 1, Safeguards and Security Program Planning and Management.

c. The results of sabotage analyses shall be documented in the SSSP.

XV. PROTECTION OF CLASSIFIED MATTER:

a. Facilities/rooms containing classified matter (including classified IS and classified conference rooms), shall be designated as LAs. Requirements for designating a building/room as an LA include:

1. Building materials shall be resistant to penetration and/or substantial enough that forced entry would be evident.

2. When transparent glazing material is used, visual access to the classified matter shall be prevented by the use of drapes, blinds, or other means.

3. Insert-type panels (if used) shall be such that they cannot be removed from outside the area being protected without showing visual evidence of tampering.

4. Walls that constitute exterior barriers of LAs shall extend from the floor to the structural ceiling. If this requirement cannot be cost effectively complied with a deviation shall be submitted with equivalent protection measures employed (e.g., materials stored in GSA approved security container equipped with a Mas Hamilton X-07, X-08, or X-09 combination lock meeting Federal Specification FF-L-2740A, "Locks, Combinations," random protective force inspections of LAs and the security containers contained therein).

b. When classified matter is used outside an LA, comparable security protection shall be provided to the material (i.e., a properly cleared and authorized individual will control the material to assure it is protected from individuals not cleared and/or not having a need to know). Classified matter shall not be stored outside a LA and may not be used or stored in areas approved for foreign national access.

c. Personnel using DOE classified matter have sole responsibility for its protection while in their possession or while the material is transported within the Hanford Site; the responsible person must maintain control, prevent unauthorized access, and properly store the material upon arrival at the destination. Appropriate courier/transport procedures established through the responsible contractor Security organization in accordance with DOE requirements must be met.

d. Whenever a security container is removed from service or transferred from one organization to another, the organization deactivating/transferring the container shall ensure that the combination is changed to the manufacturer's combination (50-25-50). All drawers/cabinets shall be thoroughly inspected to ensure all classified matter has been removed prior to changing the combination. The custodial organization must certify to their Security organization in writing that all classified matter has been removed before deactivation/transfer. Certification must include the security container's make and property tag number (or other unique identifying numbers or markings), the custodian's name and organization, and the following statement as appropriate:

1. Transfer of a security container: "All classified matter has been removed from this (these) security container(s) prior to transfer from my (transferring) organization to (receiving) organization."

2. Deactivation of a security container: "All classified matter has been removed from this (these) security container(s) prior to deactivation."

e. Security containers procured after the date of this SCRD shall be equipped with Mas Hamilton X-07, X-08, or X-09 locks meeting Federal Specification FF-L-2740A. Whenever a combination lock on a security container used for the protection of classified matter fails, it shall be replaced with a lock that meets Federal Specification FF-L-2740A before the container is returned to service.

f. Each contractor/organization authorized to store classified matter shall maintain the combination(s) to
the security container(s) in a consolidated location other than in the container in which the classified matter is stored. The combination to the consolidated security container shall be stored in a different security container.

g. Before reinstating a security container previously removed from classified service, it shall be inspected by a qualified Hanford Site locksmith, i.e., verify operation of Mas Hamilton X-07, X-08, or X-09 lock and that all drawers are functioning properly.

XVI. PROTECTION OF CATEGORY III AND IV SNM:

a. Category III SNM shall be stored within a LA and secured within a locked security container or locked room. The container or locked room containing the matter shall be under alarm protection or protective force patrols at intervals not exceeding eight (8) hours.

1. A standard/generic security plan for the movement of Category III quantities of SNM within the Hanford Site shall be developed by the owning organization. The security plan shall be reviewed by the responsible contractor Security organization and approved by RL SES.

2. Shipments of Category III SNM off the Hanford Site shall be made in accordance with requirements established in DOE M 470.4-6, Change 1, Nuclear Material Control and Accountability.

b. Category IV SNM shall be stored within a locked area when not in use.

c. Category IV SNM shall be received, processed and stored according to procedures reviewed by the responsible contractor Security organization.

d. A single individual can issue a security badge required for access to Category III and IV SNM and classified matter in approved storage as issuance of this badge does not allow direct access into a vault, vault-type room, locked room or locked security container containing the asset.

NOTE: Measures must be taken to ensure that a single individual cannot issue a security badge allowing unauthorized access into an area containing Category I or II SNM or classified matter; area being defined as a specific vault, vault-type room, or material access area (MAA) containing Category I or II SNM, or an exclusion area (EA) where mere access provides access to classified matter.

Section E – Specific Supplemental Requirements: None
## Contractor Requirements Document (CRD) (Supplemented) Form

### Attachment 6.1

#### Asset Protection Template

<table>
<thead>
<tr>
<th>Information</th>
<th>Level</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
<td>- Industrial grade standard pin-tumbler lock and key, automated access control device, receptionist/individual, administrative controls, or a combination of these. (Tagged property not contained within a facility or container shall be located within a lockable fenced area commensurate with its value as determined by the contractor asset owner.)</td>
</tr>
<tr>
<td></td>
<td>Med</td>
<td>Medium:</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>- Pick resistant lock (UL 437) and key, automated access control device, receptionist/individual, or combination of these.</td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td>- Asset will be in approved security containers as directed by appropriate DOE Orders/Directives or individual organizational security requirements.</td>
</tr>
<tr>
<td></td>
<td>Med</td>
<td>- Pick resistant locks on all exterior boundary doors with strict key accountability and control.</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>- In those instances where direct hands on access to the asset can be gained, then the area shall be secured with a pick resistant lock, except when attended by a responsible individual who is in a physical position to preclude unauthorized access to the asset. At the organization’s discretion, manufacturer controlled locksets, or GSA three-position changeable combination lock, approved automated access control device or combination of these, may be used.</td>
</tr>
<tr>
<td></td>
<td>Med</td>
<td>High:</td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td>Low-Level Protection requirements apply to non-sensitive DOE information, moveable capital property, precious metals where the value does not exceed $100K, Category IV D/E SNM and Category IVE source and other nuclear material, and other assets identified by an asset protection review.</td>
</tr>
<tr>
<td></td>
<td>Med</td>
<td>Medium-Level Protection requirements apply to information designated as controlled-use, capital property, precious metals valued at greater than $100K, firearms, Category IV B/C SNM, unique processes, other assets identified by an asset protection review.</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>High-Level Protection requirements apply to classified matter, classified AIS, classified conference rooms, Category III SNM, automatic firearms, and assets identified through asset protection reviews as requiring this level of protection.</td>
</tr>
<tr>
<td></td>
<td>Appropriate to Level of Asset</td>
<td>NOTE: Controlled-use information identified as OUO may be protected in accordance with low-level protection requirements upon approval of the responsible contractor Security organization.</td>
</tr>
<tr>
<td></td>
<td>Appropriate to Level of Asset</td>
<td>NOTE: If the asset is such that more stringent protection requirements are mandated by other DOE Orders/Directives, then the more stringent requirement shall apply.</td>
</tr>
</tbody>
</table>

*Level of protection as determined by vulnerability/risk assessment.  
^ Level of protection as mandated by WAC 296-52-445, Safety Standards for the Possession and Handling of Explosives
## Asset Protection Agreement

### Asset Characterization

1. Facility identification (building number, address, area - attach map if needed).

2. Is this facility a (mark appropriate block)?
   - Building
   - Room
   - Suite
   - Floor
   - Other

3. Facility is used for:
   - Office
   - Shop
   - Storage
   - Production
   - Training
   - Laboratory
   - Other

4. Is there a public access area(s) in this facility?  
   - Yes
   - No

5. Has a facility "focal point" been established?  
   - Yes
   - No
   (Name, phone no.: )

6. Have facility entrances been reduced to the lowest number consistent with its mission?  
   - Yes
   - No

7. Average number of personnel assigned to facility: 

8. What type of access control is used?
   - Door locks. Hours in use: 
   - Receptionist(s). Location(s): 
   - Specify what hours in use: 
   - Automated access control system. Type(s): 
   - Specify what hours in use: 
   - Administrative controls. Describe: 

9. Is an intrusion detection system (IDS) used?  
   - Yes
   - No

   a. Does the IDS have emergency power?  
      - Yes
      - No

   b. Is lighting adequate to support the IDS?  
      - Yes
      - No

10. Does this facility fall under OPSEC requirements?  
    (DOES IT CONTAIN CLASSIFIED OR SENSITIVE UNCLASSIFIED INFORMATION?)  
    - Yes
    - No

   If so, date of OPSEC Assessment (OA) or OPSEC Review (OR): 

11. Are required signs posted? Signs will be posted for all DOE-designated security areas.  
    - Yes
    - No

   (Mark appropriate block[s] denoting required sign[s]):
   - No Trespassing
   - Limited Area
   - Inspection (search)
   - Prohibited Articles
   - Instructional
   - Video Surveillance
   - Other
12. What is the protection category of the facility (using the Asset Protection Template)?
   Indicate the asset(s) requiring protection.
   - LOW LEVEL
   - MEDIUM LEVEL
   - HIGH LEVEL
     - Portable/sensitive property (cumulative value of <$1M depreciated value)
     - Precious metals (cumulative value of <$100K)
     - Category IV D/E special nuclear material/other nuclear materials (stored)
     - Controlled substances
     - Explosives
     - Sensitive unclassified DOE/proprietary/applied technology information
     - Portable property (depreciated value of >$500K per single item)
     - Precious metals (cumulative value of >$100K)
     - Firearms (handguns, rifles, dart guns, etc.)
     - Category IV B/C special nuclear material/other nuclear materials
     - Unique processes (relating to information/materials)
     - Special asset(s)/risk(s) identified (describe):

   - Classified matter
   - Classified automated information system(s) (AIS)
   - Classified conference room(s)
   - Category III special nuclear material (SNM)
   - Automatic firearms in storage
   - Special asset(s)/risk(s) identified (describe):

   - Other ____________________________

13. As determined by the asset owner(s) and the organizational security representative, is/are the asset(s) susceptible to:
   - Theft □ Yes □ No
   - Diversion of information □ Yes □ No
   - Radiological/toxicological sabotage □ Yes □ No

14. Are GSA-approved storage repositories used to protect the asset(s)?
   - Yes □ No

   If yes, location(s): ____________________________

15. Is there a facility security key accountability system?
   - Yes □ No

REQUIREMENTS FROM ASSET PROTECTION TEMPLATE

16. Does existing security protection meet minimum requirements?
   - Yes □ No

(Refer to Asset Protection Template)

(NOTE: If does not meet minimum requirements, approval is required from the responsible RL Program Office and the RL Safeguards and Security Division.)
Contractor Requirements Document (CRD)
(Supplemented) Form

ASSET PROTECTION AGREEMENT (Continued)

COMMENTS: (describe the facility, its use, and a description of the protection strategy):

SIGNATURES:

Asset Owner(s): ____________________________ Date
______________________________
Date
______________________________
Date
______________________________
Date

Security Representative: ________________________ Date

RL Program Office concurrence is required if protection DOES NOT meet minimum requirements

______________________________ Date

RL Safeguards and Security approval is required if the protection DOES NOT meet minimum requirements

______________________________ Date

OFFICIAL USE ONLY

23 of 26
11/2010
# Contractor Requirements Document (CRD)
## (Supplemented) Form
### Attachment 6.3
#### SECON - Hanford Site Tour and Visit Approval Matrix

<table>
<thead>
<tr>
<th>SECON Level</th>
<th>Homeland Security Level</th>
<th>Visit/Tour Requirement</th>
<th>Camera Use</th>
</tr>
</thead>
</table>
| 5           | GREEN                   | - The RL SES Tour Security POC shall be informed of tours and visits that do not directly support the mission of the Hanford Site by the submittal of the Visit/Tour Approval Request form, RL-698; this form is not required for tours/visits that are in direct support of the DOE or contractor's mission at Hanford.  
- Tours or visits of facilities considered sensitive due to the nature of the materials or work performed in the facility may be restricted on a case-by-case basis. | - Cameras and video equipment are normally permitted except for sensitive facilities.  
- Photographs of the Hanford Patrol security force or any other site protection measures are strictly prohibited unless prior approval has been received from the RL SES Tour Security POC. |
| 4           | BLUE                    | - The RL SES Tour Security POC shall be informed of tours and visits that do not directly support the mission of the Hanford Site by the submittal of the Visit/Tour Approval Request form, RL-698; this form is not required for tours/visits that are in direct support of the DOE or contractor's mission at Hanford.  
- Tours or visits of facilities considered sensitive due to the nature of the materials or work performed in the facility may be restricted on a case-by-case basis. | - Cameras and video equipment are normally permitted except for sensitive facilities.  
- Photographs of the Hanford Patrol security force or any other site protection measures are strictly prohibited unless prior approval has been received from the RL SES Tour Security POC. |
| 3           | YELLOW                  | - The RL SES Tour Security POC shall be informed of tours and visits that do not directly support the mission of the Hanford Site by the submittal of the Visit/Tour Approval Request form, RL-698; this form is not required for tours/visits that are in direct support of the DOE or contractor's mission at Hanford.  
- Initiation and planning for the formal public tour program shall be coordinated with the RL SES Tour Security POC.  
- Visits or tours by family members are not authorized under SECON 3. | - Approval of the use of cameras, video recorders, or other means of capturing pictures or images will be on a case-by-case basis and limited to significant events such as news conferences or major media events.  
- Special security precautions may be necessary if camera use is authorized by the RL SES Tour Security POC. |
| 2           | ORANGE                  | - The RL SES Tour Security POC shall review and approve tour and visit requests on a case-by-case basis.  
- Hanford tour and visit activity shall be restricted and limited to only special circumstance events. Special circumstances include Congressional tours or visits, tours or visits by other Federal Agencies directly involved in DOE work, or high-level governmental officials from state and local government.  
- Visits or tours by family members are not authorized under SECON 2. | - Approval of the use of cameras, video recorders, or other means of capturing pictures or images will be on a case-by-case basis and limited to critically significant events.  
- Special security precautions may be necessary if camera use is authorized by the RL SES Tour Security POC. |
<p>| 1           | RED                     | - Tours and visits will not be authorized. | - N/A |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tour Requestor’s Name and Phone</td>
<td></td>
</tr>
<tr>
<td>Visitor’s Name(s)/Group’s Identity</td>
<td></td>
</tr>
<tr>
<td>Affiliation (company/title)</td>
<td></td>
</tr>
<tr>
<td>Date(s) of Visit/Tour</td>
<td></td>
</tr>
<tr>
<td>Facilities to be Visited</td>
<td></td>
</tr>
<tr>
<td>Escort(s)</td>
<td></td>
</tr>
<tr>
<td>DOE/DOE Contractor Sponsor(s)</td>
<td></td>
</tr>
<tr>
<td>Sponsor Phone No.</td>
<td></td>
</tr>
<tr>
<td>Are camera and/or other recording device use requested?</td>
<td>No</td>
</tr>
<tr>
<td>Justification/Benefit</td>
<td></td>
</tr>
<tr>
<td>Security Review:</td>
<td>Concur</td>
</tr>
<tr>
<td>Non-concur</td>
<td></td>
</tr>
<tr>
<td>Name:</td>
<td></td>
</tr>
<tr>
<td>Date:</td>
<td></td>
</tr>
<tr>
<td>Security Review Comments (optional except for non-concurrence):</td>
<td></td>
</tr>
<tr>
<td>Counterintelligence Review: (if necessary)</td>
<td>Concur</td>
</tr>
<tr>
<td>Non-concur</td>
<td></td>
</tr>
<tr>
<td>Name:</td>
<td></td>
</tr>
<tr>
<td>Date:</td>
<td></td>
</tr>
<tr>
<td>Counterintelligence Comments (optional except for non-concurrence):</td>
<td></td>
</tr>
<tr>
<td>Management Review: (if necessary)</td>
<td>Concur</td>
</tr>
<tr>
<td>Non-concur</td>
<td></td>
</tr>
<tr>
<td>Name:</td>
<td></td>
</tr>
<tr>
<td>Date:</td>
<td></td>
</tr>
<tr>
<td>Management Comments:</td>
<td></td>
</tr>
</tbody>
</table>

25 of 26
### Level I Security Keys:
Keys providing direct access to the following assets or locations are defined as Level I keys. In addition to assets/locations identified through an asset protection review, other keys may be designated as Level I at the direction of the responsible contractor Security organization.
- Category I SNM
- Category II SNM (with credible rollup to Category I)
- Vaults
- Vault-type rooms containing Category I and II SNM or classified matter
- Material Access Areas
- Sensitive Compartmented Information Facility
- Open storage of classified matter
- Top Secret classified matter
- Secret (SRD/NSI) classified matter

### Level II Security Keys:
Keys providing direct access to the following assets or locations are defined as Level II keys. In addition to assets/locations identified through an asset protection review, other keys may be designated as Level II at the direction of the responsible contractor Security organization.
- Protected Area entry control points
- Protected Area fence gates
- Exclusion areas
- Barriers protecting Category II and discrete items of Category III SNM
- Containers protecting Category II and discrete items of Category III SNM
- Confidential (CNSI) classified matter

### Level III Security Keys:
Keys providing direct access to the following assets or locations are defined as Level III keys. In addition to assets/locations identified through an asset protection review, other keys may be designated as Level III at the direction of the responsible contractor Security organization.
- Limited Areas (where no open storage is present)
- Limited Area fence gates
- Firearms/Ammunition/Explosives storage
- Controlled substances
- Category III SNM (non-discrete items, e.g., holdup)
- Category IV B/C SNM
- Unique Processes
- Category I, II and III SNM storage cabinets and transfer wagons
- Safeguards and Security equipment

### Level IV Security Keys:
Keys providing direct access to the following assets or locations are defined as Level IV keys. In addition to assets/locations identified through an asset protection review, other keys may be designated as Level IV at the direction of the responsible contractor Security organization.
- Property Protection Areas
- Controlled-Use information
- Category IV D/E SNM and Category IV E source and other nuclear material

### Non-Security Keys:
Keys providing direct access to the following assets or locations are designated as “non-security keys.” These keys are used for administrative purposes.
- Factory cabinet keys
- Desk keys
- Vehicle keys
- Tool Box keys