Title: Safeguards and Security Program Planning and Management

Applicable Contractor(s): PHMC X RCC X OMSP X Other MSC, PRC

Section A – Headquarters CRD:
DOE M 470.4-1, Change 1, SAFEGUARDS AND SECURITY PROGRAM PLANNING AND MANAGEMENT, Attachment 2

Section B – Clarifications

General Clarifications:
1. Security Conditions, Part 1, Section B, Item #3 - Contractors shall review the measures defined in this section and provide the RL Director, SES, pre-planned protective measures. Updates shall be provided to the SES Director as protective measures change.

2. Incidents of Security Concern, Part 2, Section N, Chapter I, 3.i.(3) - Monthly Incident Compilations: Each contractor will provide to the RL SES Incident of Security Concerns Coordinator, no later than the 4th day of each month a compilation of IMI-4 incidents by month. These monthly summaries, which will contain the number of open and closed security incidents by IMI-4 subtopic, the total initiated for the calendar month, and a running total of open and closed incidents for the calendar year. If no reportable incidents occurred during the calendar month, a summary stating this is required. Reports may be accomplished informally via electronic mail.

3. Incidents of Security Concern, Part 2, Section N, Chapter, 7 - Inquiry/Incident Report Form (Exhibit G): To ensure consistent reporting at the Hanford Site, the attached inquiry report form is to be completed and submitted to DOE-RL Security and Emergency Services Division. All entries require completion to ensure each issue has been addressed. Where an entry is not applicable or the information is unknown, the field should be annotated as such (i.e. N/A or Unknown).

Specific Clarifications:
1. OMSP and RCC - Section C, is not applicable to these contracts.

2. FHI – Security Conditions, Part 1, Section B, Item #3.e.
   a. Measure 2 is clarified as follows:
      - Ensure that security personnel have access to building floor plans and emergency/evacuation plans for all site facilities.
      - Ensure that security personnel are able to seal off “target areas” immediately.
      - Ensure that key personnel required to implement security plans are on-call and readily available.
      - Maintain the site Emergency Management Team (EMT) on recall. Recall time shall be determined by the Director, RL-SES, on a case-by-case basis (i.e., graded approach).
      - Expand Operations Security measures.
      - Exercise bomb threat procedures.
   b. Measure 3 is clarified as follows:
      Secure buildings not in regular use. Maintain a list of all facilities.
   c. Measure 12. is clarified as follows:
      Maintain EMT personnel on recall; periodically exercise recall to ensure readiness. Recall time
shall be determined by the Director, RL-SES, on a case-by-case basis (i.e., graded approach). Keep all other personnel involved in implementing special response/contingency plans on call. Identify, contact, and brief specialists that may be required for unique contingencies; coordinate lines of communication.

d. Measure 14 is clarified as follows:

Move automobiles and objects, such as trash containers, newspaper boxes, crates, etc., at least 30 yards from buildings of a sensitive or prestigious nature. Identify any areas where an improvised explosive device could be hidden (i.e., pallet stacks, trash piles, stacked construction supplies, etc.). If the configuration of the facility or area precludes implementation of this measure, take appropriate compensatory measures per local plans [frequent inspection by explosive trained K-9 teams, if available, controlled access to parking areas, etc.]. Consider centralized parking.

e. Measure 15 is clarified as follows:

Secure buildings not in regular use.

f. Measure 17 is clarified as follows:

Implement screening procedures at mail distribution locations to identify possible explosive or incendiary devices or other dangerous material. If available, have K-9 teams inspect suspicious items and screen mail periodically. Provide guidance concerning suspicious packages. Encourage employees to inspect their individual mail, report suspicious items to security, and refrain from handling such items until cleared by appropriate authority.

g. Measure 18 is clarified as follows:

Implement screening procedures for other deliveries at designated inspection points to identify explosives and incendiary devices. Use K-9 teams for inspections, when available. Instruct site personnel to report suspicious packages to security and refrain from handling them until cleared by appropriate authority.

h. Measure 19 is clarified as follows:

Increase security force patrols of locally designated soft targets to improve deterrence and build confidence among site personnel.

i. Measure 22 is clarified as follows:

Randomly verify the identity of personnel entering property protection areas and other sensitive activities specified in local plans (i.e., inspect identification badges and grant access based on visual recognition). Use of automated access control systems at interior security areas is acceptable and encouraged where practical.

On a random basis, visually inspect the interior of vehicles and the exterior of suitcases, briefcases, packages, and other containers. Increase the frequency of detailed vehicle inspections (trunk, undercarriage, glove boxes, etc.) and the frequency of detailed inspections of suitcases, briefcases, and other containers.

j. Measure 25 is clarified as follows:

Provide duress alarm capability to critical/sensitive personnel identified by RL and Contractor management. Implement additional measures if warranted by the threat and existing vulnerabilities (e.g., personnel should alter established patterns of behavior when traveling in public areas).

k. Measure 28 is clarified as follows:

Participate in local emergency planning activities to determine if operational activities near the area
Contractor Requirements Document
(Supplemented) Form

might create emergencies that could affect the site/facility (e.g., airports, railroads, etc.).

l. Measure 33 is clarified as follows:
Randomly verify the identity of personnel entering the site/facilities, including facilities located in the Tri-Cities, WA, under DOE control. Inspect security badges for tampering. On a random basis, visually inspect the interior of all vehicles and the exterior of all suitcases, briefcases, packages, and other containers. Increase the frequency of detailed vehicle inspections (trunk, undercarriage, glove boxes, etc.) and the frequency of detailed inspections of suitcases, briefcases, and other containers.

m. Measure 38 is clarified as follows:
Erect barricades to control direction of traffic flow at critical/sensitive facilities. Erect barriers at facilities vulnerable to bomb attack as identified through the vulnerability analysis process.

n. Measure 46 is clarified as follows:
Increase inspections of vehicles entering the site. Inspections should include cargo storage areas, undercarriage, glove boxes, and other areas where explosives, incendiary, chemical or biological devices, or other dangerous items could be concealed.

o. Measure 48 is clarified as follows:
Increase inspections of baggage, such as suitcases, packages, and briefcases, brought on the site for the presence of explosives, incendiary, or other dangerous items.

Section C – Supplemental Requirements

I. FACILITY CLEARANCES AND REGISTRATION OF SAFEGUARDS AND SECURITY ACTIVITIES. The following general requirements are added to those of Part 2, Section I, of the HQ-CRD.

1. REGISTRATION. When the scope of a contract will require DOE access authorizations, the prime contractor shall query the Safeguards and Security Information Management System (SSIMS) to determine if the contractor is registered and possesses a DOE facility clearance.

   a. If a facility is registered in the SSIMS, the level of facility clearance shall be compared with the level required for the pending RL-related contract/sub-contract.

      (1) If the level of security clearance on the SSIMS is equal to or greater than that required for the RL-related contract/sub-contract, the prime contractor shall request a copy of the latest FDAR and complete the Contract Security Classification Specification (CSCS) Form DOE-F-470.1 and submit the completed form to the RL Facility Clearance Operations Manager (FCOM). (Note: The CSCS form is available on Hanford Site Forms.)

      (2) If the level of security clearance on the SSIMS is less than that required for the RL-related contract/sub-contract, the facility must be upgraded to meet local needs. In this case, the prime contractor shall complete the CSCS form and DOE-F-470.2, Facility Data and Approval Record (FDAR), and submit the completed form to the RL FCOM. (Note: The FDAR form is available in the Hanford Site Forms.)

   b. If the facility is not registered on the SSIMS, the prime contractor shall contact the Central Verification Activity, Defense Security Service (CVA) to determine if the facility is registered with the Department of Defense (DoD).

      (1) If the facility is registered with the DoD at a level equal to or greater than that required for the RL-related contract/sub-contract, the prime contractor shall complete the CSCS and FDAR
Contractor Requirements Document
(Supplemented) Form

forms and submit them to the RL FCOM. (Note: The DoD facility registration information shall be entered in Blocks 23a, f and g of the FDAR form.)

(2) If the level of the DoD security clearance is less than that required for the RL-related contract/sub-contract, the facility must be upgraded to meet local needs. Therefore, the prime contractor shall complete the CSCS and FDAR forms per the instructions, and submit them to the RL FCOM.

c. If the facility is not registered in SSIMS or with CVA,, the prime contractor shall request a FOCI submittal through the DOE Online Submittal system and forward to DOE-RL for determination. The contractor will request written confirmation (e/mail or facsimile) of the facility clearance information. The prime contractor will then complete the required CSCS and FDAR forms.

d. Upon approval of a CSCS and/or an FDAR, the prime contractor shall enter the data in the SSIMS as soon as possible but no later than ten (10) working days after receipt of the CSCS/FDAR form from the FCOM. Immediately after SSIMS data entry, the CSCS and/or FDAR form(s) shall be signed or initialed and dated, as appropriate, and the original copy returned to the RL FCOM.

2. CHANGES IN REGISTRATION DATA

a. The prime contractor shall submit to the RL FCOM a revised CSCS and/or FDAR form, as appropriate, for change in facility registration data (e.g., extension of contract, change in location of performance, change in address, change of key security personnel).

b. The prime contractor shall enter the revised facility registration information into the SSIMS as soon as possible but no later than ten (10) working days of receipt of the approved CSCS/FDAR form(s) from the FCOM.

3. TERMINATION OF REGISTRATION

a. Upon completion of an RL-related contract/sub-contract involving DOE access authorizations, the prime contractor shall complete a CSCS form, an FDAR form (when RL is the Lead Responsible Office (LRO)) and a Certificate of Non-Possession (Exhibit A) supplied by SES.

b. The prime contractor security organization shall verify, by signing the Security Certification that all DOE classified matter has been properly disposed of (provide a Certificate of Non-Possession signed by Contractor’s FSO) and all DOE security badges have been returned and all DOE access authorizations have been terminated, as appropriate. The Certificate of Non-Possession will be completed and signed prior to or on the final close out date. The Certificate of Non-Possession will be attached to the CSCS form and provided to the RL FCOM. (NOTE: Before canceling access authorizations, SSIMS should be checked to see if another DOE facility maintains access authorizations for the Contractor and, if so, a FDAR transferring cognizant responsibility should be initiated).

c. The prime contractor shall terminate the facility registration on the SSIMS as soon as possible but no later than ten (10) working days of receipt of the approved CSCS/FDAR form(s) from the RLFCOM.

4. EXHIBITS

a. Exhibit A – Certificate of Non-Possession

b. Exhibit B - Security Certification (Contract Closeout)

II. SURVEY, REVIEW, AND SELF-ASSESSMENT PROGRAMS. The following general requirements are added to those of Part I Section G of the HQ-CRD.

1. The contractor shall assign a finding owner for each finding and assure that an appropriate level of
Contractor Requirements Document  
(Supplemented) Form

root-cause analysis is performed and corrective actions are identified for each finding. The contractor shall have appropriately trained personnel conduct the root-cause analysis.

2. The contractor shall perform a simple root cause analysis for identified findings/incidents unless the finding/incident meets the requirements of a detailed root cause analysis or a detailed root cause analysis is directed by RL. A detailed root cause analysis is required for a finding/incident where the cause can not be determined by a simple root cause analysis, and the finding/incident indicates a single failure point (where there are no other supplemental or redundant security measures in place to mitigate the issue) that would likely lead to one of the following security incidents:

   a. Loss of accountability, theft, or diversion of Category I or II quantities of SNM
   b. Confirmed loss or unauthorized disclosure of classified matter
   c. Radiological sabotage incident as defined by the DBT
   d. Significant vulnerability to the overall Site security posture
   e. Significant vulnerability to of a PA or MAA

3. Suggestions from internal self-assessments shall be documented but do not require a corrective action plan or root cause analysis.

4. The contractor shall consolidate proposed corrective actions into a Corrective Action Plan (CAP) in the format shown in Exhibit C. The contractor shall submit the proposed CAP to the RL for approval within 30 working days after formal receipt of the survey report. If the root-cause analysis cannot be accomplished within the 30 days, specific milestones and an estimated completion date must be included in the CAP.

5. The contractor shall submit to the RL Facility Survey Operations Manager (FSOM) by the 10th of January, April, July, and October a consolidated quarterly corrective action status update, in the format shown in Exhibit D, for all open findings. When a significant change in finding status occurs between reporting periods, the contractor shall immediately send a status update to RL.

6. If an approved estimated date of completion for a finding cannot be met, the contractor shall submit a written explanation to RL. A new estimated completion date must be approved by RL.

7. When the contractor considers all corrective actions for a finding to be completed, the contractor shall prepare a Finding Validation/Closure Request in the format shown in Exhibit E and forward it to the RL FSOM via e-mail requesting closure of the finding.

8. If after validation the finding is considered "open" the contractor shall coordinate with RL to determine an appropriate course of action.

9. In the case where a finding is no longer valid or is overcome by changing events and may not require corrective action and/or validation, the contractor may request closure.

10. EXHIBITS

   a. Exhibit C – Corrective Action Plan (CAP) format
   b. Exhibit D – Quarterly Corrective Action Status Update
   c. Exhibit E – Finding Validation/Closure Request
   d. Exhibit F - Definitions

III. The following general requirements are added to those of Part I, Section G, Paragraph 6.a., of the HQ-CRD.

1. Self-assessment reports shall:
### Contractor Requirements Document (Supplemented) Form

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>Include the assessment of all applicable DOE F 470.8 topical and subtopical areas of the facility’s S&amp;S program, utilizing personnel knowledgeable of the topical or subtopical area.</td>
</tr>
<tr>
<td>b.</td>
<td>Be suitable for use by management in determining the effectiveness of S&amp;S performance and compliance with applicable DOE directives.</td>
</tr>
<tr>
<td>c.</td>
<td>List findings resulting from self-assessment activities.</td>
</tr>
<tr>
<td>d.</td>
<td>Be available for review by the Surveying Office.</td>
</tr>
<tr>
<td>e.</td>
<td>Be provided to RL SES, for information, upon completion.</td>
</tr>
</tbody>
</table>

2. All working papers and other non-record documentation associated with the performance of the assessment must be retained until the completion of the next assessment.

### IV. DEVIATION REQUEST FORMAT

The following general requirements are added to those of Part 2, Section M of the HQ-CRD.

1. **Request Number.** An alphanumeric identifier beginning with “SO” followed by the routing symbolized in the DOE National Telephone Directory, followed by the last two digits of the year of the request’s date, followed by the three-digit number that is next in the sequence of requests from that Field Element in that calendar year. For example, the third request from the Richland Operations Office during 2001 would be SO-RL-01-003. The requesting official shall obtain the deviation number from the RL SES Facility Clearance Operations Manager before the request is formally submitted.

### Specific Supplemental Requirements:

None
CERTIFICATE OF NON-POSSESSION

The contractor identified below has completed all classified work in support of DOE Contract Number:

The following security actions have been completed:

1. **Classified Documents/Materials: (Check appropriate block)**
   - [ ] No classified documents or materials were created or received by company employees under this contract.
   - [ ] All classified documents, materials, computer disks, and other media created or received under this contract have been returned to DOE custody or destroyed in accordance with DOE instructions.
   - [ ] All classified documents, materials, computer disks, and other media, created or received under this contract have been returned to DOE custody or destroyed in accordance with DOE instructions, except for those documents, materials, and media which are being retained for future use on another DOE contract.
   - [ ] A Certificate of Possession for the retained documents was issued by DOE on the following date:

2. **Personnel Security Clearances and Badges: (Check appropriate block)**
   - [ ] No personnel security clearances were granted under this contract. All Building Access Only security badges have been returned to DOE custody.
   - [ ] All personnel security clearances granted under this contract have been terminated. DOE security badges for employees with terminated clearances have been returned to DOE custody.
   - [ ] All personnel security clearances granted under this contract have been terminated, or have been transferred to another DOE contract. DOE security badges for employees with terminated clearances have been returned to DOE custody.

For Contractor Use Only

============================================================================

<table>
<thead>
<tr>
<th>Signature of Facility Security Officer</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Typed/Printed Name of Facility Security Officer</th>
<th>Facility Code</th>
</tr>
</thead>
</table>
EXHIBIT B
SECURITY CERTIFICATION
(Contract Closeout)

Contractor

Contract No.

☐ This contract did not involve possession of classified matter or special nuclear material.

☐ The following was/were possessed under this contract (check the applicable items):

☐ Classified Documents
☐ Classified Material
☐ Special Nuclear Material (SNM)

This certifies that all classified matter (documents and material) or special nuclear material originated and/or received in conjunction with the work performed under this contract have been returned to the Department of Energy (DOE) or disposed of in accordance with DOE directives.

☐ No DOE access authorizations (security clearances) were associated with this contract.

☐ All DOE access authorizations based upon this contract have been terminated in accordance with DOE directives.

(Name and Signature of Prime Contracting Official) ____________________________ (Date)____

(Name and Signature of Prime Contractor Security Official) ______________________ (Date)
**EXHIBIT C**
CORRECTIVE ACTION PLAN FORMAT

**Survey Title:** Survey title, date (listed on title page) and, if applicable, the classified document number.


**Finding:** When documenting findings, use the following:
  
  Example: 00JAN10-RL-0476-SSIS-PPO-010
- The Finding as stated in the survey report (use exact verbiage).

  **Corrective Action:** Include the following for each Finding, if applicable:
- Action(s) taken to immediately correct the situation, including any compensatory measure(s).
- Action(s) to be taken to resolve the issue.
- Identify any time lines, schedules and/or milestones associated with the resolution of the Finding.

**Estimated Completion Date:** This is the date the corrective action is considered complete.

**NOTE:** Estimated completion dates (ECD) shall reflect the exact date completion is anticipated.

**Root-Cause Analysis:**
Provide the results of the Root Cause Analysis. If a Root Cause Analysis cannot be accomplished within the 30 working days, indicate this in the CAP, and include specific milestone(s) and ECDs for the analysis.

**Estimated Cost:**
Indicate total cost involved with resolution of each finding.

---

**EXHIBIT D**
QUARTERLY CORRECTIVE ACTION STATUS UPDATE

**Finding No.:** Assigned Finding Number from the Survey Report.

Example: 00JAN10-RL-0476-SSIS-PPO-010 RV 6

**Finding:** Exactly as stated in the survey report.

**Corrective Action:** Describe the specific activity that has taken place during the reporting period regarding completion of the corrective action.

**NOTE:** “No Change” is an acceptable entry if no action has taken place during the reporting period.
EXHIBIT E

FINDING VALIDATION/CLOSURE REQUEST


Example: 00JAN10-RL-0476-SSIS-PPO-010

Finding: Exactly as stated in the survey report.

Corrective Action: Exactly as stated in the approved Corrective Action Plan.

Surveyed Organization Comments: Document all actions taken to validate completion of the corrective action(s). If more space is required, append additional pages. Any supporting documentation should be appended.

Surveyed Organization Validating Official __________________________ Date __________________________

* * * * * * * * * * * RL SES REVIEW * * * * * * * * * * *

RL SES Oversight Designee Comments: This block is required to be completed to validate closure of the finding. State how the corrective action(s) was/were validated. If the finding cannot be closed, include specific information regarding the reasons why, and what needs to be accomplished for closure. If more space is required, append additional pages.

Status: Open _____ Closed _____

RL SES Validation Official: __________________________ Date: ________

(Print Name)

* * * * * * * * * * * * RL SES SSIMS DATA ENTRY * * * * * * * * * * *

Entered by: __________________________ Date: ________
EXHIBIT F

DEFINITION OF TERMS

Definitions of terms commonly used in the safeguards and security program are provided in the DOE “Safeguards and Security Glossary of Terms,” which is distributed by SES.

Finding. A separate, distinct, condition identified during a SES safeguards and security survey or Office of Independent Oversight and Performance Assurance (OA) inspection that is not in compliance with directives or requirements.

Root Cause. The cause(s), which if corrected, will prevent or reduce recurrence of a finding. Root causes may be identified through a variety of analytical techniques, varying from management evaluations based on the specific situations presented to rigorous mathematical analyses.

Safeguards and Security Assignment Grid. A tabular grid that relates the potential consequence of an uncorrected condition to various attributes in such a way as to provide a numerical "Risk Value." The Risk Value is then used to determine the level of effort with which root cause analysis and/or other follow-up are done.

Suggestion. Information a field organization provides to identify potential program enhancements.

Validation. The confirmation, by testing, observation, etc., that approved corrective actions for a finding have been satisfactorily implemented and that the deficiency is corrected.

EXHIBIT G

Incident/Inquiry Report

DOE HQ Tracking Number:

Locally Assigned Incident Tracking Number:

Impact Measurements Index (IMI) Number:

1.0 Location: (Complete the following responsible Office and Facility information as identified in SSIMS.)

Operations/Field/Site Office:
SSIMS Facility Code:
Facility Abbreviation:

Facility Responsible for Inquiry:
SSIMS Facility Code:
Facility Abbreviation:
Location (Bldg./Rm.):

Facility at which incident occurred (if other than above), and any Other Facilities/Location(s) affected by incident:
Location Name:
SSIMS Facility Code (if applicable).
Address:
City:
State:
Location (Bldg./Rm.):

Security area where incident occurred: (check all that apply)
[ ] Property Protection Area
[ ] Limited Area
[ ] Exclusion Area
[ ] Protected Area
[ ] Material Access Area
[ ] Vital Area
[ ] SCIF
[ ] SAPF/SSWA
[ ] Classified Information System Facility
[ ] Secure Communications Center
[ ] Non-Security Area (e.g., private residence, public areas, etc.)

2.0 Dates:

2.1 Reporting:
Incident Occurred Date/Time:
Incident Discovered Date/Time:
IMI Categorization made Date/Time:
Incident contained to prevent further compromise Date/Time:
DOE F 471.1 transmitted to HQ EOC Date/Time:
Inquiry initiated (determination that an incident has occurred) Date:
Inquiry Status Report transmitted to SO Date:
Inquiry completed Date:
Inquiry Report transmitted to SO Date:

2.2 Follow-up:
Interim corrective actions implemented Date:
Proposed corrective actions transmitted to SO Date:
GEN-16 policy applied by Classification Office Date:
Damage Assessment completed Date:
Incident officially closed Date:

3.0 Identification: Copy and Paste additional IDENTIFICATION sections below, as necessary.

3.1 Notifications
Facility Security Officer:
Name:
Phone:

DOE Cognizant Security Organization or HQ Representative:
Name:
Contractor Requirements Document
(Supplemented) Form

Phone:

Others Notified (e.g., ISSO, security personnel, etc...):
Name:
Phone:

SO Representative:
Name:
Phone:

3.2 Inquiry
Lead Organization and Inquiry Official:
Name:
Organization:
Phone:

Inquiry Official(s) at other affected sites:
Name:
Organization:
Phone:

Inquiry Participant(s)/Assistant Inquiry Officials:
Name:
Organization:
Phone:

Other Departmental Elements, Field/Operations Offices, Area Offices, Government Agencies, Foreign Government Agencies, or Contractors involved in the Inquiry:
Organization Name:
POC Name:
Phone:

Case released to other agency(s), including but not limited to LLEA (outside of DOE, including NNSA):
Organization Name:
POC Name:
Phone:

3.3 Individuals Involved
Responsible Individual(s):
Name:
Organization:
Title:
Phone:
Was this individual interviewed? [ ] Yes [ ] No
Written statement available? [ ] Yes [ ] No
Is this individual a foreign national? [ ] Yes [ ] No
Was this individual appropriately cleared? [ ] Yes [ ] No
First Line Supervisor’s Name:

Other Individual(s):
Name:
Contractor Requirements Document
(Supplemented) Form

Organization:
Title:
Phone:
Was this individual interviewed? [ ] Yes [ ] No
Written statement available? [ ] Yes [ ] No
Is this individual a foreign national? [ ] Yes [ ] No
Was this individual appropriately cleared? [ ] Yes [ ] No

4.0 Security Incident Description: (from the tables below, identify the incident)

Reportable Categories of Incidents of Security Concern

4.1 Impact Measurement Index (IMI-1)

Actions, inactions, or events that pose the most serious threats to national security interests and/or critical DOE assets, create serious security situations, or could result in deaths in the workforce or general public. Report within 1 hour.

[ ] 1.1 Confirmed or suspected loss, theft, or diversion of a nuclear device or components.
[ ] 1.2 Confirmed or suspected loss, theft, diversion, or unauthorized release of weapon data.
[ ] 1.3 Confirmed or suspected loss, theft, or diversion of Category I/II quantities of Special Nuclear Materials (SNM).
[ ] 1.4 A shipper-receiver difference involving a loss in the number of items which total a Category I or II quantity of SNM.
[ ] 1.5 Confirmed or suspected loss, theft, diversion, unauthorized release of TOP SECRET information, Special Access Program (SAP) information, or Sensitive Compartmentalized Information (SCI) regardless of the medium, method, or action resulting in the incident.
[ ] 1.6 Confirmed or suspected intrusions, hacking or break-ins into DOE computer systems containing TOP SECRET, SAP, or SCI information.
[ ] 1.7 Confirmed or suspected physical intrusion attempts or attacks against DOE facilities containing nuclear devices and/or materials, classified information, or other national security related assets.
[ ] 1.8 Confirmed or suspected attacks against DOE federal and contractor employees that adversely impact a facility’s or site’s security posture.
[ ] 1.9 Confirmed or suspected acts or attempts of terrorist-type actions.
[ ] 1.10 Confirmed reports of DOE or DOE contractor employees making threats against Departmental facilities, employees, or the US Government.
[ ] 1.11 Confirmed threats that immediately endanger personnel health or safety and may require immediate protective force/law enforcement intervention.
[ ] 1.12 Dangerous weapons and firearms-related incidents where an individual is killed, wounded, or an intentional discharge occurs.
[ ] 1.13 Confirmed or suspected acts of sabotage, at any DOE facility, that places the safety or security of personnel, facilities, or the public at risk.
[ ] 1.14 Confirmed compromise of root/administrator privileges in DOE unclassified computer systems that have a significant possibility of being contaminated with Top Secret information, SAP information, or SCI.
[ ] 1.15 Confirmed compromise of root/administrator privileges in DOE computer systems containing Secret or Confidential information.
[ ] 1.16 Confirmed intrusions into information systems containing classified information.
[ ] 1.17 Instances of malicious code that cause disruption, degradation, or compromise of information systems for an entire site/facility.
[ ] 1.18 Instances of malicious code that allow unauthorized or undetected access to information systems containing classified information (Top Secret, Secret, Confidential, SAP information, or SCI).
Contractor Requirements Document
(Supplemented) Form

[ ] 1.19 Other (describe “Other”):
<Select the Topical Area for this “Other” IMI category:
[ ] PHYSEC, [ ] INFOSEC, [ ] PERSEC, [ ] OTSEC, or [ ] NMC&A>

4.2 Impact Measurement Index (IMI-2)
*Actions, inactions, or events that pose threats to national security interests and/or critical DOE assets or that potentially create dangerous situations. Report within 8 hours.*

[ ] 2.1 Suspected loss, theft, or diversion of any radioactive material not categorized as special nuclear materials (SNM), or dangerous materials that could pose a health threat or endanger security.
[ ] 2.2 Confirmed or suspected intrusions, hacking or break-ins into DOE computer systems containing SECRET or CONFIDENTIAL information.
[ ] 2.3 Any amount of SNM found in an exceptionally dangerous/hazardous unapproved storage environment or unapproved mode of transportation/transfer.
[ ] 2.4 Alarms or other loss detection indicators for security areas containing a Category I or II quantity of SNM that cannot be proven false within 24 hours.
[ ] 2.5 Inventory differences exceeding alarm limits in Category I and II SNM material balance areas, where there is no indication or reason to believe the difference is created by loss, theft or diversion.
[ ] 2.6 Confirmed or suspected unauthorized disclosure, loss, or potential loss of Secret matter regardless of the medium, method, or action resulting in the incident.
<Select the Topical Area for this specific IMI category:
[ ] PHYSEC, [ ] INFOSEC, [ ] PERSEC, [ ] OTSEC, or [ ] NMC&A>

[ ] 2.7 Actual or suspected technical interceptions of any level of classified information.
[ ] 2.8 Actions, by electronic or physical means, that interfere with any DOE safeguards and security practices.
[ ] 2.9 Notifications, by any media or source, of validated threats that do not appear to immediately threaten personal safety or health
[ ] 2.10 Loss of classified information that must be reported to other Government agencies of foreign organizations.
[ ] 2.11 Unsecured classified repositories of any type, including safes, doors, or other protective encasements, that contain Top Secret information, Special Access Program Information, or Sensitive Compartmented Information.
[ ] 2.12 The loss of any DOE classified interest that requires state or local government or other Federal agency notification.
[ ] 2.13 Confirmed compromise of root/administrator privileges in DOE unclassified computer systems.
[ ] 2.14 Confirmed compromise of root/administrator privileges in DOE unclassified computer systems that have a significant possibility of being contaminated with Secret or Confidential information.
[ ] 2.15 Potential compromise of root/administrator privileges in DOE computer systems containing classified information.
[ ] 2.16 Instances of malicious code that cause disruption/degradation or compromise of information systems dedicated to safety, security, or critical operations.
[ ] 2.17 Detection of activities involving individuals who have confirmed as physically watching/casing/surveilling a site in an effort to gather information to aid in the conduct of a terrorist-type attack.
[ ] 2.18 Other (describe “Other”):
<Select the Topical Area for this “Other” IMI category:
[ ] PHYSEC, [ ] INFOSEC, [ ] PERSEC, [ ] OTSEC, or [ ] NMC&A>

4.3 Impact Measurement Index (IMI-3)
*Actions, inactions, or events that pose threats to DOE security interests or that potentially degrade the overall effectiveness of the Department’s safeguards and security protection program. Report within 8 hours.*
### Contractor Requirements Document
(Supplemented) Form

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>A shipper-receiver difference or inventory difference involving a gain in the number of items for which the additional items total a Category I or II quantity of SNM.</td>
</tr>
<tr>
<td>3.2</td>
<td>Bomb-related incidents at any DOE facility including location of a suspected device.</td>
</tr>
<tr>
<td>3.3</td>
<td>Confirmed or suspected unauthorized disclosure, loss or potential loss of CONFIDENTIAL matter by any medium, method, or action.</td>
</tr>
<tr>
<td>3.4</td>
<td>Confirmed or alleged noncompliance with laws or DOE directives/standards that jeopardizes the protection of the facility or site security interests.</td>
</tr>
<tr>
<td>3.5</td>
<td>Demonstrators or protestors that cause site and facility damage.</td>
</tr>
<tr>
<td>3.6</td>
<td>Labor strikes that could degrade or impede the required protection of the facility or site.</td>
</tr>
<tr>
<td>3.7</td>
<td>Physical violence or threat of retaliation against facility security personnel.</td>
</tr>
<tr>
<td>3.8</td>
<td>Dangerous weapons and firearms-related incidents involving protective force operations/personnel where an unauthorized weapon discharge occurs.</td>
</tr>
<tr>
<td>3.9</td>
<td>Loss or theft of DOE firearms or ammunition, per DOE M 470.4-3, PROTECTIVE FORCE.</td>
</tr>
<tr>
<td>3.10</td>
<td>Unplanned/unscheduled power outages that cause a disruption/degradation of physical security systems and that would allow unauthorized or undetected entry to access controlled/protected areas.</td>
</tr>
<tr>
<td>3.11</td>
<td>Incidents involving the attempted or actual introduction of controlled and prohibited items into Limited, Exclusion, Protected, or Material Access Areas, excluding unauthorized cellular phones or personal digital assistants where there is no potential for compromise of classified or unclassified controlled information.</td>
</tr>
<tr>
<td>3.12</td>
<td>Confirmed or suspected malicious activities, including but not limited to stealing badges or vehicle licenses.</td>
</tr>
<tr>
<td>3.13</td>
<td>Discovery of malicious activities, disorderly conduct, or vandalism that disrupts facility activities or causes damage between $10K and $100K.</td>
</tr>
<tr>
<td>3.14</td>
<td>Circumvention of established access control procedures into a security area (excluding Property Protection Area).</td>
</tr>
<tr>
<td>3.15</td>
<td>Inventory differences exceeding alarm limits in Category III SNM material balance areas or inventory differences greater than 50 g of Tritium, where there is no indication or reason to believe the difference is created by loss, theft, or diversion.</td>
</tr>
<tr>
<td>3.16</td>
<td>A shipper-receiver difference involving a loss in the number of items which total a Category III or IV quantity of SNM.</td>
</tr>
<tr>
<td>3.17</td>
<td>Confirmed or suspected loss, theft, or diversion of Category III or IV quantities of SNM.</td>
</tr>
<tr>
<td>3.18</td>
<td>Intrusion attempts into information systems containing classified information.</td>
</tr>
<tr>
<td>3.19</td>
<td>Confirmed intrusions into unclassified information systems that are not publicly available (e.g. behind a firewall).</td>
</tr>
<tr>
<td>3.20</td>
<td>Confirmed instances of “denial of service” attacks on information systems that result in disruption of site/facility ability to access the Internet, disruption of site/facility information systems operations, or disruption of site/facility information system protection measures (e.g. firewall).</td>
</tr>
<tr>
<td>3.21</td>
<td>Unauthorized network scans/probes on information systems possessing classified information.</td>
</tr>
<tr>
<td>3.22</td>
<td>Incidents of apparent surveillance of facilities or operations (studying, photographing, low over-flights, outsiders questioning employees or protection force, unusual calls for information, etc.).</td>
</tr>
<tr>
<td>3.23</td>
<td>Other (describe “Other”): &lt;Select the Topical Area for this “Other” IMI category: [ ] PHYSEC, [ ] INFOSEC, [ ] PERSEC, [ ] OTSEC, or [ ] NMC&amp;A&gt;</td>
</tr>
</tbody>
</table>

#### 4.4 Impact Measurement Index (IMI-4)

**Actions, inactions, or events that could pose threats to DOE by adversely impacting the ability of organizations to protect DOE safeguards and security interests. Report monthly.**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Identified special nuclear materials (SNM) inventory differences beyond alarm limits in a Category IV SNM material balance area where there is no indication or reason to believe the difference is created by loss, theft, or diversion.</td>
</tr>
<tr>
<td>4.2</td>
<td>Significant shipper/receiver differences that exceed 200 grams of fissile material and the combined limit of error for the shipment.</td>
</tr>
</tbody>
</table>
### Contractor Requirements Document (Supplemented) Form

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ] 4.3</td>
<td>Alarms or other loss detection indicators, excluding inventory differences and shipper/receiver differences, for a security area containing a Category III or IV quantity of SNM.</td>
</tr>
<tr>
<td>[ ] 4.4</td>
<td>A shipper-receiver difference or inventory difference involving a gain in the number of items for which the additional items total to a Category III or IV quantity of SNM.</td>
</tr>
<tr>
<td>[ ] 4.5</td>
<td>Confirmed or suspected unauthorized disclosure of Unclassified Controlled Nuclear Information, Export Control information, and unclassified Naval Nuclear Propulsion Information by any medium, method, or action.</td>
</tr>
<tr>
<td>[ ] 4.6</td>
<td>Non-credible bomb threats at any DOE nuclear or non-nuclear facility.</td>
</tr>
<tr>
<td>[ ] 4.7</td>
<td>Unsecured classified repositories of any type including safes, doors, or other protective encasements in which no likely classified disclosure occurred. If the repository contains Top Secret Information, Special Access Program information, or Sensitive Compartmented Information, report under the IMI-1, IMI-2, or IMI-3 category, as appropriate.</td>
</tr>
<tr>
<td>[ ] 4.8</td>
<td>Peaceful demonstrations or protests that do not threaten facility or site security interests or activities.</td>
</tr>
<tr>
<td>[ ] 4.9</td>
<td>Failure to adhere to established procedures contributing to the misuse or misprocessing of or failure to maintain security badges and passes.</td>
</tr>
<tr>
<td>[ ] 4.10</td>
<td>Loss of security badges in excess of 5 percent of total issued during 1 calendar year.</td>
</tr>
<tr>
<td>[ ] 4.11</td>
<td>Failure to adhere to established procedures contributing to the mismanagement or faulty application of the DOE Human Reliability Program.</td>
</tr>
<tr>
<td>[ ] 4.12</td>
<td>Failure to adhere to established administrative procedures contributing to problems with foreign visitors.</td>
</tr>
<tr>
<td>[ ] 4.13</td>
<td>Classified information sent via e-mail that is contained within the firewall. All parties involved are cleared to the level of information transmitted, and the affected systems are identified, taken off-line and appropriately stored in approved areas pending sanitization. If more than 8 hours are required to isolate the affected systems, then such incidents will be handled as suspected compromises in accordance with their classification levels and categories.</td>
</tr>
<tr>
<td>[ ] 4.14</td>
<td>Unauthorized cellular phones and personal electronic devices (e.g., PDAs) introduced into a Limited Area, Protected Area, or Material Access Area, where there is no potential for compromise of classified or unclassified controlled information.</td>
</tr>
<tr>
<td>[ ] 4.15</td>
<td>Circumvent established access control procedures into a Property Protection Area.</td>
</tr>
<tr>
<td>[ ] 4.16</td>
<td>High rate/amount of loss (excluding natural disasters) or theft of Government property.</td>
</tr>
<tr>
<td>[ ] 4.17</td>
<td>Other (describe “Other”):</td>
</tr>
</tbody>
</table>

   <Select the Topical Area for this “Other” IMI category: |
   [ ] PHYSEC, [ ] INFOSEC, [ ] PERSEC, [ ] OTSEC, or [ ] NMC&A> |

### 5.0 Classified Matter Description:

#### 5.1 Type

**Incident Type:** (check all that apply)

- [ ] Unsecured/Improperly secured matter
- [ ] Classified matter processed on an unclassified computer
- [ ] Improper transmission (e.g. Facsimile, E-Mail, package carrier)
- [ ] Located/Found in an unapproved facility (including private residences)
- [ ] Verbal
- [ ] Media leak
- [ ] Classification Issue (includes failure to obtain classification review)
- [ ] Other (describe “Other”):

**Form(s) of the matter involved in the incident:** (check all that apply)

- [ ] Electronic Storage Media
- [ ] E-Mail
- [ ] Facsimile
Contractor Requirements Document (Supplemented) Form

[ ] Hard Copy
[ ] Internet
[ ] Visual
[ ] Audio/Verbal
[ ] Other (describe “Other”):

Identify the owner of the information (e.g., SO-10, NN-55, etc.):

Did the matter involve Work for Others?” [ ] Yes [ ] No

Did the matter involved belong to an “Other Government Agency?” [ ] Yes [ ] No

If “Yes,” Identify Other Government Agency(s) involved:

5.2 Classification
Classification Level: (check only one)
[ ] Top Secret
[ ] Secret
[ ] Confidential

Category of Information: (check only one)
[ ] Restricted Data
[ ] Formerly Restricted Data
[ ] National Security Information

Caveats: (check all that apply)
[ ] Weapons Data (WD)
[ ] Special Access Program (SAP)
[ ] Sensitive Compartmented Information (SCI)
[ ] Foreign Government Information (FGI)
[ ] Naval Nuclear Propulsion Information (NNPI)
[ ] No Foreign Dissemination (NOFORN)
[ ] Other (describe “Other”):

5.3 Description
In the following field, identify/describe the classified matter lost, compromised, or potentially compromised (e.g., document title and date, description of matter):

In the following field, list the Classification Guide and Topic, or Source Document, including date, that apply to the classification of the matter:

Classification Official(s) that verified the matter’s classification (if applicable):
Name:
Phone:
6.0 Narrative:

Describe the incident (including an executive summary, chronology of events, and conclusion, identifying who, what, when, where, why, and how) in accordance with DOE requirements for Inquiry Report Content identified in “Reporting Incidents of Security Concern.” (Specifics captured elsewhere in this report may be excluded):

7.0 Containment:

Summarize the actions taken to contain (and sanitize if appropriate) the incident:

8.0 Mitigating/Aggravating Factors:

Identify any information that may be considered as a mitigating factor and reduces the potential impact of the incident:

Identify any information that may be considered as an aggravating factor and increases the potential impact of the incident:

9.0 Determination of Inquiry:

9.1 Determination

Determination of Unauthorized Disclosure:(check only one)
[ ] Loss/compromise did occur
[ ] Probability of compromise is not remote
[ ] Probability of compromise is remote
[ ] Loss/compromise did not occur

(UD ONLY) If the inquiry established credible information that a Violation of U.S. law pertaining to the Unauthorized Disclosure of classified information to the media occurred, is the DOJ 11-point criteria satisfied? [ ] Yes [ ] No

Fundamental (root) cause(s) of the incident involves: (check all that apply)
[ ] Equipment/Material Problem
[ ] Management Problem
[ ] Personnel Error
[ ] Procedure Problem
[ ] Training Deficiency
[ ] Design Problem
[ ] External Phenomena
[ ] Other (describe “Other”):

Summarize the root cause of the incident (include direct and contributing factors). This can include formal and/or information root cause analysis:

How would the responsible individual(s) non-compliance be characterized: (check only one)
[ ] Inadvertent  
[ ] Negligence  
[ ] Gross Negligence  
[ ] Willful

9.2 Summary  
Summarize the Conclusion of the Inquiry (include basis/facts that support the conclusion and potential risk to the security interest based upon subjective analysis):

9.3 Damage Assessment  
Has the Program Office requested a Damage Assessment be done? [ ] Yes [ ] No  
Was a damage assessment completed (formal and/or informal)? [ ] Yes [ ] No  
Summarize the results of the (formal and/or informal) damage assessment:

9.4 Documentation  
**Documentation included in inquiry report:** (check all that apply. * indicates a required item.)  
[ ] Security Incident Notification Report (DOE F 471.1)*  
[ ] Inquiry Official(s) Appointment Letter*  
[ ] Reporting Unaccounted for Documents (DOE F 5639.2)  
[ ] Inquiry Report*  
[ ] Copy of Compromised or Potentially Compromised Information (portion marking must be applied to identify what is classified)*  
[ ] Interview Statement(s)*  
[ ] Damage Assessment Report  
[ ] Proposed Corrective Action Plan  
[ ] Report of Security Incident/Infraction (DOE F 5639.3) or a form comparable in content, as applicable  
[ ] Occurrence Reporting and Processing System (ORPS)  
[ ] Chain of Custody Form(s)  
[ ] Other (describe “Other”):

10.0 Corrective Actions:  
**Categorize Action(s) Taken:** (check all that apply)  
[ ] Communication security system modification  
[ ] Cyber security system modification  
[ ] Disciplinary action  
[ ] Physical security system modification  
[ ] Policy/procedural change  
[ ] Training Modification  
[ ] Other (describe “Other”):

**Summarize the proposed corrective actions identified to prevent recurrence** (corrective actions identified in response to an incident of security concern must be documented and, for incidents categorized as IMI-1, 2, & 3 a copy forwarded to
Management Official(s) responsible for Corrective Actions:
Name:
Phone:

11.0 Disciplinary Actions:

Action taken: (check all that apply)
[ ] Mandatory training
[ ] Oral admonishment
[ ] Personnel reassignment
[ ] Suspension of access authorization
[ ] Termination of access authorization
[ ] Termination of employment
[ ] Written reprimand
[ ] Other (describe “Other”):

Are there mitigating factors affecting disciplinary action? [ ] Yes [ ] No

If “Yes”, identify the factors: (check all that apply)
[ ] Culpability of others
[ ] Employee cooperativeness
[ ] Enticements or provocations
[ ] Possibility of genuine misunderstanding
[ ] Other (describe “Other”):

Are there aggravating factors affecting disciplinary action? [ ] Yes [ ] No

If “Yes”, identify the factors: (check all that apply)
[ ] Employee willfulness
[ ] Nature of other breaches
[ ] Past breaches
[ ] Series of breaches
[ ] Other (describe “Other”):

Management Official(s) responsible for Disciplinary Actions:
Name:
Phone:

12.0 Comments and Attachments:
Include any comments associated with the incident and attachment references (e.g. Photos, Spreadsheets, Database files, Signed documents, etc.): Attach information as appropriate.