

## **ERRATA SHEET**

This Errata Sheet transmits the following minor change to NSO O 471.X, INCIDENTS OF SECURITY CONCERN, dated 2-9-09. The directive number has been changed to NSO O 470.X4.

The change is reflected in this directive.

This Errata Sheet must remain with NSO O 470.X4.

**U.S. DEPARTMENT OF ENERGY  
NATIONAL NUCLEAR SECURITY ADMINISTRATION  
NEVADA SITE OFFICE**

**ORDER**

**NSO O 470.X4**

**Approved: 02-09-09  
Review Date: 02-09-13**

---

**INCIDENTS OF SECURITY CONCERN**

---



---

**INITIATED BY:  
Office of the Assistant Manager  
for Safeguards and Security**

## INCIDENTS OF SECURITY CONCERN

NSO O 470.X4  
2-9-09

1

1. OBJECTIVE. This Order provides National Nuclear Security Administration (NNSA) Nevada Site Office (NNSA/NSO) policies and procedures for the implementation of Incidents of Security Concern.
2. CANCELLATION. None.
3. APPLICABILITY.
  - a. The provisions of this Order apply to all NNSA/NSO organizational elements.
  - b. The Contractor Requirements Document (CRD), Attachment 1, sets forth intended requirements to be applied to contractors, National Laboratories, other federal agencies, and other user organizations. Compliance with the CRD will be required to the extent set forth in a contract or management agreement.
  - c. This directive applies to NNSA/NSO-related facilities only.
4. REQUIREMENTS. These requirements apply to all NNSA/NSO, contractors, National Laboratories, and other federal agencies whose security personnel or other designated representatives are involved with Incidents of Security Concern.
  - a. 24-Hour Determination/Categorization Period. A review of all pertinent facts and circumstances must be conducted within a 24-hour timeframe to determine whether an Incident of Security Concern has occurred. During this 24-hour period, the incident must be categorized by an Impact Measurement Index (IMI) number as identified in DOE M 470.4-1 Chg 1, Tables 1-4, Part 2, Section N, Chapter I. If it is determined that an Incident of Security Concern did not occur, no further action is required.
  - b. Initial Incident Reporting.
    - (1) Security incidents, IMI-1, IMI-2, IMI-3, and IMI-4, must be immediately reported verbally to the Office of the Assistant Manager for Safeguards and Security (OAMSS) Security Incident Program Manager.
    - (2) The OAMSS Security Incident Program Manager will then:
      - (a) Within one hour following categorization for security incidents determined to be IMI-1 (see Table 1, DOE M 470.4-1 Chg 1), must transmit the DOE F 471.1 form to the Department of Energy (DOE) Headquarters (HQ) Operations Center (OC) and NNSA/HQ through the NNSA/NSO Emergency OC (EOC). If verbal notification of the

incident is made to the DOE/HQ OC, a follow-up transmission of the DOE F 471.1 form to the DOE/HQ OC must still be made.

- (b) Within eight hours following categorization for security incidents determined to be IMI-2 or IMI-3, must transmit the DOE F 471.1 form to DOE/HQ OC and NNSA/HQ through the NNSA/NSO EOC. If verbal notification of the incident is made to the DOE/HQ OC, a follow-up transmission of the DOE F 471.1 form to the DOE/HQ OC must still be made.
- (c) Within eight hours following categorization for security incidents determined to be IMI-4, must transmit the DOE F 471.1 form to OAMSS.

5. RESPONSIBILITIES.

a. OAMSS.

- (1) Ensures the requirements outlined in this Order are in compliance with DOE M 470.4-1.
- (2) Ensures a Security Incident Program Manager is appointed in writing.

b. Security Incident Program Manager.

- (1) Provides oversight of the Security Incident Program.
- (2) Transmits the required forms to DOE/HQ and NNSA/HQ and EOC, as required.
- (3) Enters Incidents of Security Concern into the incident tracking system and provides a case number to the inquiry official.
- (4) Ensures incidents are entered into the Safeguards and Security Information Management System.
- (5) Ensures final inquiry reports or status reports are submitted in accordance with DOE M 470.4-1 Chg 1, Part 2, Section N, Chapter I, Section 3k.
- (6) Provides to DOE/HQ a monthly report recapping all IMI-4 Incidents of Security Concern no later than the first working day of each month to reflect data for the preceding month.

## INCIDENTS OF SECURITY CONCERN

NSO O 470.X4  
2-9-09

3

---

c. Facility Security Officer (FSO) or Designee.

- (1) Ensures an Inquiry Official is appointed, in writing, and trained.
- (2) Reports all security incidents immediately to OAMSS.
- (3) Ensures a security incident is investigated.
- (4) Ensures each security incident is completed to include corrective actions.
- (5) Submits to OAMSS an annual indicator/trend analysis report of Incidents of Security Concern no later than January 15 of each calendar year.
- (6) Provides security incident synopsis to the Security Awareness Coordinator for inclusion in the security awareness training/briefing.

d. Inquiry Official.

- (1) Conducts inquiries to establish the pertinent facts and circumstances surrounding Incidents of Security Concern.
- (2) Inquiry Officials must have previous investigative experience or department inquiry training, and must be knowledgeable of appropriate laws, executive orders, departmental directives, and/or regulatory requirements.
- (3) Responsible for conducting the inquiries and maintaining records and documentation associated with the inquiry (e.g., logs of events, notes, recording, and statements).
- (4) Immediately notify OAMSS upon discovery of suspected or confirmed violations of law.
- (5) Ensure inquiries are conducted and the reports are processed in accordance with DOE M 470.4-1, Section N.
- (6) Conducting Inquiries.
  - (a) An inquiry must be conducted to review the circumstances surrounding an Incident of Security Concern to develop all pertinent information and to determine whether an infraction, criminal violation, or loss has occurred. Inquiries are not to be used as a means of holding in abeyance a decision to initiate a full-scale investigation.

## INCIDENTS OF SECURITY CONCERN

NSO O 470.X4  
2-9-09

4

---

- (b) The organizational Inquiry Official will initiate an inquiry and assign a case number provided by OAMSS. The appointed individual must have an appropriate security clearance and must NOT be someone involved, directly or indirectly, in the incident. An initial review, 24-hour determination/categorization, will determine if the incident is of security concern. For any incident determined to be of security concern, an inquiry will be conducted and documented.
- (c) When an inquiry establishes that an alleged or suspected violation of law involving a national security interest has occurred, OAMSS will refer the incident to the Federal Bureau of Investigation and/or the appropriate law enforcement agency.
- (d) Upon determining or becoming aware of the fact that classified matter **may** be lost or unaccounted for, an inspection of the area(s) where the matter was stored, handled, or processed will be immediately initiated and completed within 48 hours. The completion of this inspection would then determine if an incident has in fact occurred. The 24-hour time limit for IMI categorization required by DOE M 470.4-1 would then begin.
- (e) Ensure inquiry reports contain the following information:
  - 1 When, where, and how did the incident occur?
  - 2 What persons, situations, or conditions caused or contributed to the incident?
  - 3 Who reported the incident, to whom, and when?
  - 4 The name of the individual(s) who was primarily responsible for the incident, including prior Incidents of Security Concern for which the individual has been determined responsible. When individual responsibility cannot be established and the facts show that management allowed conditions to exist that led to an Incident of Safeguards and Security Concern, the responsibility will be assessed upon that manager.
  - 5 A statement of corrective action taken to preclude recurrence and disciplinary action taken against responsible individual(s), if any.  
**NOTE:** In most cases, confirmation of a compromise or potential compromise will be provided through the inquiry process.

## INCIDENTS OF SECURITY CONCERN

NSO O 470.X4  
2-9-09

5

- 
- (f) In cases of compromise of classified information to public media, the inquiry should determine:
- 1 In what specific media article or program did the classified information appear?
  - 2 To what extent was the compromised information disseminated?
  - 3 Was the information properly classified?
  - 4 Was the information officially released?
- (7) Reporting Requirements.
- (a) Reporting Incidents Associated with Non-U.S. Citizens. Security incidents having any association with non-U.S. citizens must be clearly identified and reported on the initial DOE F 471.1 form and subsequently in any related update or follow-on activity pertaining to the incident. For security incidents involving any credible information that a non-U.S. citizen or an agent of a foreign power is involved, the Nevada Counterintelligence Office must also be notified.
  - (b) Numbering Incidents and Changing Categories. When the initial incident notification report (i.e., DOE F 471.1 form) is transmitted, it must include a local incident tracking number, which is obtained through the Security Incident Program Manager. Changes in IMI categorizations require resubmission of a DOE F 471.1 form to the DOE/NNSA Office of Security through OAMSS.
  - (c) Reporting Incidents Associated with Sensitive Programs. Only the initial DOE F 471.1 form is required for incidents involving activities associated with sensitive programs. These programs include the Sensitive Compartmented Information Program, Special Access Program, the Technical Surveillance Countermeasures Program, the Counterintelligence Program, or other programs identified by the DOE/NNSA Office of Security. All Subsequent reporting must be handled "within channels" until such time as the inquiry report has been distributed.

- (8) Inquiry Process.
- (a) Document interviews in writing. **NOTE:** Inquiry Officials are not authorized to detain individuals for interviews or obtain sworn statements; however, they may conduct consensual interviews and obtain signed statements.
  - (b) Collect all data/information regarding the security incident.
  - (c) Ensure physical evidence is protected and controlled and a *Chain-of-Custody* form (see DOE M 470.4-1, Figure 2) is used and maintained.
- (9) Inquiry Report. The Inquiry Report will include:
- (a) An executive summary.
  - (b) A detailed narrative describing the facts and circumstances surrounding the security incident with the who, when, what, and where.
  - (c) A conclusion.
  - (d) A corrective action to prevent a reoccurrence.
  - (e) A copy of the memorandum appointing the inquiry official.
- (10) Closing Inquiries.
- (a) IMI-1 and IMI-2 incidents are considered closed upon completion of the inquiry report. Completion reports must be forwarded to OAMSS within 55 working days.
  - (b) IMI-3 incidents are considered closed upon completion of the DOE F 5639.3 form and transmission of the completed DOE F 5639.3 form to the DOE/NNSA Office of Security through OAMSS. The completion of the section on assignment and acceptance of security infractions (Part II, DOE F 5639.3) must be completed prior to submission to OAMSS. These reports must also include an executive summary, narrative, and corrective action(s). Completion reports must be forwarded to OAMSS within 30 working days.

## INCIDENTS OF SECURITY CONCERN

NSO O 470.X4  
2-9-09

7

- (c) IMI-4 incidents are considered closed upon submission of the DOE F 5639.3 form to OAMSS. Completion reports must be forwarded to OAMSS within 30 working days.
  - (d) Requests for time extensions for submitting completion/final reports must be submitted in writing to OAMSS and provide justification for the extension.
  - (e) For employees who have an access authorization, a sanitized (unclassified) copy of the DOE F 5639.3 form will be placed in the employee's DOE/NNSA personnel security file. If an employee does not have an access authorization, it will be placed in the employee's personnel file.
- (11) Criteria for Taking Administrative/Disciplinary Action.
- (a) Federal management/supervisors are responsible for taking disciplinary action in accordance with DOE Order 3750.1.
  - (b) Contractor management/supervisors are responsible for taking disciplinary action in accordance with their respective company procedures.
  - (c) The party or parties responsible for an incident of security concern must be subject to appropriate administrative actions, including disciplinary measures, retraining, counseling, or other directed actions necessary to reduce the likelihood or recurrence of the incident.
  - (d) Corrective actions must be documented in the inquiry report for all Incidents of Security Concern. When no disciplinary action is deemed necessary or required, it is to be documented on the inquiry report for all Incidents of Security Concern.
  - (e) Individual supervisors are responsible for administrative/disciplinary actions when the individual(s)' responsibility for a security incident has been determined and one of the following factors is evident:
    - 1 Deliberate disregard of security requirements.
    - 2 Gross negligence in the handling of classified matter.

## INCIDENTS OF SECURITY CONCERN

NSO O 470.X4  
2-9-09

8

---

- 3 Not deliberate in nature, but involves a pattern of negligence or carelessness.
  - 4 Breaches of any other provision of Safeguards and Security Policies and procedures, as applicable are apparent.
- (f) Administrative/disciplinary action may include, but is not limited to, counseling, reprimand, suspension without pay, forfeiture of pay, removal, discharge, loss or denial of access to classified information, and withdrawal of Derivative Classifier authority. Coordination should be made with the organization's Human Resources and/or Personnel Office before any action is taken. **NOTE:** According to DOE M 470.4-1, Chapter I, paragraph 8a, whenever possible, the responsibility for an incident is fixed upon an individual rather than upon a position or office. When individual responsibility cannot be established and the facts show that a responsible official allowed conditions to exist that led to an incident of security concern, responsibility must be assigned to the official.
- e. Employees. Reports any knowledge about a potential security incident to the OAMSS FSO. Examples of incidents that must be reported include, but not limited to:
- (1) Improper escorting of uncleared personnel in a security area.
  - (2) Leaving classified matter unattended.
  - (3) Leaving a repository open at the end of the workday or unattended.
  - (4) Failure to properly protect security keys or combinations of repositories.
  - (5) Transmitting classified matter over nonsecure computing system or fax machine.
  - (6) Improperly transmitting sensitive matter (Official Use Only or Unclassified Controlled Nuclear Information).
  - (7) Allowing foreign national access without proper approval.
  - (8) Discussing classified information over nonsecure telephones.
  - (9) Discussing classified information in the presence of or within hearing distance of unauthorized persons.

## INCIDENTS OF SECURITY CONCERN

NSO O 470.X4  
2-9-09

9

(10) Violation of NNSA/NSO Prohibited Articles Policy.

### 6. DEFINITIONS.

- a. Incident Identification. Incidents of Security Concern are identified as actions, inactions, or events that have occurred at NNSA/NSO which:
  - (1) Pose threat to national security interests and/or critical DOE/NNSA assets.
  - (2) Create potentially serious or dangerous security situations.
  - (3) Potentially endanger the health and safety of the workforce or public (excluding safety-related items).
  - (4) Degrade the effectiveness of the Safeguards and Security Program.
  - (5) Adversely impact the ability of organizations to protect DOE/NNSA Safeguards and Security interests.
- b. IMI-1. Actions, inactions, or events that pose the most serious threats to national security interests and/or critical DOE/NNSA assets, create serious security situations, or could result in deaths in the workforce or general public. See Table 1, Reportable Categories of Incidents of Security Concern, IMI-1, in DOE M 470.4-1.
- c. IMI-2. Actions, inactions, or events that pose threat to national security interests and/or critical DOE/NNSA assets or that potentially create dangerous situations. See Table 2, Reportable Categories of Incidents of Security Concern, IMI-2, in DOE M 470.4-1.
- d. IMI-3. Actions, inactions, or events that pose threats to DOE/NNSA security interests or that potentially degrade the overall effectiveness of the Department's Safeguards and Security Protection Program. See Table 3, Reportable Categories of Incidents of Security Concern, IMI-3, in DOE/NNSA M 470.4-1.
- e. IMI-4. Actions, inactions, or events that could pose threats to DOE/NNSA by adversely impacting the ability of organizations to protect DOE/NNSA Safeguards and Security interests. See Table 4, Reportable Categories of Incidents of Security Concern, IMI-4, in DOE M 470.4-1.

INCIDENTS OF SECURITY CONCERN

NSO O 471.X  
2-9-09

10

---

7. REFERENCES.

- a. DOE M 470.4-1, SAFEGUARDS AND SECURITY PROGRAM PLANNING AND MANAGEMENT, dated 8-26-05, and Changes thereto.
  - b. DOE Order 3750.1, WORK FORCE DISCIPLINE, dated 3-23-83, and Changes thereto.
  - c. Form DOE F 471.1, *Security Incident Notification Report*.
  - d. Form DOE F 5639.3, *Report of Security Incident/Infraction*.
8. CONTACT. Questions concerning this Order should be addressed to OAMSS at 702-295-1594.



*Stephen A. Mellington*  
Stephen A. Mellington  
Manager

## INCIDENTS OF SECURITY CONCERN

NSO O 470.X4  
2-9-09

Attachment 1  
Page 1 (and 2)

---

### CONTRACTORS REQUIREMENTS DOCUMENT (CRD)

1. This CRD establishes the requirements for the National Nuclear Security Administration Nevada Site Office (NNSA/NSO) contractors, National Laboratories, other federal agencies, and other user organizations whose contracts involve Incidents of Security Concern. This directive applies to NNSA/NSO-related facilities only.
2. Regardless of the performer of the work, the contractor, National Laboratory, other federal agency, and other user organization is responsible for complying with the requirements of this CRD. The contractor, National Laboratory, other federal agency, and other user organization is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure compliance with the requirements.
3. The contractor must implement and comply with this directive, as provided by NNSA/NSO for all activities involving incidents of security concern; compliance with this directive is monitored by NNSA/NSO.