U.S. Department of Energy
Washington, D.C.

NOTICE

DOE N 471.3

Approved: 4-13-01
Expires: 4-13-02

SUBJECT: REPORTING INCIDENTS OF SECURITY CONCERN

1. OBJECTIVE. This Notice is designed to enhance the Department of Energy (DOE) Incidents of Security Concern Reporting Program through more consistent reporting, better information tracking, and interactive coordination. These procedures will reduce the amount of security incident reporting by (a) eliminating 15-day update reports, (b) placing Group 5 Occurrence Reporting Processing System (ORPS) reporting subjects into the incident reporting program, (c) eliminating the need to send inquiry reports on less sensitive incidents to Headquarters, and (d) providing a regular Headquarters-to-field feedback process. This Notice will also streamline initial and follow-up reporting and improve field/Headquarters coordination on incident inquiry status.

2. CANCELLATION. Deputy Secretary Glauthier memorandum, subject: Reporting Security Incidents, dated 9-7-99.

3. APPLICABILITY.

   a. DOE Elements. This Notice applies to all DOE elements, including the National Nuclear Security Administration.

   b. Contractors. This Notice is intended to apply to all DOE contractors. Contractor requirements are listed in the Contractor Requirements Document (CRD), Attachment 1. Compliance with the CRD is required to the extent set forth in a contract.

4. REQUIREMENTS. See paragraph 7 for definitions of terms used in this Notice.

   a. 24-hour Determination/Categorization Period. When an incident is suspected to have occurred, the facility where the incident occurred has 24 hours to examine and document all pertinent facts and circumstances to determine whether an incident has occurred. During this period, the incident must be categorized by an Impact Measurement Index (IMI) Number. If it is determined that an incident of security concern did not occur, no further action is required.

   b. Initial Incident Reporting. Initial incidents of security concern reports will be sent to Headquarters using DOE Form 471.1, *Security Incident Notification Report,* through the responsible field element, through the DOE Emergency Operations Center (EOC). Initial security incident reports should be forwarded using the following criteria:

      (1) Within 1 hour following categorization for the most serious security incidents determined to be IMI-1(see attachment 2), the originating site/facility will transmit a

DOE Form 471.1 to the DOE EOC. Verbal notification may be made, then followed-up with the transmission of DOE Form 471.1.

(2) Within 8 hours following categorization of security incidents determined to be IMI-2/3, the originating site/facility will transmit a DOE Form 471.1 to the DOE EOC.

Upon receipt of DOE F 471.1, the Headquarters EOC will immediately notify the lead program secretarial office, the Office of Defense Nuclear Security, and the Office of Safeguards and Security. Further notifications, if necessary, will be accomplished by the Office of Safeguards and Security (i.e., other secretarial offices, other government agencies, or foreign governments).

c. Incident/Inquiry Update Reporting. Only initial reports will be transmitted to the EOC. All other reports pertaining to a security incident (i.e., inquiry reports, status updates, and other related activities) will be transmitted directly to the Office of Safeguards and Security, which will inform all other affected parties.

d. Report Updates. Security incident and inquiry update status will be provided as follows:

(1) Final Inquiry Reports and Special Updates. Inquiry officials will forward final inquiry reports to the Office of Safeguards and Security through the responsible field element within 30 working days of categorization of the incident. If the inquiry cannot be completed within 30 working days, a status report that describes actions taken and an estimated date of completion will be submitted. These reports will be reviewed by the Office of Safeguards and Security and a determination made as to final status of the incident as either closed or requiring further inquiry (i.e., open). Inquiry reports for IMI-4 incidents do not have to be provided to the Office of Safeguards and Security.

(2) Monthly Update (Headquarters Feedback). The Office of Safeguards and Security will send a summary of recorded incident and inquiry status to respective operations office and facility incident points of contact and program secretarial offices, preferably via e-mail, during the last week of each month. New closures during the current month and all open incidents will be reflected in the monthly update. This monthly update will be used to ensure that Headquarters and the field element maintain accurate, coordinated, and reconciled incident/inquiry status information.

(3) Monthly Incident Compilations. Each site/facility will maintain a compilation of IMI-4 incidents. These monthly summaries will be provided to the Office of Safeguards and Security.

NOTE: The above update procedures eliminate the need for more frequent field-to-Headquarters incident inquiry updates; that is, updates at 15-day intervals. This interactive approach is intended to ensure information accuracy and reduce field reporting workloads. Special notifications should be provided at any time to improve progress or understanding on an incident.

e. Related but Separate Reporting.

(1) Occurrence Reporting Processing System (ORPS). To eliminate reporting redundancy and centralize the reporting of security-related occurrences, all occurrences within the Group 5 - Safeguards and Security category once contained in DOE M 232.1-1A are now incorporated into this Notice. If an event does not meet the criteria for reporting as an incident of security concern, it does not negate the reporting responsibilities as an Occurrence Report under DOE M 232.1-1A.

(2) DOE O 151.1A, COMPREHENSIVE EMERGENCY MANAGEMENT SYSTEM. Incidents that are reportable under the provisions of DOE O 151.1A should continue to be reported in accordance therewith. Reporting procedures for DOE incidents of security concern do not alter DOE O 151.1A requirements.

(3) Flash Reporting. DOE/NV, DOE/OAK, and DOE/AL "Flash Reporting" procedures are not affected by DOE incidents of security concern reporting requirements.

f. Inquiry Report Content/Closure Considerations. At a minimum, inquiry reports must describe the conduct and results of the inquiry process. The following minimum information must be addressed in the inquiry report to consider the incident closed:

(1) An executive summary.

(2) A narrative, which must include the following:

(a) WHEN. The report must state the date and time of incident discovery, any notifications, the incident inquiry, and other time-related elements depicting any actions taken on the incident.

(b) WHERE. The report must include all data pertinent to the location of an incident, including the facility name and facility code (as registered in the Safeguards and Security Information Management System), building/room numbers, and other identifying information as appropriate. Such information is required for the facility responsible for the incident and any other facilities affected by the incident.

(c) WHAT. The report must completely discuss the facts and circumstances surrounding the incident, including all supportive information, such as the following:

1 A detailed description of the incident of security concern.

2 Identification of all personnel involved in the incident and when they were notified, including those associated with the inquiry process (i.e., inquiry officials and assisting personnel).

3 Identification of the causes for the incident (direct and contributing factors) and a description of the mitigating or aggravating factors that may reduce or increase the impact of the incident.

4 Descriptions of the actions that precipitated the incident.

5 Descriptions of all physical evidence, including all records/documents reviewed (e.g., training records, policy/procedures, personnel security files, etc.).

6 Results of any interviews performed.

7 Descriptions of actions taken to minimize vulnerabilities created by the incident and prevent further loss/compromise of the security interest.

8 If the incident involves classified information, the following information should be included:

- Describe the potentially compromised classified matter, to include, but not be limited to, classification level, category, caveats (if any), and form of information (e.g., document title, date, description). A copy of the evidence (or photograph) must be retained and provided to Headquarters if requested.
- Identify the classification guide and topic, or source document, including date, that apply (e.g., classification determination).
- Identify known recipients of potentially compromised matter.
- Identify owner of the classified information (e.g., program office or other government agency).

(3) Attachments. Attachments to the report of inquiry must include—

(a) a copy of the documentation appointing the inquiry official;

(b) a copy of any signed statements of involved individuals;

(c) a description of the compromised or potentially compromised information (as appropriate);

(d) a copy of the DOE F 471.1, *Security Incident Notification Report*, and other documents obtained during the data collection phase of the inquiry; and

(e) a copy of any DOE F 5639.3, *Report of Security Incident/Infraction*, or a form comparable in content, issued as a result of the inquiry, must also be submitted once it is completed.

(4) Conclusion. An inquiry officer's conclusion and the basis/facts that support the conclusion are essential. Given the facts determined through the inquiry, the conclusion of the final report must address the potential risk to the security interest based upon a subjective analysis of the facts and circumstances surrounding the incident of security concern. Identification of management officials responsible for corrective action(s) and disciplinary action(s) as applicable must be included.

g. Corrective actions identified in response to an incident of security concern must be documented and, for incidents at IMI-1, -2, or -3 levels, a copy forwarded to the Office of Safeguards and Security. Corrective actions for IMI-4 incidents are not required to be forwarded to the Office of Safeguards and Security.

5. RESPONSIBILITIES.

a. Office of Security and Emergency Operations (SO), through the Office of Security Affairs (SO-20).

(1) Develops and maintains policies, guidance, and training for the incident of security concern program.

(2) Maintains a centralized database for incidents of security concern to conduct trending and analysis, provide summary incident reporting, and develop lessons learned for distribution.

(3) Provides all required internal DOE Headquarters and external notifications and distributions for incidents of security concern, as necessary.

b. Administrator, National Nuclear Security Administration. Establishes procedures, in accordance with this Notice, to ensure prompt reporting of any significant problem, abuse, violation of law or Executive order, or deficiency relating to the management of classified information by personnel of the Administration.

c. Field Elements and the Office of Safeguards and Security, Headquarters Operations Division.

(1) Ensure implementing procedures for the provisions of this Notice are established at facilities or activities for which they are responsible.

(2) Ensure that incidents of security concern are reported in accordance with this Notice.

d. Deputy Administrator for Naval Reactors. Due to the dual-agency (Navy/DOE) nature of the Naval Nuclear Propulsion Program as described in Executive Order 12344 (set forth in Public Law 106-65), the Deputy Administrator for Naval Reactors will implement this Notice as appropriate for the Naval Nuclear Propulsion Program.

6. CONTACT. Questions concerning this Notice should be addressed to the Program Manager, Technical and Operations Security, Office of Safeguards and Security, at 301-903-2528.

7. DEFINITIONS.

a. Incidents of security concern, as defined in Attachment 2, are any actions or inactions, that—

(1) pose an immediate danger or short- or long-term threat to national security interests and/or critical DOE assets, that potentially create a serious security situation, or that create high-visibility media interest;

(2) pose long-term threats to DOE security interests or that potentially degrade the overall effectiveness of the Department's protection program; and

(3) in combination and over time, adversely impact the level of security awareness and program responsiveness necessary to protect DOE's security interests.

b. Impact Measurement Index Number. Incidents of Security Concern are categorized as follows, in accordance with their potential to cause serious damage to or place security

interests and activities at risk. An IMI is determined based on the safeguards and security situation at the time the incident occurred. The IMI is used to identify, track, and evaluate each security incident or combination of incidents.

(1) IMI-1. Any security incident that can be expected to cause serious damage to national security or DOE security interests.

(2) IMI-2. Any security incident that can be expected to cause damage to national security or DOE security interests.

(3) IMI-3. Any security incident with a low probability of causing damage to national security or DOE security interests.

(4) IMI-4. Any security incident that causes no damage to national security, but that can, in combination, indicate weakened security awareness or inadequate procedures and practices.

8. REFERENCES.

a. DOE O 151.1A, COMPREHENSIVE EMERGENCY MANAGEMENT SYSTEM, dated 11-01-00.

b. DOE M 232.1-1A, OCCURRENCE REPORTING AND PROCESSING OF OPERATIONS INFORMATION, dated 7-21-97.

SPENCER ABRAHAM
Secretary of Energy

CONTRACTOR REQUIREMENTS DOCUMENT

DOE N 471.3, REPORTING INCIDENTS OF SECURITY CONCERN

1. RESPONSIBILITIES. Department of Energy (DOE) contractors shall—

   a. ensure implementing procedures for the provisions of this Notice are established at facilities or activities for which they are responsible and

   b. ensure that incidents of security concern are reported in accordance with this Notice.

2. REQUIREMENTS.

   a. 24-hour Determination/Categorization Period. When an incident is suspected to have occurred, the contractor office responsible for the facility where the incident occurred has 24 hours to examine and document all pertinent facts and circumstances to determine whether an incident has occurred. During this period, the incident must be categorized by an Impact Measurement Index (IMI) Number. If it is determined that an incident of security concern did not occur, no further action is required.

   b. Initial Incident Reporting. Initial incidents of security concern reports will be sent to Headquarters using DOE Form 471.1, *Security Incident Notification Report,* through the responsible field element, through the DOE Emergency Operations Center (EOC). Initial security incident reports should be forwarded using the following criteria:

      (1) Within 1 hour following categorization for the most serious security incidents determined to be IMI-1 (see DOE N 471.3, attachment 2), the originating site/facility will transmit a DOE Form 471.1 to the DOE EOC. Verbal notification may be made, then followed-up with the transmission of DOE Form 471.1.

      (2) Within 8 hours following categorization of security incidents determined to be IMI-2/3, the originating site/facility will transmit a DOE Form 471.1 to the DOE EOC.

   c. Incident/Inquiry Update Reporting. Only initial reports will be transmitted through the EOC. All other reports pertaining to a security incident (i.e., inquiry reports, status updates, and other related activities) will be transmitted to the Office of Safeguards and Security.

   d. Status Updates. Security incident and inquiry update status will be provided to the Office of Safeguards and Security as follows:

      (1) Final Inquiry Reports and Special Updates. Contractor inquiry officials will forward final inquiry reports to the Office of Safeguards and Security through the responsible field element within 30 working days of categorization of the incident. (Procedures

for the appointment of inquiry officials are currently described in DOE O 470.1). If the inquiry cannot be completed within 30 working days, a status report that describes actions taken and an estimated date of completion will be submitted. These reports will be reviewed by the Office of Safeguards and Security and a determination made as to final status of the incident as either closed or requiring further inquiry (i.e., open). Inquiry reports for IMI-4 incidents do not have to be provided to the Office of Safeguards and Security.

(2) Monthly Incident Compilations. Each site/facility will maintain a compilation of IMI-4 incidents. These monthly summaries will be provided to the Office of Safeguards and Security.

e. Inquiry Report Content/Closure Considerations. At a minimum, inquiry reports must describe the conduct and results of the inquiry process. The following minimum information must be addressed in the inquiry report to consider the incident closed:

(1) An executive summary.

(2) A narrative, which must include the following information:

(a) WHEN. The report must state the date and time of incident discovery, any notifications, the incident inquiry, and other time-related elements depicting any actions taken on the incident.

(b) WHERE. The report must include all data pertinent to the location of an incident, including the facility name and facility code (as registered in the Safeguards and Security Information Management System), building/room numbers, and other identifying information as appropriate. Such information is required for the facility responsible for the incident and any other facilities affected by the incident.

(c) WHAT. The report must completely discuss the facts and circumstances surrounding the incident, including all supportive information, such as the following:

1 A detailed description of the incident of security concern.

2 Identification of all personnel involved in the incident and when they were notified, including those associated with the inquiry process (i.e., inquiry officials and assisting personnel).

3 Identification of the causes for the incident (direct and contributing factors) and a description of the mitigating or aggravating factors that may reduce or increase the impact of the incident.

4 Descriptions of the actions that precipitated the incident.

5 Description of all physical evidence, including all records/documents reviewed (e.g., training records, policy/procedures, personnel security files, etc.).

6 Results of any interviews performed.

7 Descriptions of actions taken to minimize vulnerabilities created by the incident and prevent further loss/compromise of the security interest.

8 If the incident involves classified information, the following information should be included:

- Describe the potentially compromised classified matter, to include, but not be limited to, classification level, category, caveats (if any), and form of information (e.g., document title, date, description). A copy of the evidence (or photograph) must be retained and provided to Headquarters if requested.
- Identify the classification guide and topic, or source document, including date, that apply (e.g., classification determination).
- Identify known recipients of potentially compromised matter.
- Identify owner of the classified information (e.g., Program Office or other Government Agency).

(3) Attachments. Attachments to the report of inquiry must include—

(a) a copy of the documentation appointing the contractor inquiry official;

(b) a copy of any signed statements of involved individuals;

(c) a description of the compromised or potentially compromised information (as appropriate); and

(d) a copy of the DOE F 471.1, *Security Incident Notification Report*, and other documents obtained during the data collection phase of the inquiry; and

(e) a copy of any DOE F 5639.3, *Report of Security Incident/Infraction*, or a form comparable in content, issued as a result of the inquiry, which must also be submitted once it is completed.

(4) Conclusion. An inquiry officer's conclusion and the basis/facts that support the conclusion are essential. Given the facts determined through the inquiry, the conclusion of the final report must address the potential risk to the security interest based upon a subjective analysis of the facts and circumstances surrounding the incident of security concern. Identification of management officials responsible for corrective action(s) and disciplinary action(s) as applicable must be included.

g. Corrective actions identified in response to an incident of security concern must be documented and, for incidents at IMI-1, -2, or -3 levels, a copy forwarded to the Office of Safeguards and Security. Corrective actions for IMI-4 incidents are not required to be forwarded to the Office of Safeguards and Security.

Reportable Categories of Incidents of Security Concern

Impact Measurement Index (IMI-1)

A. Incidents that pose an immediate danger or short-term threat to national security interests and/or critical Department of Energy assets, potentially create a serious security situation, or create high visibility media interest.

DOE Order 151.1A, COMPREHENSIVE EMERGENCY MANAGEMENT SYSTEM, and facility emergency management plans, may require more stringent reporting times for IMI-1 type incidents than listed herein. Shorter reporting times should be determined on an individual incident basis and applied accordingly.

	Report within 1 hour	Report within 8 hours	Report monthly
Confirmed or suspected loss, theft, or diversion of a nuclear device or components.	X		
Confirmed or suspected loss, theft, diversion, or unauthorized release of weapon data.	X		
Confirmed or suspected loss, theft, or diversion of Category I/II quantities of Special Nuclear Materials (SNM).	X		
Confirmed or suspected loss, theft, diversion, unauthorized release of TOP SECRET information, Special Access Program (SAP) information, or Sensitive Compartmentalized Information (SCI).	X		
Confirmed or suspected intrusions, hacking or break-ins into DOE computer systems containing TOP SECRET, SAP, or SCI information	X		
Confirmed or suspected physical intrusion attempts or attacks against DOE facilities containing critical nuclear devices, materials, information, or assets	X		
Confirmed or suspected attacks against DOE federal and contractor employees that adversely impact a facility's or site's security posture.	X		
Confirmed or suspected acts or attempts of terrorist-type actions.	X		
Any security incident that could create immediate high-visibility media attention or create a situation requiring high-level Departmental management intervention.	X		
Validated threat notifications, via any medium or source, that immediately endanger personnel health or safety and that could require immediate protective force/law enforcement intervention.	X		
Confirmed or suspected acts of sabotage occurring at any DOE facility that places the safety or security of personnel, facilities, or the public at risk.	X		

Impact Measurement Index (IMI-2)

B. Incidents that pose a near- or long-term threat to national security interests and/or critical Department of Energy assets or that potentially create a crisis or dangerous situation.

	Report within 1 hour	Report within 8 hours	Report monthly
Suspected loss, theft, or diversion of any non-SNM radioactive, sensitive, or dangerous materials that could pose a health threat or endanger security.		X	
Confirmed or suspected intrusions, hacking or break-ins into DOE computer systems containing SECRET or CONFIDENTIAL information.		X	
Any amount of SNM found in an exceptionally dangerous/unaccounted storage environment or unapproved mode of transportation/transfer.		X	
Alarms or other loss detection indicators, excluding inventory differences or shipper-receiver differences for Category I or II material balance areas that cannot be proven to be false within 24 hours.		X	
Confirmed or suspected unauthorized disclosure, loss/potential loss of SECRET matter via any medium, method, or action.		X	
Actual or suspected technical interceptions of any level of classified information.		X	
Actions, electronic, physical, or by other methods, that interfere with any DOE safeguards and security practices.		X	
Validated threat notifications, via any media or source, that do not appear to immediately threaten personal safety or health.		X	
Loss of classified information that must be reported to other Government agencies or foreign associates.		X	
Unsecured classified repositories of any type including safes, doors, or other protective encasements, that contain TOP SECRET, SAP, SCI information.		X	
The loss of any DOE classified interest that requires State or local government or other Federal agency notification.		X	

Impact Measurement Index (IMI-3)

C. Incidents that could pose long-term threats to Department of Energy security interest or that potentially degrade the overall effectiveness of the Department's protection program.

	Report within 1 hour	Report within 8 hours	Report monthly
A shipper-receiver difference involving a gain in the number of items for which the additional items total to a Category I or II quantity of SNM.		X	
Bomb-related incidents at any DOE nuclear or non-nuclear facility including location of a suspected device.		X	
Confirmed or suspected unauthorized disclosure, loss/potential loss of CONFIDENTIAL matter via any medium, method, or action.		X	
Confirmed or alleged noncompliance with laws or Departmental standards that jeopardizes the protection of the facility or site security interests.		X	
Demonstrations or protestors that cause site and facility damage.		X	
Labor strikes that could degrade or interfere with required protection for the facility's or site's protection responsibilities.		X	
Physical violence or threat of retaliation against facility security personnel.		X	
Dangerous weapons and firearms-related incidents involving protective force operations/personnel (i.e., accidental weapons discharge, personal wounding).		X	
Loss or theft of DOE firearms, per DOE O 473.2, PROTECTIVE FORCE PROGRAM.		X	
Unplanned/unscheduled power outages that cause a disruption/degradation of physical security systems and that would allow unauthorized or undetected access to access controlled/protected areas.		X	
Inventory differences exceeding alarm limits in Category I/II/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.		X	
Incidents involving the attempted or actual introduction of controlled and prohibited items (e.g., weapons, drugs, explosive devices, recording equipment, cameras, etc.) into Limited, Exclusion, Protected or Material Access Areas.		X	
Discovery of malicious activities, disorderly conduct, or vandalism that disrupts facility activities or causes damage between $10K and $100K.		X	

Impact Measurement Index (IMI-4)

D. Incidents that, in combination and over time, could pose a long-term threat to Department of Energy security interests by adversely impacting the level of security awareness and program responsiveness necessary to protect the Department's security interests.

	Report within 1 hour	Report within 8 hours	Report monthly
Identified SNM inventory differences beyond alarm limits in a Category IV SNM material balance area.			X
Significant shipper/receiver differences that exceed 200 grams of fissile material and the combined limit of error for the shipment.			X
Alarms or other loss detection indicators, excluding inventory differences and shipper/receiver differences, that involve a Category III or IV quantity of nuclear material.			X
Confirmed or suspected unauthorized disclosure of UCNI, Export Control, and NNPI information via any medium, method or action.			X
Non-credible bomb threats at any DOE nuclear or non-nuclear facility.			X
Unsecured classified repositories of any type including safes, doors, or other protective encasements in which no likely classified disclosure occurred. See 1-hour and 8-hour reporting for TOP SECRET, SAP, or SCI information involvement.			X
Peaceful demonstrations or protests that do not threaten facility or site security interests or activities.			X
Lapses in administrative procedures contributing to the misuse, misprocessing, or maintenance of security badges and passes.			X
Loss of security badges in excess of 5 percent of total issued during 1 calendar year.			X
Lapses in administrative procedures contributing to the mismanagement or faulty application of the DOE PSAP and PAP programs.			X
Lapses in administrative procedures contributing to security problems with foreign visitors.			X
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 greater than 8 hours, such incidents will be handled as a suspected compromise in accordance with its classification level and category.			X
The blatant misuse of a security badge or pass to circumvent established access control procedures into a security area.			X
Inexplicably high rate/amount of loss or theft of Government property.			X