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

ORDER

DOE O 471.4

Approved: 3-17-04
Review: 3-17-06
Expires: 3-17-08

SUBJECT: INCIDENTS OF SECURITY CONCERN

1. OBJECTIVES. To set forth requirements for the Department of Energy (DOE) Incidents of Security Concern Program, including timely identification and notification of, response to, inquiry into, reporting of, and closure actions for incidents of security concern.

2. CANCELLATIONS. The directives listed below are cancelled. All policy memorandums relating to the Incidents of Security Concern Program issued before the date of this Order have been incorporated. Cancellation of a directive does not, by itself, modify or otherwise affect any contractual obligation to comply with the directive. Cancelled directives incorporated by reference in a contract remain in effect until the contract is modified to delete the references to the requirements in the cancelled directives.

   a. DOE O 470.1, *Safeguards and Security Program*, dated 9-28-95, Chapter VII, "Incidents of Safeguards and Security Concern."

   b. DOE N 471.3, *Reporting Incidents of Security Concern,* dated 4-13-01.

   c. DOE M 471.2-1B, *Classified Matter Protection and Control Manual,* dated 1-6-99, Chapter IV. (Note: Paragraphs 1 and 2 of Chapter III remain in effect.)

3. APPLICABILITY.

   a. Primary DOE Organizations, Including National Nuclear Security Administration Organizations. Except for the exclusions in paragraph 3.c., this Order applies to all Primary DOE Organizations, listed on Attachment 1. This Order automatically applies to Primary DOE Organizations created after the date it is issued.

   b. Site/Facility Management Contracts.

      (1) The Contractor Requirements Document (CRD), Attachment 2, sets forth requirements of this Order that will apply to contractors responsible for the management and operation of Department-owned facilities (hereafter referred to as site/facility management contractors) whose contracts include the CRD.

      (2) This CRD must be included in all site/facility management contracts that contain the clause at 48 CFR 952.204-2, *Security*. This Order does not automatically apply to other than site/facility management contracts.

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of Security

(3) Application of any of the requirements of this Order to other than site/facility management contracts will be communicated separately from this Order. (See paragraph 5., Responsibilities.)

(4) The officials identified in paragraph 5., Responsibilities, are responsible for notifying contracting officers of which contracts are affected. Once notified, contracting officers are responsible for incorporating the CRD into affected contracts through the laws, regulations, and DOE directives clause of the affected contracts.

(5) As the laws, regulations, and DOE directives clause of site/facility management contracts states, regardless of the performer of the work, the site/facility management contractors with the CRD incorporated into their contracts are responsible for compliance with the requirements of the CRD.

(a) Affected site/facility management contractors are responsible for flowing down the requirements of the CRD to subcontracts at any tier to the extent necessary to ensure the site/facility management contractors' compliance with the requirements.

(b) Contractors must not unnecessarily or imprudently flow down requirements to subcontractors. That is, contractors will:

1 ensure that they and their subcontractors comply with the requirements of the CRD; and

2 incur only costs that would be incurred by a prudent person in the conduct of competitive business.

c. Exclusions. Consistent with the responsibilities identified in Executive Order 12344, *Naval Nuclear Propulsion Program*, dated 2-1-82, the Director, Naval Nuclear Propulsion Program, will determine the applicability of this Order for activities and facilities under his control.

4. REQUIREMENTS. The broad-based requirements for implementing this Order are listed below with elaboration provided in associated chapters. Additionally, there may be instances where security incidents are required to be reported through other department reporting systems (e.g., cyber, Occurrence Reporting and Processing System).

a. Implementation Plans.

(1) If implementation of this Order cannot be accomplished within 6 months of the effective date of this Order, a local implementation plan must be developed.

(2) If required, implementation plans must be developed and submitted for approval to the Office of Security through the Head of the appropriate Primary DOE Organization within 90 days of the effective date of this Order. In the case of the NNSA, implementation plans must be developed and submitted through the Administrator to the Deputy Secretary within 90 days of the effective date of this Order. (The Deputy Secretary may choose to request a review of the plans by the Office of Security).

(3) Plans must ensure that implementation of this Order is accomplished within 1 year of the effective date of this Order.

b. Deviations from the requirements in this Order must be processed in accordance with DOE O 470.1, paragraph 4.f.

c. Any person who observes, finds, or has knowledge or information about a potential incident of security concern must immediately report this information to the Facility Security Officer (FSO) or designee of the facility where the incident occurred. The FSO or designee must make notifications as specified in Chapter I, paragraph 3, of this Order.

d. Any person discovering a potential incident of security concern, including one that involves classified matter; special nuclear material (SNM), including material protected, controlled, and accounted for as SNM; or other security interests at risk (e.g., interests not properly controlled), must make reasonable efforts to safeguard the security interests in an appropriate manner. He/she must also ensure evidence associated with the incident is not tampered with or destroyed.

e. Any person discovering actual or suspected fraud, waste, or abuse of government resources must report such incidents to the Office of the Inspector General in accordance with DOE O 221.1, *Reporting Fraud, Waste, and Abuse to the Office of Inspector General*, dated 3-22-01.

f. Locally developed procedures must be established, documented, approved by the Head of the appropriate Primary DOE Organization, and disseminated to ensure the identification, reporting, root cause analysis, and resolution of incidents of security concern. These procedures must also identify guidelines for corrective actions and documentation of time and funds expended on incidents.

g. Inquiries must be conducted to establish the facts and circumstances surrounding an incident of security concern.

h. Appropriate Federal (to include Office of Security), state, and local organizations must be contacted when a violation is suspected or discovered.

i. Appropriate corrective actions must be taken for each incident of security concern to reduce the likelihood of recurrence of the incident, including review and/or revision of applicable safeguards and security plans and procedures.

j. 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 of recurrence of the incident.

k. Any disciplinary or adverse actions involving DOE employees must be conducted according to DOE 3750.1, *Work Force Discipline,* dated 3-23-83.

5. RESPONSIBILITIES.

a. Heads of Primary DOE Organizations. Attachment 1 contains a list of the Primary DOE Organizations to which this Order is applicable. Heads of those organizations must:

(1) Ensure facilities under their cognizance have implemented this Order.

(2) Notify contracting officers of site/facility management contracts that must include the CRD of this Order.

(3) Ensure procurement requests for new non-site-/non-facility-management contracts require inclusion of appropriate language, including the clause at 48 CFR 952.204-2, *Security*, and this Order's CRD in the resulting contracts, if necessary.

(4) Provide sufficient resources for the reporting of incidents, the conduct of inquiries, and the implementation of corrective actions.

(5) Assist in inquiries when requested.

(6) Conduct damage assessments as required in Chapter II of this Order.

(7) Ensure corrective actions are implemented to prevent recurrence of incidents of security concern.

(8) Ensure notification is made to the Office of Security when an incident of security concern is confirmed or suspected. Examples of the most serious incidents include (a) intentional infliction or threat of death or serious physical harm to DOE/NNSA officials and personnel; (b) penetrations of classified automated information systems; (c) threats of terrorism, sabotage, or malevolent acts against DOE/NNSA nuclear facilities; (d) technical intercept of classified or unclassified sensitive information; (e) loss/failure to account for, theft of, or diversion of SNM, nuclear weapons and their components, tritium, plutonium, or precious metals; (f) loss or compromise of Top Secret (TS) information or material; (g) loss or compromise of Special Access Program (SAP) information or material;

and (h) loss or compromise of Sensitive Compartmented Information (SCI).

b. Office of Security.

(1) Develops and maintains policies, guidance, and training for the Incidents of Security Concern Program.

(2) Initiates inquiries, when necessary, and monitors the status of inquiries into incidents of security concern such as intentional infliction or threat of death or serious physical harm to DOE/NNSA officials and personnel; penetrations of classified automated information systems; threats of terrorism, sabotage, or malevolent acts against DOE/NNSA nuclear facilities; technical intercept of classified or unclassified sensitive information; loss/failure to account for, theft of, or diversion of SNM, nuclear weapons and their components, tritium, plutonium, or precious metals; loss or compromise of TS information or material; loss or compromise of SAP information or material; and loss or compromise of SCI.

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

(4) Serves as the focal point for all incidents of security concern originating at HQ.

(5) Serves as the primary liaison with other Federal agencies, including but not limited to the Federal Bureau of Investigation (FBI) and the Office of the Inspector General, for incidents of security concern. Liaison activities for incidents involving a foreign nexus will be handed over to the Office of Counterintelligence (OCI)/Office of Defense Nuclear Counterintelligence (ODNCI).

(6) Provides all required internal DOE HQ and external notifications and distributions for incidents of security concern, as necessary. When there exists a suspicion of foreign activity and/or involvement with a security concern, the security concern will be forwarded to OCI/ODNCI.

(7) Ensures timely classification/declassification reviews of information involved in incidents of security concern when requested.

(8) Notifies OCI/ODNCI when an incident is the result of a deliberate compromise and a foreign nexus is involved.

c. Administrator, National Nuclear Security Administration. Establishes procedures, in accordance with this Order, to ensure prompt reporting of incidents of security concern, including but not limited to any significant problem, abuse, violation of law or Executive order, or deficiency relating to the management of classified information by NNSA personnel.

d. National Nuclear Security Administration, Office of Nuclear Safeguards and Security Programs. Assists in the conduct of inquiries when required, and participates in joint inquiries with the Office of Security when appropriate.

e. Deputy Administrator for Naval Reactors. Because of the dual-Agency (Navy/DOE) nature of the Naval Nuclear Propulsion program, as described in Executive Order 12344, *Naval Nuclear Propulsion Program,* dated 2-1-82, and set forth in Public Law 106-65, the Deputy Administrator for Naval Reactors will implement this Order as appropriate for the Naval Nuclear Propulsion Program.

f. Under Secretary for Energy, Science and Environment. Establishes procedures, in accordance with this Order, to ensure prompt reporting of incidents of security concern, including but not limited to any significant problem, abuse, violation of law or Executive order, or deficiency relating to the management of classified information by DOE personnel under his cognizance.

g. General Counsel. Provides resources for timely legal advice and assistance regarding incidents of security concern.

h. Office of Independent Oversight and Performance Assurance. Validates and verifies the management and implementation of the Incidents of Security Concern Program as part of the Independent Safeguards and Security Oversight Program.

i. Office of Counterintelligence/Office of Defense Nuclear Counterintelligence (when directed by the Administrator, NNSA).

(1) Processes inquiries where there is a suspicion of foreign activity.

(2) Provides support as appropriate to the conduct of inquiries.

(3) Notifies the appropriate security offices upon the discovery of security incidents during the course of counterintelligence activities.

(4) Provides criteria to local site security incident investigations personnel to assist them in identifying specific security incident reports that local counterintelligence officers would have an interest in reviewing.

j. Office of Intelligence. For incidents involving SCI and SCI facilities, the Office of Intelligence:

(1) ensures the implementation of procedures for the provisions of this Order;

(2) ensures incidents of security concern are reported in accordance with this Order;

(3) ensures inquiries are conducted and documented to establish all the facts and circumstances surrounding incidents of security concern;

(4) assists with inquiries conducted by the Office of Security upon request;

(5) provides sufficient resources for conducting inquiries and implementing corrective actions;

(6) coordinates with the Office of Security, FBI, the Office of the Inspector General, and State and local law enforcement agencies for incidents of security concern, as appropriate;

(7) coordinates with OCI/ODNCI on incidents of security concern suspected of having foreign activity and/or involvement; and

(8) approves in writing the designation of inquiry officials.

k. Managers of Operations/Field/Area/Regional Offices; Site Offices; Service Centers Directors; and Director, Office of Headquarters Security Operations.

(1) Designate individuals to be responsible for alerting contracting officers of the applicable requirements in the CRD, including supporting details for each procurement. [Unless another individual is designated, the responsibility is that of the procurement request originator (the individual responsible for initiating the request on the DOE F 4200.33, "Procurement Request-Authorization").]

(2) Develop and submit implementation plans as required.

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

(4) Ensure incidents of security concern are reported in accordance with this Order.

(5) Ensure inquiries are conducted and documented to establish all the facts and circumstances surrounding incidents of security concern.

(6) Ensure corrective actions are taken to reduce the likelihood of recurrence of incidents of security concern.

(7) Assist with inquiries conducted by the Office of Security, when requested.

(8) Provide sufficient resources for conducting inquiries and corrective actions.

(9) Coordinate with the FBI, the Office of the Inspector General, and State and local law enforcement agencies for incidents of security concern, as appropriate.

(10) Approve in writing the designation of inquiry officials.

l. Contracting Officers.

(1) After notification by the appropriate program official, incorporate the CRD into affected site/facility management contracts in accordance with the laws, regulations, and DOE directives clause of the contracts.

(2) Assist procurement request originators who want to incorporate the clause at 48 CFR 952.204-2, *Security*, and the requirements of the CRD of this Order in new non-site-/non-facility-management contracts, as appropriate.

6. CONTACT. Questions concerning this Order should be directed to the Office of Security at 202-586-3345.

BY ORDER OF THE SECRETARY OF ENERGY:

KYLE E. McSLARROW
Deputy Secretary

CONTENTS

Chapter I. Identification and Reporting Requirements

1. General I-1
2. Incident Identification and Categorization I-1
   Table 1. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 1 (IMI-1) I-3
   Table 2. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 2 (IMI-2) I-4
   Table 3. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 3 (IMI-3) I-5
   Table 4. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 4 (IMI-4) I-7
3. Reporting Requirements I-8
   Figure 1. Incidents of Security Concern I-10
4. Inquiry Officials I-14
5. Federal, State, or Local Law Enforcement Personnel I-15
6. Conduct of Inquiries I-16
   Figure 2. Example Chain-of-Custody Form I-17
7. Inquiry Report Content/Closure Considerations I-19
8. Administrative Actions I-21
9. Records Retention I-21

Chapter II. Incidents of Security Concern Involving Compromise or Potential Compromise of Classified Information

1. Inquiries into Potential Compromise of, Compromise of, or Missing Classified Information II-1
2. Damage Assessments II-2
3. Conduct of Damage Assessments II-3
4. Procedures II-3
5. Content of Damage Assessment Reports II-3
6. Combining Similar Incidents II-4
7. Cases Involving Other Government Agency Information II-4

CONTENTS (continued)

8. Cases Involving Foreign Government Information II-4

9. Joint Damage Assessment with Another Government Agency II-5

ATTACHMENT 1. DOE ORGANIZATIONS TO WHICH DOE O 471.4, *INCIDENTS OF SECURITY CONCERN,* IS APPLICABLE

ATTACHMENT 2. CONTRACTOR REQUIREMENTS DOCUMENT

CHAPTER I. IDENTIFICATION AND REPORTING REQUIREMENTS

1. GENERAL.

   a. A system of controls and procedures must be developed, approved, implemented, enforced, and maintained:

      (1) to deter, detect, and prevent incidents of security concern;

      (2) for the timely identification and notification of, inquiry into, analysis of, and reporting of incidents of security concern.

   b. Inquiries must be used to determine the root causes and individuals responsible for incidents of security concern.

   c. All discussions and documents associated with an incident of security concern must be classified or controlled according to current classification or control guidance and following procedures contained in appropriate Department of Energy (DOE) directives.

2. INCIDENT IDENTIFICATION AND CATEGORIZATION. DOE uses a graded approach for identification and categorization of incidents of security concern. This approach provides a framework for the requirements of reporting timelines and the level of detail for inquiries into and root cause analysis of specific security incidents. By establishing a graded approach, line management can effectively allocate the resources necessary to implement this Order based on the severity of security incidents. The following paragraphs provide the basis for identification and categorization of incidents of security concern.

   a. Incident Identification. Incidents of security concern are actions, inactions, or events that have occurred at a site that:

      (1) pose threats to national security interests and/or critical DOE 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, or

      (5) adversely impact the ability of organizations to protect DOE safeguards and security interests.

b. Incident Categorization. Incidents of security concern are categorized in accordance with their potential to cause serious damage or place safeguards and security interests and activities at risk. Four categories of security incidents have been established based on the relative severity of the incident. Each of the four categories is identified by an impact measurement index (IMI) number as follows (from most severe to least severe): IMI-1, IMI-2, IMI-3, and IMI-4. Each of the four categories is further subdivided into specific subcategories based on the security topical areas of physical security, protective forces, information security, personnel security, and nuclear material control and accountability. The categorization of specific security incidents occurs at the time the security incident is discovered. The categorization of specific security incidents can change based on information developed during the inquiry into the incident.

c. Impact Measurement Index (IMI). The IMI number is used to identify, trend, and evaluate each security incident or combination of incidents. (Specific information to be used to categorize incidents of security concern is contained in Table 1 through Table 4; however, the IMI subcategories contained in these tables are not all inclusive and if they overlap, the more stringent reporting category will apply.) The basis for each IMI category is provided below.

(1) 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. [See Table 1, Reportable Categories of Incidents of Security Concern, Impact Measurement Index 1 (IMI-1).]

(2) IMI-2. Actions, inactions, or events that pose threats to national security interests and/or critical DOE assets or that potentially create dangerous situations. [See Table 2, Reportable Categories of Incidents of Security Concern, Impact Measurement Index 2 (IMI-2).]

(3) 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. [See Table 3, Reportable Categories of Incidents of Security Concern, Impact Measurement Index 3 (IMI-3).]

(4) 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. [See Table 4, Reportable Categories of Incidents of Security Concern, Impact Measurement Index 4 (IMI-4).]

Table 1. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 1 (IMI-1)

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.

DOE O 151.1B, *Comprehensive Emergency Management System,* dated 10-29-03, and facility emergency management plans may require more stringent reporting times for IMI-1 type incidents than listed here. Shorter reporting times should be determined on an individual incident basis and applied accordingly.

Incident Type	Report within 1 hour	Report within 8 hours	Report monthly
1. Confirmed or suspected loss, theft, or diversion of a nuclear device or components.	X		
2. Confirmed or suspected loss, theft, diversion, or unauthorized disclosure of weapon data.	X		
3. Confirmed or suspected loss, theft, or diversion of Category I or II quantities of special nuclear material (SNM).	X		
4. A shipper-receiver difference involving a loss in the number of items which total a Category I or II quantity of SNM.	X		
5. Confirmed or suspected loss, theft, diversion, unauthorized disclosure of Top Secret (TS) information, Special Access Program (SAP) information, or Sensitive Compartmented Information (SCI), regardless of the medium, method, or action resulting in the incident.	X		
6. Confirmed or suspected intrusions, hacking, or break-ins into DOE computer systems containing TS information, SAP information, or SCI.	X		
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.	X		
8. Confirmed or suspected attacks against DOE Federal and contractor employees that adversely impact a facility's or site's security posture.	X		
9. Confirmed or suspected acts or attempts of terrorist-type actions.	X		
10. Confirmed threats that immediately endanger personnel health or safety and may require immediate protective force/law enforcement intervention.	X		
11. Dangerous weapons and firearms-related incidents involving protective force operations/personnel where an individual is killed, wounded, or an intentional discharge occurs.	X		
12. Confirmed or suspected acts of sabotage, at any DOE facility, that place the safety or security of personnel, facilities, or the public at risk.	X		
13. Confirmed compromise of root/administrator privileges in DOE unclassified computer systems that have a significant possibility of being contaminated with TS information, SAP information, or SCI.	X		
14. Confirmed compromise of root/administrator privileges in DOE computer systems containing Secret or Confidential information.	X		
15. Confirmed intrusions into information systems containing classified information.	X		
16. Instances of malicious code that cause disruption, degradation, or compromise of information systems for an entire site/facility.	X		
17. Instances of malicious code that allow unauthorized or undetected access to information systems containing classified information (Top Secret, Secret, Confidential, SAP information, or SCI).	X		

Table 2. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 2 (IMI-2)

IMI-2 Actions, inactions, or events that pose threats to national security interests and/or critical DOE assets or that potentially create dangerous situations.

Incident Type	Report within 1 hour	Report within 8 hours	Report monthly
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.		X	
2. Confirmed or suspected intrusions, hacking, or break-ins into DOE computer systems containing Secret or Confidential classified information.		X	
3. Any amount of SNM found in an exceptionally dangerous/hazardous unapproved storage environment, or unapproved mode of transportation/transfer.		X	
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.		X	
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.		X	
6. Confirmed or suspected unauthorized disclosure, loss, or potential loss of Secret matter regardless of the medium, method, or action resulting in the incident.		X	
7. Actual or suspected technical interceptions of any level of classified information.		X	
8. Actions, by electronic or physical means, that interfere with any DOE safeguards and security practices.		X	
9. Notifications, by any media or source, of validated threats that do not appear to immediately threaten personal safety or health.		X	
10. Loss of classified information that must be reported to other Government agencies or foreign organizations.		X	
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.		X	
12. The loss of any DOE classified interest that requires state or local government or other Federal agency notification.		X	
13. Confirmed compromise of root/administrator privileges in DOE unclassified computer systems.		X	
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.		X	
15. Potential compromise of root/administrator privileges in DOE computer systems containing classified information.		X	
16. Instances of malicious code that cause disruption/degradation or compromise of information systems dedicated to safety, security, or critical operations.		X	
17. Detection of activities involving individuals who have been confirmed as physically watching/casing/surveilling a site in an effort to gather information to aid in the conduct of a terrorist-type attack.		X	

Table 3. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 3 (IMI-3)

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.			
Incident Type	Report within 1 hour	Report within 8 hours	Report monthly
1. 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 special nuclear material (SNM).		X	
2. Bomb-related incidents at any DOE facility, including location of a suspected device.		X	
3. Confirmed or suspected unauthorized disclosure, loss, or potential loss of Confidential matter by any medium, method, or action.		X	
4. Confirmed or alleged noncompliance with laws or DOE directives/standards that jeopardizes protection of the facility or site security interests.		X	
5. Demonstrators or protestors that cause site and facility damage.		X	
6. Labor strikes that could degrade or impede the required protection of the facility or site.		X	
7. Physical violence or threat of retaliation against facility security personnel.		X	
8. Dangerous weapons and firearms-related incidents involving protective force operations/personnel where an accidental weapon discharge occurs.		X	
9. Loss or theft of DOE firearms, per DOE O 473.2, *Protective Force Program,* dated 6-30-00.		X	
10. 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.		X	
11. 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 sensitive information.		X	
12. Confirmed or suspected malicious activities, including but not limited to stealing badges or vehicle licenses.		X	
13. Discovery of malicious activities, disorderly conduct, or vandalism that disrupts facility activities or causes damage between $10K and $100K.		X	
14. Circumvention of established access control procedures into a security area (excluding Property Protection Area).		X	
15. 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.		X	
16. A shipper-receiver difference involving a loss in the number of items which total a Category III or IV quantity of SNM.		X	
17. Confirmed or suspected loss, theft, or diversion of Category III or IV quantities of SNM.		X	
18. Intrusion attempts into information systems containing classified information.		X	
19. Confirmed intrusions into unclassified information systems that are not publicly available (e.g., behind a firewall).		X	

Table 3. continued

Incident Type	Report within 1 hour	Report within 8 hours	Report monthly
20. 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).		X	
21. Unauthorized network scans/probes on information systems possessing classified information.		X	
22. Incidents of apparent surveillance of facilities or operations (studying, photographing, low over-flights, outsiders questioning employees or protective force, unusual calls for information, etc.).		X	

Table 4. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 4 (IMI-4)

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.

Incident Type	Report within 1 hour	Report within 8 hours	Report monthly
1. 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.			X
2. Significant shipper-receiver differences that exceed 200g of fissile material and the combined limit of error for the shipment.			X
3. 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.			X
4. 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.			X
5. 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.			X
6. Non-credible bomb threats at any DOE nuclear or non-nuclear facility.			X
7. 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.			X
8. Peaceful demonstrations or protests that do not threaten facility or site security interests or activities.			X
9. Failure to adhere to established procedures contributing to the misuse or misprocessing of or failure to maintain security badges and passes.			X
10. Loss of security badges in excess of 5 percent of total issued during 1 calendar year.			X
11. Failure to adhere to established procedures contributing to the mismanagement or faulty application of the DOE Personnel Security Assurance Program, Personnel Assurance Program or Human Reliability Program.			X
12. Failure to adhere to established administrative procedures contributing to problems with foreign visitors.			X
13. Classified information sent by 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 offline, 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.			X
14. Unauthorized cellular phones and personal digital assistants introduced into a Limited Area, Protected Area, or Material Access Area, where there is no potential for compromise of classified or sensitive information.			X
15. Circumvent established access control procedures into a Property Protection Area.			X
16. High rate/amount of loss (excluding natural disasters) or theft of Government property.			X

3. REPORTING REQUIREMENTS.

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. (See Figure 1, Incidents of Security Concern.) During this period, the suspected incident must be categorized by an IMI number. If it is determined that an incident of security concern did not occur, no further action is required.

b. Initial Incident Reporting. Incidents of security concern initial reports for IMI-1, IMI-2, and IMI-3 (as well as those for IMI-4 involving foreign nationals, per paragraph 3.d. below) will be sent to the DOE HQ Operations Center (OC) using DOE F 471.1, "Security Incident Notification Report," in accordance with locally developed procedures approved by the responsible element. Initial security incident reports will be forwarded based on the following criteria.

(1) Within 1 hour following categorization for security incidents determined to be IMI-1 (see Table 1), the originating site/facility will transmit a DOE F 471.1 to the DOE HQ OC. If a verbal notification of the incident is made to the DOE HQ OC, a follow-up transmission of the DOE F 471.1 to the DOE HQ OC must be made.

(2) Within 8 hours following categorization of security incidents determined to be IMI-2/IMI-3 (see Tables 2 and 3), the originating site will transmit a DOE F 471.1 to the DOE HQ OC. If a verbal notification of the incident is made to the DOE HQ OC, a follow-up transmission of the DOE F 471.1 to the DOE HQ OC must be made.

c. Reporting Incidents Receiving Media Attention. In addition to the IMI reporting time frames, the Office of Security must be notified within 8 hours of any security incidents that have been or will be reported in the media. The initial DOE F 471.1 and any subsequent updates must clearly identify the fact of media reporting.

d. Reporting Incidents Associated with Foreign Nationals. Security incidents having any association with foreign nationals will be clearly identified and reported on the initial DOE F 471.1 and subsequently in any related update or follow-on activity pertaining to the incident, including incidents categorized as IMI-4. For security incidents involving any credible information that a foreign national or an agent of a foreign power is involved, the closest element of the Office of Counterintelligence (OCI)/Office of Defense Nuclear Counterintelligence (ODNCI) will be notified.

e. Numbering Incidents and Changing Categories. When the initial incident report (i.e., DOE F 471.1) is transmitted, it is to include a local incident tracking number. All subsequent reports pertaining to a security incident (e.g., inquiry and

other related activities) will be transmitted to the Office of Security. Changes in IMI categorizations require resubmission of a DOE F 471.1 to the Office of Security.

f. Reporting Incidents Associated with Sensitive Programs. Only the initial DOE F 471.1 will be required for incidents involving activities associated with sensitive programs. These programs will include the Sensitive Compartmented Information (SCI) Program, Special Access Programs (SAPs), Technical Surveillance Countermeasures Program, Counterintelligence Program, or other programs identified by the Office of Security. All subsequent reporting will be handled "within channels" until such time as the inquiry report has been distributed. The date of the inquiry report will be transmitted to the Office of Security for database entry.

g. Closing Inquiries.

(1) IMI-1 and IMI-2 incidents are considered closed upon completion of the inquiry report. The inquiry report must be completed within 60 working days of the incident categorization or a status report must be provided in accordance with paragraph 3.k.(1), below.

(2) IMI-3 incidents are considered closed upon completion of DOE F 5639.3, "Report of Security Incident/Infraction" (except for completing the section on assignment and acceptance of the security infractions), transmission of the completed DOE F 5639.3 to the Office of Security, and completion of actions required in local procedures.

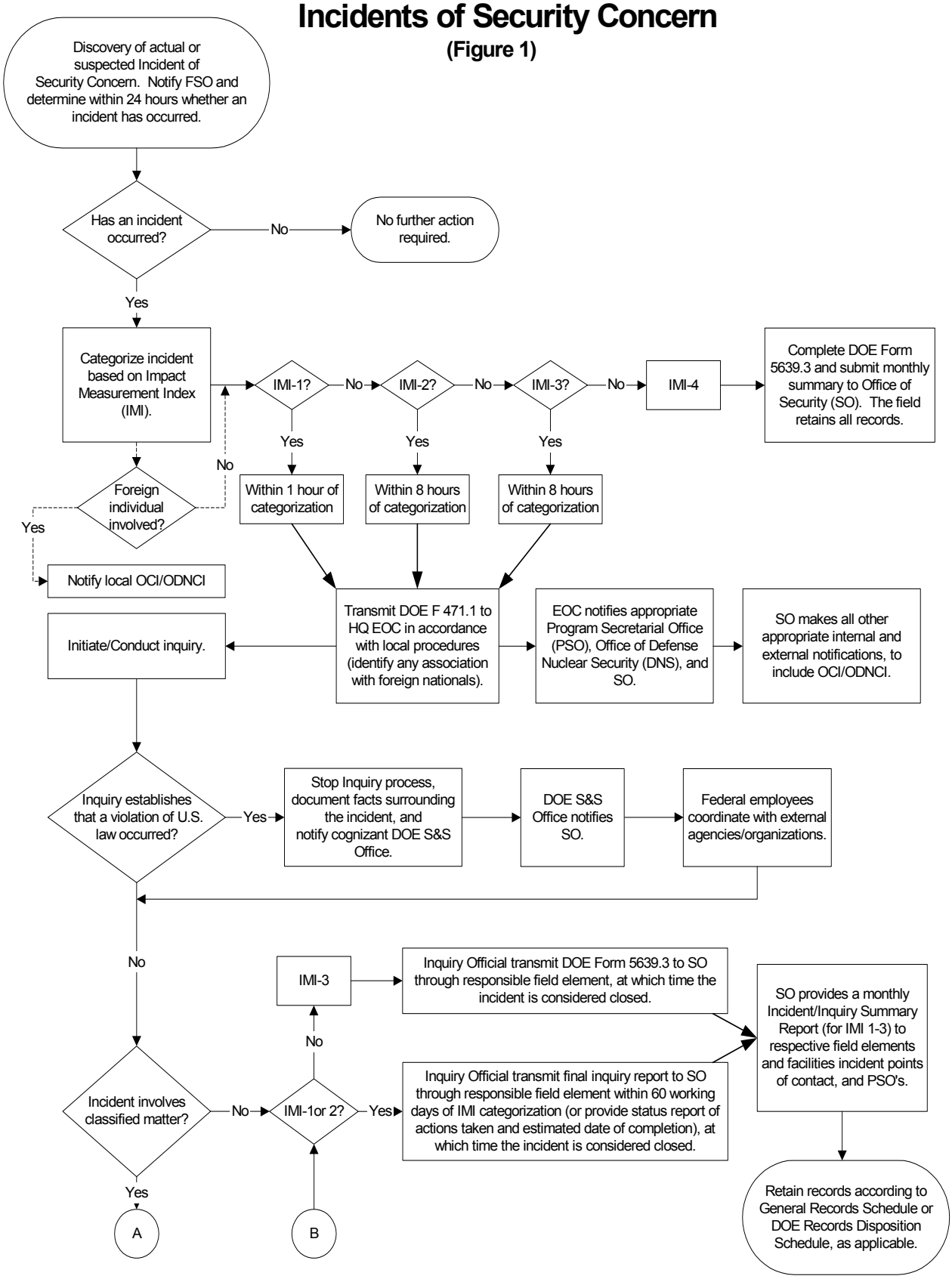
(3) IMI-4 incidents are considered closed upon completion of the DOE F 5639.3 or associated local procedures.

(4) A sanitized (unclassified) copy of the DOE F 5639.3 will be provided to the local personnel security office for placement in the appropriate personnel security file.

h. Final Inquiry Reports. Inquiry officials will forward final inquiry reports in accordance with local procedures to appropriate management for action and to the Office of Security.

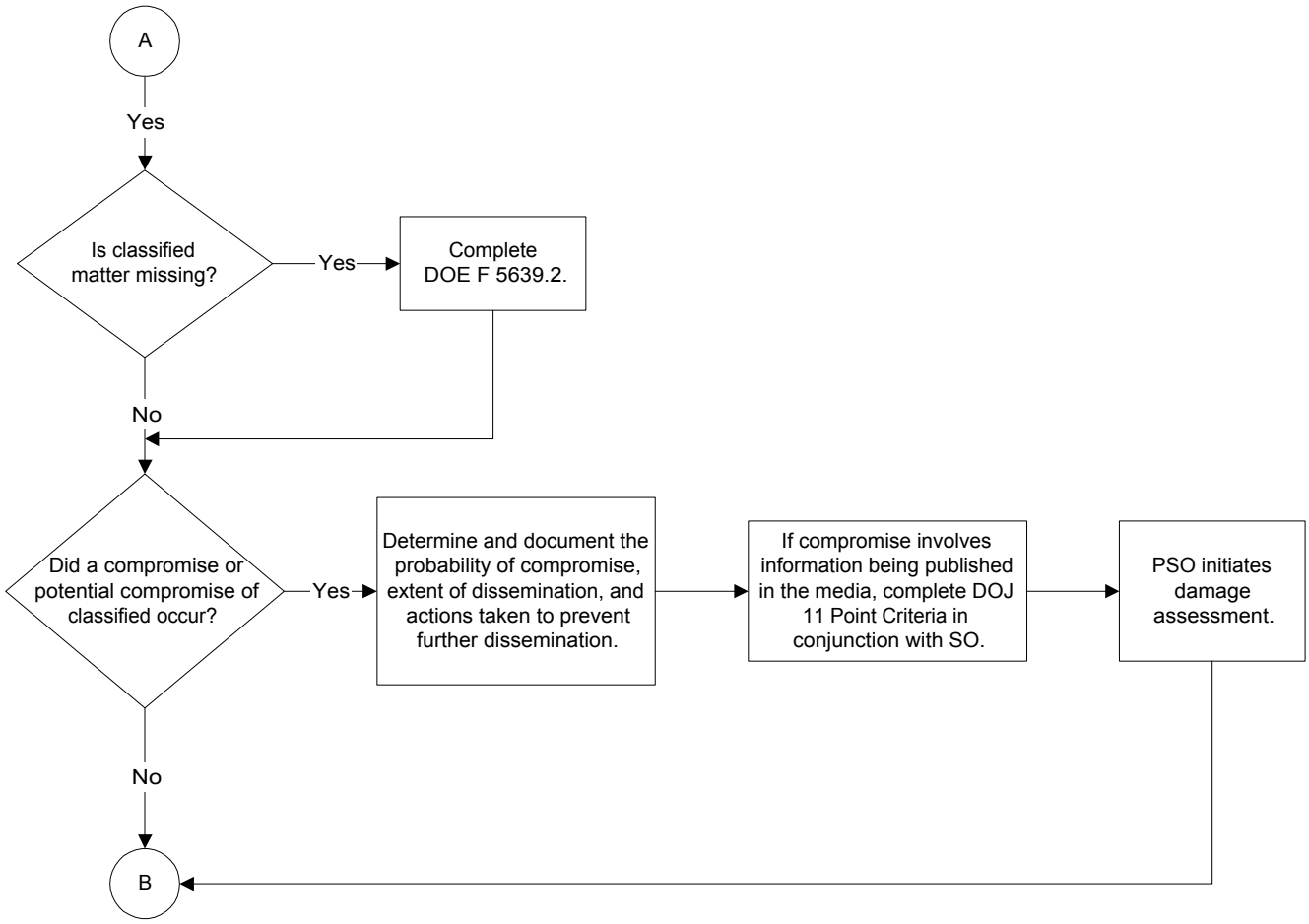
Incidents of Security Concern

(Figure 1)



Incidents of Security Concern

(Figure 1 continued)



i. Office of Security Monthly Incident Summary Report. By the 10th working day of each month, the Office of Security will e-mail a summary status report of the previous month's recorded incidents and inquiries to field element/facility incident points of contact and Primary DOE Organizations.

(1) New closures during the current month and all open incidents will be reflected in the monthly update.

(2) These monthly updates will be used to ensure the Office of Security and the field elements maintain accurate, coordinated, and reconciled incident/inquiry status information.

j. Status/Summary Reports.

(1) IMI-1 and IMI-2. A monthly status report will be provided to the Office of Security and the Primary DOE Organization for IMI-1 and IMI-2 incidents that have not been closed within 60 working days of notification of the incident.

(a) Status reports will consist of the original DOE F 471.1, completed and planned actions, identification of issues precluding closure, and estimated date of closure.

(b) Status reports are due by the fifth working day of each month.

(2) IMI-3. Status reports are not required for IMI-3 incidents.

(3) IMI-4. Each facility will maintain 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, will be provided to the Office of Security. If no reportable incidents occurred during the calendar month, a summary stating this will be forwarded to the Office of Security by the fifth working day of each month.

k. Separate but Related Reporting.

(1) Occurrence Reporting Processing System. To eliminate reporting redundancy and centralize the reporting of security-related occurrences, all occurrences previously reported within the "Group 5—Safeguards and Security" category once contained in cancelled DOE M 232.1-1A, *Occurrence Reporting and Processing of Operations Information,* dated 7-21-97, are now incorporated into this Order. Because an event meets the criteria for reporting as an incident of security concern does not negate the responsibility to report it as an occurrence under DOE O 231.1A,

Environment, Safety, and Health Reporting, dated 8-19-03 (i.e., event affects both safety and security).

(2) DOE O 151.1B, *Comprehensive Emergency Management System,* dated 10-29-03. Incidents that are reportable under the provisions of DOE O 151.1B must continue to be reported in accordance with the Order. Reporting procedures for DOE incidents of security concern do not alter DOE O 151.1B requirements.

(3) Flash Reporting. National Nuclear Security Administration "Flash Reporting" procedures are not affected by Departmental incidents of security concern reporting requirements.

(4) Special Reporting Situations. Under certain circumstances, related incidents of security concern, that are anticipated to recur over a long period of time, may be consolidated into single monthly reports. This situation will be handled on a case-by-case basis between the site, the responsible Primary DOE Organization, and the Office of Security. Specific plans for this reporting process will be developed by the site and submitted through the responsible Primary DOE Organization to the Office of Security.

l. Documenting Corrective Actions. Corrective actions identified in response to an incident of security concern must be documented. For incidents categorized as IMI-1, IMI-2, or IMI-3, a copy of the documentation must be forwarded to the Office of Security if this information is not included in the inquiry report. Documentation on corrective actions for IMI-4 incidents does not have to be forwarded to the Office of Security.

m. Reporting to Congress. Section 3150 of the Defense Authorization Act requires the Secretary of Energy to notify the Committees on Armed Services of the Senate and House of Representatives of each "significant nuclear defense intelligence loss." A "significant nuclear defense intelligence loss" is defined in the Defense Authorization Act as "any national security or counterintelligence failure or compromise of classified information at a facility of the Department or operated by a contractor of the Department that the Secretary considers likely to cause significant harm or damage to the national security interest of the United States."

(1) The Department regards the loss or compromise (i.e., disclosure of classified information to unauthorized persons) of Top Secret information; SCI; SAP information; and Weapons Data Sigmas 1, 2, 14, and 15 as reportable under Section 3150.

(2) Within 30 days of discovery of Section 3150 reportable incidents, the Office of Security, after consultation with the Director, Central

Intelligence, and the Director, Federal Bureau of Investigation (FBI), must provide notification to Congress.

4. INQUIRY OFFICIALS.

a. Inquiry officials will conduct inquiries to establish the pertinent facts and circumstances surrounding incidents of security concern.

b. Inquiry officials may be either Federal or contractor employees but must have previous investigative experience or Department inquiry training and must be knowledgeable of appropriate laws, Executive orders, Departmental directives, and/or regulatory requirements.

(1) Contractors may conduct inquiries into incidents of security concern; however, if a violation of law is determined or suspected or the inquiry establishes information that a foreign power or an agent of a foreign power is involved, the contractor must stop further inquiry actions and notify the cognizant Departmental safeguards and security office, which will assume further notification and reporting responsibilities, to include coordination with OCI/ODNCI. In such instances, the contractor must document the known circumstances surrounding the incident of security concern and submit all accumulated data to the cognizant Departmental safeguards and security office.

(2) In all instances where the cognizant Departmental safeguards and security office disagrees with the contractor report, the cognizant Departmental safeguards and security office assumes supplemental inquiry responsibilities.

(3) When the inquiry into an incident of security concern necessitates communication with Agencies/organizations external to the Department (e.g., the U.S. Postal Service, the FBI, or other Federal agencies), a Federal employee must be responsible for performing all such communication.

(4) Contact with Federal, state, and local law enforcement officials may be made by contractors with the written concurrence of the head of the field element.

c. Inquiry officials are not authorized to detain individuals for interviews nor to obtain sworn statements; however, they may conduct consensual interviews and obtain signed statements.

d. Inquiry officials must be appointed in writing by the head of the field element, the head of the Office of Headquarters Security Operations, or the Office of Security.

e. Inquiry officials are responsible for conducting the inquiry and maintaining records and documentation associated with the inquiry (e.g., logs of events, notes, recordings, and statements).

f. When inquiry officials discover suspected or confirmed violations of law, they will immediately notify the Office of Security.

5. FEDERAL, STATE, OR LOCAL LAW ENFORCEMENT PERSONNEL.

a. If a violation of law has occurred and the preservation of evidence requires the immediate notification of Federal, state, or local law enforcement agencies (e.g., theft of special nuclear material, homicide, assault, location or detonation of an explosive device), the cognizant DOE safeguards and security office will perform all necessary referrals and notifications, including notification to the Office of Security. The Office of Security will notify the HQ elements of all appropriate Federal agencies, including the FBI.

b. Federal, State, or local law enforcement agency personnel requiring access to limited areas or higher for investigative actions must be escorted, have a current access authorization passed to DOE, or possess an active DOE access authorization. Such personnel will be approved for access to classified matter only if they possess the appropriate access authorization, the matter directly pertains to the investigation, and appropriate programmatic approvals have been granted if such approvals are required. Access to Restricted Data and Formerly Restricted Data will require a DOE Q or L or appropriate access authorization.

c. When authorized and approved Federal, state, or local law enforcement personnel are given access to classified information, they will be immediately advised of the classification level and category. They will also be informed of the protection and control requirements associated with the classified information they possess.

d. When an inquiry establishes information that a foreign power or an agent of a foreign power is involved, the Office of Security must immediately notify OCI/ODNCI, which in turn will notify the FBI in accordance with 50 U.S.C. 402a.

e. When an inquiry surrounding an incident of security concern establishes information indicating that fraud, waste, or abuse has occurred, the Office of the Inspector General must be notified for information and/or action.

f. The cognizant DOE safeguards and security office must make arrangements for the issuance of standard DOE security badges, the granting of access to classified information, and any other necessary agreements or items requested or required by Federal, state, or local law enforcement agencies involved in investigations.

6. CONDUCT OF INQUIRIES.

a. If an incident affects more than one site/facility, the following criteria must be used in determining the lead organization responsible for conducting the inquiry.

(1) If the sites/facilities fall under the purview of a single field element, that field element must assign responsibility to a lead organization.

(2) If the sites/facilities fall under the purview of multiple field elements, those field elements must, by mutual agreement, decide on a lead organization with responsibility for the inquiry.

b. The following actions must be taken when conducting inquiries into incidents of security concern and be reflected in the inquiry report. (See Chapter II for additional requirements.)

(1) Data Collection.

(a) Collect all data/information relevant to the incident, such as operations logs, inventory reports, requisitions, receipts, photographs, signed statements, etc.

(b) Conduct interviews to obtain additional information regarding the incident.

(c) Collect physical evidence associated with the inquiry, if available. (Examples of physical evidence include, but are not limited to, recorder charts, computer hard drives, defective/failed equipment, procedures, readouts from monitoring equipment, etc.)

(d) Ensure physical evidence is protected and controlled and a chain-of-custody is maintained. (See Figure 2. Example Chain-of-Custody Form.)

(2) Incident Reconstruction.

(a) Reconstruct the incident of security concern to the greatest extent possible using collected information and other evidence.

(b) Develop a chronological sequence of events that describes the actions preceding and following the incident.

(c) Identify persons associated with the incident.

Figure 2. Example Chain-of-Custody Form

EVIDENCE/PROPERTY CUSTODY DOCUMENT **For use of this form see ISC-301 Conduct of Inquiries Course Manual.** **Proponent is the DOE Computer Forensics Laboratory.**	DOE TRACKING NUMBER: CFL CASE NUMBER

RECEIVING ACTIVITY	LOCATION	
NAME, GRADE AND TITLE OF PERSON FROM WHOM RECEIVED ☐ OWNER ☐ OTHER	ADDRESS *(Including Zip Code)*	
LOCATION FROM WHERE OBTAINED	REASON OBTAINED	DATE/TIME OBTAINED

ITEM NO.	QUANTITY	DESCRIPTION OF ARTICLES *(Include model, serial number, condition and unusual marks or scratches)*

CHAIN OF CUSTODY

ITEM NO.	DATE	RELEASED BY	RECEIVED BY	PURPOSE OF CHANGE OF CUSTODY
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	

Figure 2. Example Chain-of-Custody (continued)

		CHAIN OF CUSTODY *(CONTINUED)*		
ITEM NO.	DATE	RELEASED BY	RECEIVED BY	PURPOSE OF CHANGE OF CUSTODY
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	

FINAL DISPOSAL ACTION

RELEASE TO OWNER OR OTHER (Name/Organization) _____

DESTROY _____

OTHER (Specify)

FINAL DISPOSAL AUTHORITY

ITEM(S)_____ON THIS DOCUMENT, PERTAINING TO THE INQUIRY/INVESTIGATION INVOLVING:

_____(IS)(ARE) NO LONGER
(Grade) *(Name)* *(Organization)*

REQUIRED AS EVIDENCE AND MAY BE DISPOSED OF AS INDICATED ABOVE. *(If articles must be retained do not sign, but explain in separate correspondence.)*

_____
(Typed/Printed Name, Grade, Title) *(Signature)* *(Date)*

WITNESS TO DESTRUCTION OF EVIDENCE

THE ARTICLE(S) LISTED AT ITEM NUMBER(S)_____(WAS) (WERE) DESTROYED BY THE EVIDENCE CUSTODIAN IN MY PRESENCE, ON THE DATE INDICATED ABOVE.

_____
(Typed/Printed Name, Grade, Title, Organization) *(Signature)* *(Date)*

(3) Incident Analysis and Evaluation. This analysis will determine which systems/functions performed correctly or failed to perform as designed; it must provide the basis for determining the cause of the incident and subsequent corrective actions.

(a) Analyze the information collected during the inquiry to determine whether it describes the incident completely and accurately.

(b) Collect additional data and reconstruct the incident if more information is required.

(c) Identify any collateral impact with other programs or security interests.

7. INQUIRY REPORT CONTENT/CLOSURE CONSIDERATIONS. At a minimum, inquiry reports must describe the conduct and results of the inquiry and include the following information for the incident to be closed.

a. An executive summary.

b. A narrative, which must include the following:

(1) The date and time of incident discovery, any notifications, the incident inquiry, and other time-related actions pertaining to the incident (WHEN).

(2) 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 (WHERE).

(3) A complete discussion of the facts and circumstances surrounding the incident, including a description of all supporting information (WHAT), such as the following:

(a) detailed description of the incident of security concern;

(b) 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);

(c) identification of the causes for the incident (direct and contributing factors) and descriptions of the mitigating or aggravating factors that may reduce or increase the impact of the incident;

(d) descriptions of the actions that precipitated the incident;

(e) descriptions of all physical evidence, including all records/documents reviewed (e.g., training records, policies/procedures);

(f) results of any interviews performed;

(g) descriptions of actions taken to minimize vulnerabilities created by the incident and prevent further loss/compromise of the security interest; and

(h) if the incident involves classified matter, the following must also be included:

1 a description of the potentially compromised classified matter, including but not limited to classification level, category, caveats (if any), and form (e.g., document title, date, and description). [A copy of the evidence (or photograph) must be retained and provided to HQ if requested.];

2 the classification guide and topic or source document, including date, of guide or source document;

3 known recipients of potentially compromised matter; and

4 owner of the classified matter (e.g., program office or other Government agency).

(4) An inquiry official's conclusion and the basis/facts that support the conclusion are essential.

(a) 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.

(b) The final report must also identify the management officials responsible for corrective actions and disciplinary actions.

c. The following must be included as attachments to the report of inquiry:

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

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

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

(4) a copy of the DOE F 471.1 and other documents obtained during the data collection phase of the inquiry;

(5) a copy of DOE F 5639.3, or a form comparable in content, issued as a result of the inquiry; and

(6) a copy of DOE F 5639.2, "Reporting Unaccounted for Documents," or a form comparable in content, if applicable.

8. ADMINISTRATIVE ACTIONS.

a. Whenever possible, the responsibility for an incident of security concern must be assigned to an individual rather than to a position or office.

(1) 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.

(2) Security infractions are issued to document the assignment of responsibility for an incident of security concern. Individuals who do not possess an access authorization may be issued a security infraction.

b. Corrective actions taken in response to incidents of security concern must be documented, and for incidents categorized as IMI-1, IMI-2, or IMI-3, a copy of the documentation must be forwarded to the Office of Security. Documentation of corrective actions for IMI-4 incidents does not have to be forwarded to the Office of Security.

c. A copy of Part 1 of DOE F 5639.3 or similar form will be placed in the employee's DOE personnel security file. If an employee does not have an access authorization, it will be placed in his/her personnel file.

9. RECORDS RETENTION.

a. Records pertaining to incidents of security concern cannot be sent to Federal Records Centers.

b. Records must be dispositioned in accordance with an applicable General Records Schedule, published by the National Archives and Records Administration (NARA), or in accordance with a DOE Records Disposition Schedule approved by NARA, whichever is applicable.

c. The site records manager or similarly titled person should be routinely consulted regarding the maintenance and disposition of records.

CHAPTER II. INCIDENTS OF SECURITY CONCERN INVOLVING COMPROMISE OR POTENTIAL COMPROMISE OF CLASSIFIED INFORMATION

1. INQUIRIES INTO COMPROMISE OF, POTENTIAL COMPROMISE OF, OR MISSING CLASSIFIED INFORMATION. The following requirements are in addition to those contained in Chapter I of this Order. Inquiry officials will perform, but not necessarily be limited to, the following actions.

   a. Query custodians and others having knowledge of the incident. When necessary, records must be audited for evidence of destruction, transmission, or other disposition.

   b. Ensure a DOE F 5639.2, or a form comparable in content, is completed if classified information is missing.

   c. Determine which Primary DOE Organization has programmatic responsibility for the information or whether the information was originated by another Government agency or foreign government.

   d. Determine whether a compromise or potential compromise occurred. If there was a potential compromise, seek to determine the probability of compromise. Document the basis for such findings (i.e., potential compromise is defined as an incident of security concern where circumstances exist that cannot rule out the compromise of classified information).

   e. If an inquiry determines that a compromise or potential compromise has occurred, document the extent of the dissemination of the classified information and the actions taken to prevent further dissemination.

   f. When an inquiry establishes that classified information has been compromised by being published in the media, the questions contained in the Department of Justice Eleven-Point Criteria, which are listed below, must be answered and coordinated with the Office of Security. When completing the questions, provide all documentation and appropriate information to support affirmative responses. Each question must be answered affirmatively before the Department of Justice will initiate a formal investigation into the compromise; however, failure to affirmatively answer all the Department of Justice criteria does not preclude the Department of Justice from pursuing administrative or criminal action.

      (1) Could the date and identity of the article or articles disclosing the classified information be provided?

      (2) Could specific statements in the article that are considered classified be identified? Was the data properly classified?

(3) Is the classified data that was disclosed accurate? If so, provide the name of the person competent to testify concerning the accuracy.

(4) Did the data come from a specific document, and, if so, what is the origin of the document and the name of the individual(s) responsible for the security of the classified data disclosed?

(5) Could the extent and official dissemination of the data be determined?

(6) Has it been determined that the data has not been officially released in the past?

(7) Has it been determined that prior clearance for publication or release of the information was not granted by proper authorities?

(8) Does review reveal that educated speculation on the matter cannot be made from material, background data, or portions thereof which have been published officially or have previously appeared in the press?

(9) Could the data be made available for the purpose of prosecution? If so, include the name of the person competent to testify concerning the classification.

(10) Has it been determined that declassification had not been accomplished prior to the publication or release of the data?

(11) Will disclosure of the classified data have an adverse impact on the national defense?

2. DAMAGE ASSESSMENTS. Damage assessments determine potential damage to national security when classified information has been compromised or potentially compromised. Damage assessments are conducted by security personnel to evaluate possible countermeasures and document actions to limit potential damage. The Primary DOE Organization will use the damage assessment to determine future courses of action within the program. Additionally, damage assessments are used by appropriate authorities when criminal prosecution is sought. Classification policy staff use damage assessments to revise classification guidance, if appropriate. Damage assessments will be conducted when:

a. inquiries disclose evidence that classified information, Weapons Data (Sigmas 1, 2, 14, and 15), SCI, or SAP data have been compromised or potentially compromised;

b. analysis reveals similar information has been compromised frequently or when the information has been compromised to a wide audience (e.g., public media, international conference, Internet);

c. a violation of laws appears to have occurred and criminal prosecution is contemplated; or

d. the Primary DOE Organization determines one is necessary.

3. CONDUCT OF DAMAGE ASSESSMENTS. The Primary DOE Organization with programmatic responsibility for the compromised or potentially compromised classified information must designate, in writing, a Federal employee responsible for conducting the damage assessment. He/she must also appoint an assessment team consisting of a derivative classifier and appropriate technical experts (e.g., experts in weapons design, nuclear policy, material production communications, intelligence, counterintelligence) to assist in assessing the value of the compromised information to foreign governments and/or hostile organizations.

4. PROCEDURES. The following procedures must be followed for all Departmental damage assessments.

a. The originator of the compromised information must provide the cognizant Departmental safeguards and security office with a copy of the compromised or potentially compromised information, if available. If no other copy exists, the originator must provide a detailed description of the compromised information.

b. The originator must coordinate with a derivative classifier to confirm the classification level and category of the compromised information according to current classification guidance and policy. The derivative classifier provides the basis from the classification determination (i.e., classification guide used).

c. The team performing the damage assessment must prepare a draft assessment and coordinate it with the originator of the compromised or potentially compromised information.

d. The damage assessment must be approved by the Primary DOE Organization with programmatic responsibility for the compromised or potentially compromised information, and at a minimum, copies will be submitted to the Director, Office of Security and the cognizant Departmental safeguards and security office responsible for the inquiry. The Director, Office of Security will coordinate with the Primary DOE Organization and distribute additional copies as appropriate.

5. CONTENT OF DAMAGE ASSESSMENT REPORTS. Damage assessment reports must contain the following information at a minimum:

a. identification of the source, date, and circumstances of the compromise or potential compromise;

b. classification of the specific information compromised or potentially compromised;

c. description of the specific information compromised or potentially compromised;

d. analysis and statement of the known or probable damage to national security that has resulted or may result;

e. assessment of the possible advantage to foreign governments and/or hostile organizations as a result of the compromise or potential compromise;

f. recommendation to Information Classification Control Policy regarding whether specific information or parts thereof must be:

(1) modified to minimize or nullify the effects of the reported compromise or potential compromise and the classification retained, or

(2) downgraded, declassified, or upgraded;

g. assessment of whether countermeasures are appropriate and feasible to negate or minimize the effect of the compromise or potential compromise; and

h. assessment of other appropriate corrective, administrative, disciplinary, or legal actions.

6. COMBINING SIMILAR INCIDENTS. Damage assessments may be completed for a group of similar incidents when such grouping is a logical method of meeting this requirement. A logical grouping includes a situation where multiple matters requiring a damage assessment are related to a programmatic area and would result in the same or similar damage to national security or advantage to foreign governments and/or hostile organizations.

7. CASES INVOLVING OTHER GOVERNMENT AGENCY INFORMATION. Whenever a compromise or potential compromise involves the classified information of another Government agency, the cognizant Departmental safeguards and security office responsible for the inquiry must provide the facts and circumstances that affect the other Government agency's information or interests to the Director, Office of Security. The Director, Office of Security, must coordinate with the other Government agency, as appropriate.

8. CASES INVOLVING FOREIGN GOVERNMENT INFORMATION. Whenever a compromise or potential compromise involves the information of a foreign government that requires protection (i.e., classified or Confidential Foreign Government Information Modified Handling [C/FGI-Mod]), the cognizant Departmental safeguards and security office responsible for the inquiry must provide the facts and circumstances that affect the foreign government's information or interests to the Director, Office of Security. The foreign government, however, will not normally be advised of any Departmental security system vulnerabilities that allowed or contributed to the compromise or potential

compromise. The Director, Office of Security must coordinate with the foreign government, as appropriate.

9. JOINT DAMAGE ASSESSMENT WITH ANOTHER GOVERNMENT AGENCY. Whenever a compromise or potential compromise involves the classified information or interests of more than one Government agency, the following requirements apply.

a. Each Government agency is responsible for conducting the assessment of damage resulting from its compromised or potentially compromised information.

b. If a compromise or potential compromise involves the classified information of DOE and another Government agency, and if more than one damage assessment is performed, the Primary DOE Organization responsible for the Department damage assessment must provide the damage assessment to the Director, Office of Security, who will coordinate with the other Government agency.

c. When a joint damage assessment is to be made, the Office of Security will coordinate assignment of responsibility between the Department and the other Government agency.

d. If a compromise or potential compromise of Departmental classified information is the result of actions taken by foreign nationals, foreign government officials, and/or U.S. nationals employed by international organizations, the Director, Office of Security, through coordination with OCI/ODNCI, must ensure, through appropriate intergovernmental liaison channels, that information pertinent to the assessment is obtained.

e. If a compromise or potential compromise of SCI has occurred, the Director, Office of Intelligence must consult with the designated representative of the Director, Central Intelligence and other appropriate officials responsible for the information involved.

PRIMARY DOE ORGANIZATIONS TO WHICH DOE O 471.4,
***Incidents of Security Concern,* IS APPLICABLE**

Office of the Secretary
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Office of Counterintelligence
Departmental Representatives to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Electric Transmission and Distribution
Office of Energy Assurance
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Hearings and Appeals
Office of Independent Oversight and Performance Assurance
Office of the Inspector General
Office of Intelligence
Office of Legacy Management
Office of Management, Budget and Evaluation and Chief Financial Officer
National Nuclear Security Administration
Office of Nuclear Energy, Science and Technology
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Secretary of Energy Advisory Board
Office of Security
Office of Security and Safety Performance Assurance
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

CONTRACTOR REQUIREMENTS DOCUMENT
DOE O 471.4, *Incidents of Security Concern*

This Contractor Requirements Document (CRD) establishes the requirements for Department of Energy (DOE) contractors, including National Nuclear Security Administration contractors. Contractors must comply with the requirements listed in the CRD to the extent set forth in their contracts.

Regardless of the performer of the work, contractors with this CRD incorporated into their contracts are responsible for compliance with the requirements of the CRD. Affected contractors are also responsible for flowing down the requirements of the CRD to subcontracts at any tier to the extent necessary to ensure the contractors' compliance with the requirements. In so doing, contractors must not unnecessarily or imprudently flow down requirements to subcontractors. That is, contractors will ensure that they and their subcontractors comply with the requirements of the CRD and incur only those costs that would be incurred by a prudent person in the conduct of competitive business.

DOE contractors with the CRD incorporated into their contracts must comply with the requirements of DOE O 471.4, *Incidents of Security Concern,* dated 3-17-04, and all other applicable rules, regulations, and directives, including the following.

1. Any contractor who observes, finds, or has knowledge or information about an incident of security concern must immediately report this information to the Facility Security Officer (FSO) or designee. The FSO or designee must make notifications as specified in Chapter I, paragraph 3, of this CRD.

2. If a contractor discovers an incident of security concern, including one that involves classified matter, special nuclear material, or other security interests at risk (e.g., interests not properly controlled), the contractor must make reasonable steps to safeguard the security interests in an appropriate manner. The contractor must also ensure evidence associated with the incident is not tampered with or destroyed.

3. Any contractor discovering actual or suspected fraud, waste, or abuse of government resources must report such incidents to the Office of the Inspector General.

4. Locally developed procedures must be established, documented, approved by the cognizant Primary DOE Organization, and disseminated to ensure the identification, reporting, root cause analysis, and resolution of incidents of security concern and tracking of time and funds expended in these and related activities. These procedures must also provide guidelines for possible administrative and disciplinary actions.

5. Inquiries must be conducted to determine all the pertinent facts and circumstances surrounding incidents of security concern. (Inquiries are addressed further in Chapter 1 of this CRD.)

6. When a violation is suspected or discovered, appropriate Federal, state, and local organizations must be contacted by the contractor when written concurrence has been obtained from the head of the field element.

7. Appropriate corrective actions must be taken for each incident of security concern to prevent recurrence of the incident, including review and/or revision of applicable safeguards and security plans and procedures. (Corrective actions are addressed further in Chapter I of this CRD.)

8. In addition to DOE administrative actions or procedures initiated and conducted under 10 CFR 710, if the contractor is responsible for conducting an inquiry under Chapter I of this CRD and the parties responsible for an incident of security concern are contractor employees, the contractor must determine whether other administrative action is appropriate, including reprimand, retraining, counseling, or other action necessary to prevent recurrence of the incident.

9. The contractor must assist in conducting damage assessments when requested by the head of the field element.

CONTENTS

Chapter I. Identification and Reporting Requirements

1. General I-1
2. Incident Identification and Categorization I-1

   Table 1. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 1 (IMI-1) I-3
   Table 2. Reportable Categories of Incidents of Security Concern, Impact Measurement Index2 (IMI-2) I-4
   Table 3. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 3 (IMI-3) I-5
   Table 4. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 4 (IMI-4) I-7

3. Reporting Requirements I-8

   Figure 1. Incidents of Security Concern I-9

4. Inquiry Officials I-13
5. Federal, State, or Local Law Enforcement Personnel I-14
6. Conduct of Inquiries I-14

   Figure 2. Example Chain-of-Custody Form I-16

7. Inquiry Report Content/Closure Considerations I-18
8. Administrative Actions I-20
9. Records Retention I-20

Chapter II. Incidents of Security Concern Involving Compromise or Potential Compromise of Classified Information

1. Inquiries into Potential Compromise of, Compromise of, or Missing Classified Information II-1

CHAPTER I. IDENTIFICATION AND REPORTING REQUIREMENTS

1. GENERAL.

   a. A system of controls and procedures must be developed, approved, implemented, enforced, and maintained:

      (1) to deter, detect, and prevent incidents of security concern, and

      (2) for the timely identification and notification of, inquiry into, analysis of, and reporting of incidents of security concern.

   b. Inquiries must be used to determine the root causes and the individuals responsible for incidents of security concern.

   c. All discussions and documents associated with an incident of security concern must be classified or controlled according to current classification or control guidance and following procedures contained in appropriate Department of Energy (DOE) directives.

2. INCIDENT IDENTIFICATION AND CATEGORIZATION. DOE uses a graded approach for identification and categorization of incidents of security concern. This approach provides a framework for the requirements of reporting time lines and the level of detail for inquiries into and root cause analysis of specific security incidents. By establishing a graded approach, line management can effectively allocate the resources necessary to implement this Contractor Requirements Document (CRD) based on the severity of the security incident. The following paragraphs provide the basis for identification and categorization of incidents of security concern.

   a. Incident Identification. Incidents of security concern are actions, inactions, or events that have occurred at a site that:

      (1) pose threats to national security interests and/or critical DOE 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, or

      (5) adversely impact the ability of organizations to protect DOE safeguards and security interests.

b. Incident Categorization. Incidents of security concern are categorized in accordance with their potential to cause serious damage or place safeguards and security interests and activities at risk. Four categories of security incidents have been established based on the relative severity of the incident. Each of the four categories is identified by an impact measurement index (IMI) number as follows (from most severe to least severe): IMI-1, IMI-2, IMI-3, and IMI-4. Each of the four categories is further subdivided into specific subcategories based on the security topical areas of physical security, protective forces, information security, personnel security, and nuclear material control and accountability. The categorization of specific security incidents occurs at the time the security incident is discovered. The categorization of specific security incidents can change based on information developed during the inquiry into the incident.

c. Impact Measurement Index (IMI). The IMI number is used to identify, trend, and evaluate each security incident or combination of incidents. (Specific information to be used to categorize incidents of security concern is contained in Table 1 through Table 4; however, the IMI subcategories contained in these tables are not all inclusive, and if they overlap, the more stringent reporting category will apply.) The basis for each IMI category is provided below:

(1) 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. [See Table 1, Reportable Categories of Incidents of Security Concern, Impact Measurement Index 1 (IMI-1).]

(2) IMI-2. Actions, inactions, or events that pose threats to national security interests and/or critical DOE assets or that potentially create dangerous situations. [See Table 2, Reportable Categories of Incidents of Security Concern, Impact Measurement Index 2 (IMI-2).]

(3) 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. [See Table 3, Reportable Categories of Incidents of Security Concern, Impact Measurement Index 3 (IMI-3).]

(4) 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. [See Table 4, Reportable Categories of Incidents of Security Concern, Impact Measurement Index 4 (IMI-4).]

Table 1. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 1 (IMI-1)

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.

DOE O 151.1B, *Comprehensive Emergency Management System,* dated 10-29-03, and facility emergency management plans may require more stringent reporting times for IMI-1 type incidents than listed here. Shorter reporting times should be determined on an individual incident basis and applied accordingly.

Incident Type	Report within 1 hour	Report within 8 hours	Report monthly
1. Confirmed or suspected loss, theft, or diversion of a nuclear device or components.	X		
2. Confirmed or suspected loss, theft, diversion, or unauthorized disclosure of weapon data.	X		
3. Confirmed or suspected loss, theft, or diversion of Category I or II quantities of special nuclear material (SNM).	X		
4. A shipper-receiver difference involving a loss in the number of items which total a Category I or II quantity of SNM.	X		
5. Confirmed or suspected loss, theft, diversion, unauthorized disclosure of Top Secret (TS) information, Special Access Program (SAP) information, or Sensitive Compartmented Information (SCI), regardless of the medium, method, or action resulting in the incident.	X		
6. Confirmed or suspected intrusions, hacking, or break-ins into DOE computer systems containing TS information, SAP information, or SCI.	X		
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.	X		
8. Confirmed or suspected attacks against DOE Federal and contractor employees that adversely impact a facility's or site's security posture.	X		
9. Confirmed or suspected acts or attempts of terrorist-type actions.	X		
10. Confirmed threats that immediately endanger personnel health or safety and may require immediate protective force/law enforcement intervention.	X		
11. Dangerous weapons and firearms-related incidents involving protective force operations/personnel where an individual is killed, wounded, or an intentional discharge occurs.	X		
12. Confirmed or suspected acts of sabotage, at any DOE facility, that place the safety or security of personnel, facilities, or the public at risk.	X		
13. Confirmed compromise of root/administrator privileges in DOE unclassified computer systems that have a significant possibility of being contaminated with TS information, SAP information, or SCI.	X		
14. Confirmed compromise of root/administrator privileges in DOE computer systems containing Secret or Confidential information.	X		
15. Confirmed intrusions into information systems containing classified information.	X		
16. Instances of malicious code that cause disruption, degradation, or compromise of information systems for an entire site/facility.	X		
17. Instances of malicious code that allow unauthorized or undetected access to information systems containing classified information (Top Secret, Secret, Confidential, SAP information, or SCI).	X		

Table 2. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 2 (IMI-2)

IMI-2 Actions, inactions, or events that pose threats to national security interests and/or critical DOE assets or that potentially create dangerous situations.

Incident Type	Report within 1 hour	Report within 8 hours	Report monthly
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.		X	
2. Confirmed or suspected intrusions, hacking, or break-ins into DOE computer systems containing Secret or Confidential classified information.		X	
3. Any amount of SNM found in an exceptionally dangerous/hazardous unapproved storage environment, or unapproved mode of transportation/transfer.		X	
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.		X	
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.		X	
6. Confirmed or suspected unauthorized disclosure, loss, or potential loss of Secret matter regardless of the medium, method, or action resulting in the incident.		X	
7. Actual or suspected technical interceptions of any level of classified information.		X	
8. Actions, by electronic or physical means, that interfere with any DOE safeguards and security practices.		X	
9. Notifications, by any media or source, of validated threats that do not appear to immediately threaten personal safety or health.		X	
10. Loss of classified information that must be reported to other Government agencies or foreign organizations.		X	
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.		X	
12. The loss of any DOE classified interest that requires state or local government or other Federal agency notification.		X	
13. Confirmed compromise of root/administrator privileges in DOE unclassified computer systems.		X	
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.		X	
15. Potential compromise of root/administrator privileges in DOE computer systems containing classified information.		X	
16. Instances of malicious code that cause disruption/degradation or compromise of information systems dedicated to safety, security, or critical operations.		X	
17. Detection of activities involving individuals who have been confirmed as physically watching/casing/surveilling a site in an effort to gather information to aid in the conduct of a terrorist-type attack.		X	

Table 3. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 3 (IMI-3)

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.

Incident Type	Report within 1 hour	Report within 8 hours	Report monthly
1. 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 special nuclear material (SNM).		X	
2. Bomb-related incidents at any DOE facility, including location of a suspected device.		X	
3. Confirmed or suspected unauthorized disclosure, loss, or potential loss of Confidential matter by any medium, method, or action.		X	
4. Confirmed or alleged noncompliance with laws or DOE directives/standards that jeopardizes protection of the facility or site security interests.		X	
5. Demonstrators or protestors that cause site and facility damage.		X	
6. Labor strikes that could degrade or impede the required protection of the facility or site.		X	
7. Physical violence or threat of retaliation against facility security personnel.		X	
8. Dangerous weapons and firearms-related incidents involving protective force operations/personnel where an accidental weapon discharge occurs.		X	
9. Loss or theft of DOE firearms, per DOE O 473.2, *Protective Force Program,* dated 6-30-00.		X	
10. 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.		X	
11. 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 sensitive information.		X	
12. Confirmed or suspected malicious activities, including but not limited to stealing badges or vehicle licenses.		X	
13. Discovery of malicious activities, disorderly conduct, or vandalism that disrupts facility activities or causes damage between $10K and $100K.		X	
14. Circumvention of established access control procedures into a security area (excluding Property Protection Area).		X	
15. 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.		X	
16. A shipper-receiver difference involving a loss in the number of items which total a Category III or IV quantity of SNM.		X	
17. Confirmed or suspected loss, theft, or diversion of Category III or IV quantities of SNM.		X	
18. Intrusion attempts into information systems containing classified information.		X	
19. Confirmed intrusions into unclassified information systems that are not publicly available (e.g., behind a firewall).		X	

Table 3. continued			
Incident Type	Report within 1 hour	Report within 8 hours	Report monthly
20. 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).		X	
21. Unauthorized network scans/probes on information systems possessing classified information.		X	
22. Incidents of apparent surveillance of facilities or operations (studying, photographing, low over-flights, outsiders questioning employees or protective force, unusual calls for information, etc.).		X	

Table 4. Reportable Categories of Incidents of Security Concern, Impact Measurement Index 4 (IMI-4)

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			
Incident Type	Report within 1 hour	Report within 8 hours	Report monthly
1. 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.			X
2. Significant shipper-receiver differences that exceed 200g of fissile material and the combined limit of error for the shipment.			X
3. 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.			X
4. 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.			X
5. 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.			X
6. Non-credible bomb threats at any DOE nuclear or non-nuclear facility.			X
7. 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.			X
8. Peaceful demonstrations or protests that do not threaten facility or site security interests or activities.			X
9. Failure to adhere to established procedures contributing to the misuse or misprocessing of or failure to maintain security badges and passes.			X
10. Loss of security badges in excess of 5 percent of total issued during 1 calendar year.			X
11. Failure to adhere to established procedures contributing to the mismanagement or faulty application of the DOE Personnel Security Assurance Program, Personnel Assurance Program, or Human Reliability Program.			X
12. Failure to adhere to established administrative procedures contributing to problems with foreign visitors.			X
13. Classified information sent by 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 offline, 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.			X
14. Unauthorized cellular phones and personal digital assistants introduced into a Limited Area, Protected Area, or Material Access Area, where there is no potential for compromise of classified or sensitive information.			X
15. Circumvent established access control procedures into a Property Protection Area.			X
16. High rate/amount of loss (excluding natural disasters) or theft of Government property.			X

3. REPORTING 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. (See Figure 1, Incidents of Security Concern.) During this period, the suspected incident must be categorized by an IMI number. If it is determined an incident of security concern did not occur, no further action is required.

b. Initial Incident Reporting. Incidents of security concern initial reports for IMI-1, IMI-2, and IMI-3 (as well as those for IMI-4 incidents involving foreign nationals, per paragraph 3.d.below) will be sent to the DOE Headquarters (HQ) Operations Center (OC) using DOE F 471.1, "Security Incident Notification Report," in accordance with locally developed procedures approved by the responsible element. Initial security incident reports will be forwarded based on the following criteria.

(1) Within 1 hour following categorization for security incidents determined to be IMI-1 (see Table 1), the originating site/facility will transmit a DOE F 471.1 to the DOE HQ OC. If a verbal notification of the incident is made to the DOE HQ OC, then a follow-up transmission of the DOE F 471.1 to the DOE HQ OC must be made.

(2) Within 8 hours following categorization of security incidents determined to be IMI-2/IMI-3 (see Tables 2 and 3), the originating site will transmit a DOE F 471.1 to the DOE HQ OC. If a verbal notification of the incident is made to the DOE HQ OC, then a follow-up transmission of the DOE F 471.1 to the DOE HQ OC must be made.

c. Reporting Incidents Receiving Media Attention. In addition to the IMI reporting time frames, the Office of Security must be notified within 8 hours of any security incidents that have been or will be reported in the media. The initial DOE F 471.1 and any subsequent updates must clearly identify the fact of media reporting.

d. Reporting Incidents Associated with Foreign Nationals. Security incidents having any association with foreign nationals will be clearly identified and reported on the initial DOE F 471.1 and in any related update or follow-on activity pertaining to the incident, including incidents categorized as an IMI-4. For security incidents involving any credible information that a foreign national or an agent of a foreign power is involved, the closest element of the Office of Counterintelligence (OCI)/Office of Defense Nuclear Counterintelligence (ODNCI) will be notified.

e. Numbering Incidents and Changing Categories. When the initial incident report (i.e., DOE F 471.1) is transmitted, it is to include a local incident tracking

number. All subsequent reports pertaining to a security incident (e.g., inquiry and other related activities) will be transmitted to the Office of Security. Changes in IMI categorizations require resubmission of DOE F 471.1 to the Office of Security.

f. Reporting Incidents Associated with Sensitive Programs. Only the initial report, DOE F 471.1, will be required for incidents involving activities associated with sensitive programs. These programs will include the Sensitive Compartmented Information (SCI) Program, Special Access Programs (SAPs), Technical Surveillance Countermeasures Program, Counterintelligence Program, or other programs identified by the Office of Security. All subsequent reporting will be handled "within channels" until such time as the inquiry report has been distributed. The date of the inquiry report will be transmitted to the Office of Security for database entry.

g. Closing Inquiries.

(1) IMI-1 and IMI-2 incidents are considered closed upon completion of the inquiry report. The inquiry report must be completed within 60 working days of the incident categorization or a status report must be provided in accordance with paragraph 3.j.(1), below.

(2) IMI-3 incidents are considered closed upon completion of DOE F 5639.3, "Report of Security Incident/Infraction" (except for completing the section on assignment and acceptance of the security infractions), transmission of the completed DOE F 5639.3 to the Office of Security, and completion of actions required in local procedures.

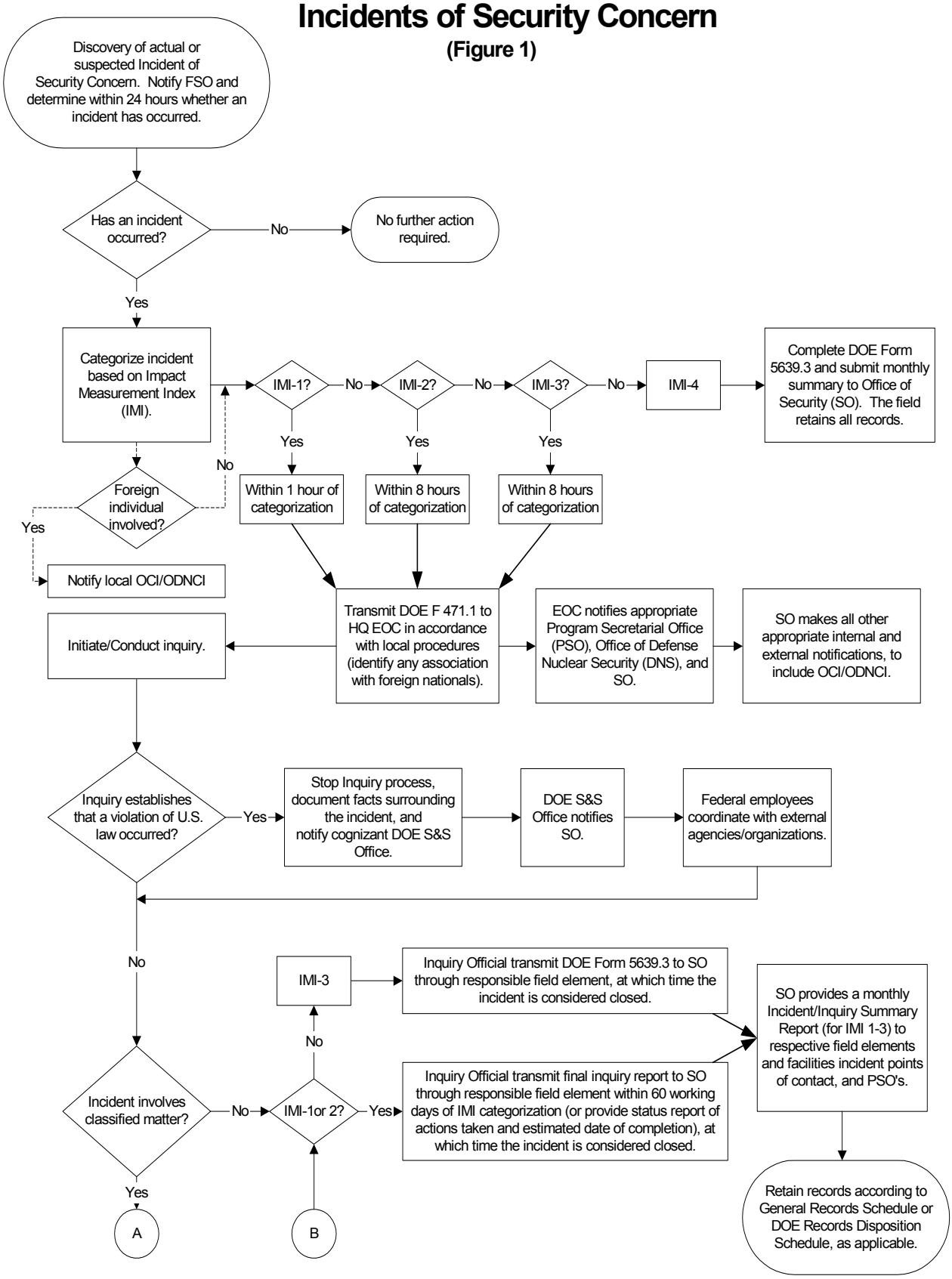
(3) IMI-4 incidents are considered closed upon completion of the DOE F 5639.3 or associated local procedures.

(4) A sanitized (unclassified) copy of the DOE F 5639.3 will be provided to the local personnel security office for placement in the appropriate personnel security file.

h. Final Inquiry Reports. Contractor inquiry officials will forward final inquiry reports in accordance with local procedures to appropriate contractor management for action and to the Office of Security.

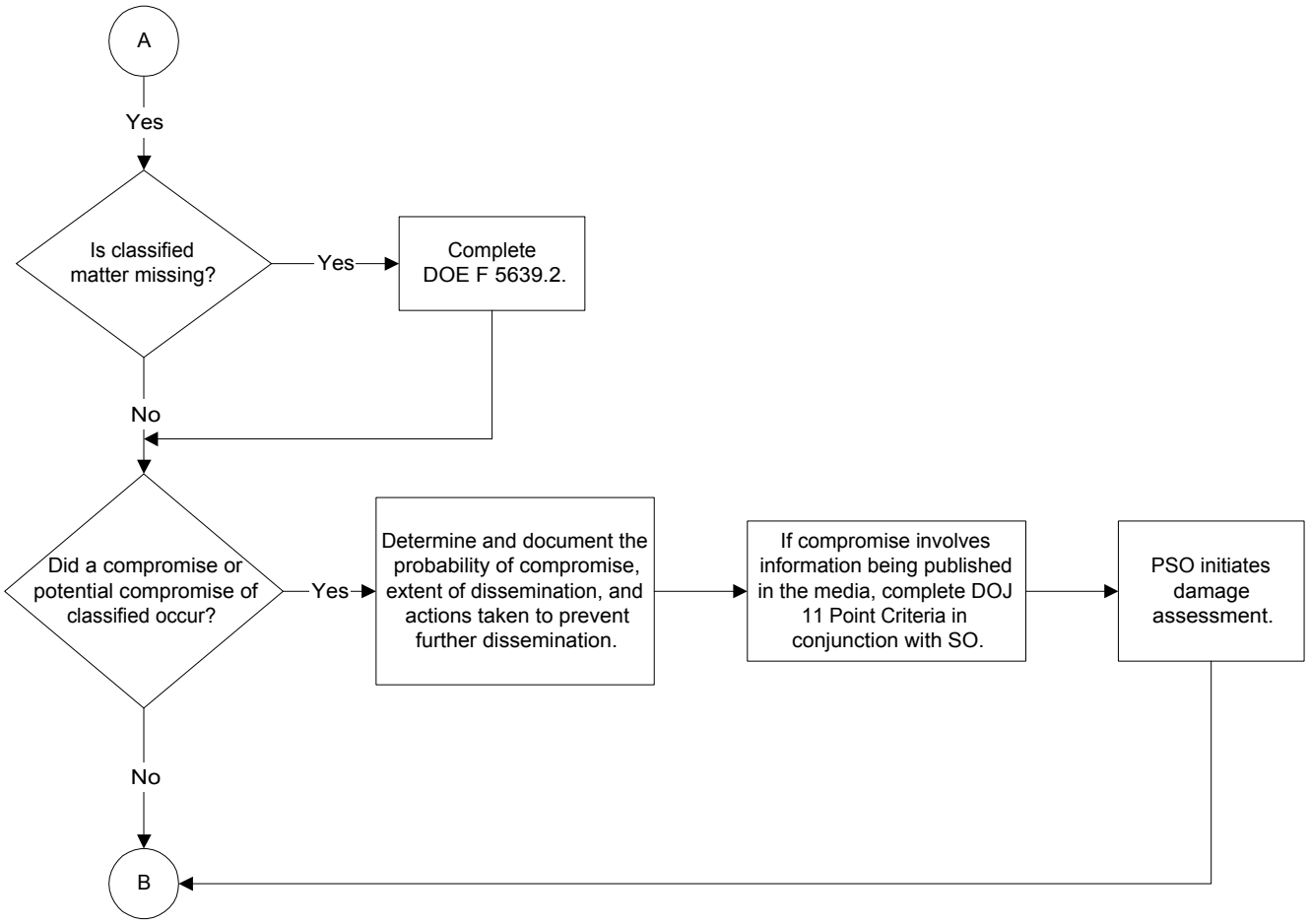
Incidents of Security Concern

(Figure 1)



Incidents of Security Concern

(Figure 1 continued)



i. Status/Summary Reports.

(1) IMI-1 and IMI-2. A monthly status report will be provided to the Office of Security and the cognizant Primary DOE Organization for IMI-1 and IMI-2 incidents that have not been closed within 60 working days of notification of the incident.

(a) Status reports will consist of the original DOE F 471.1, completed and planned actions, identification of issues precluding closure, and estimated date of closure.

(b) Status reports are due by the fifth working day of each month.

(2) IMI-3. Status reports are not required for IMI-3 incidents.

(3) IMI-4. Each facility will maintain 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, will be provided to the Office of Security. If no reportable incidents occurred during the calendar month, a summary stating this will be forwarded to the Office of Security by the fifth working day of each month.

j. Separate but Related Reporting.

(1) Occurrence Reporting Processing System. To eliminate reporting redundancy and centralize the reporting of security-related occurrences, all occurrences previously reported within the "Group 5—Safeguards and Security" category once contained in cancelled DOE M 232.1-1A, *Occurrence Reporting and Processing of Operations Information*, dated 7-21-97, are now incorporated into this CRD. Because an event meets the criteria for reporting as an incident of security concern does not negate the responsibility to report it as an occurrence under DOE O 231.1A, *Environment, Safety, and Health Reporting,* dated 8-19-03 (i.e., event affects both safety and security).

(2) DOE O 151.1B, *Comprehensive Emergency Management System*, dated 10-29-03. Incidents that are reportable under the provisions of DOE O 151.1B must continue to be reported in accordance with that Order. Reporting procedures for DOE incidents of security concern do not alter DOE O 151.1B requirements.

(3) Flash Reporting. National Nuclear Security Administration "Flash Reporting" procedures are not affected by Departmental incidents of security concern reporting requirements.

(4) Documenting Corrective Actions. Corrective actions identified in response to an incident of security concern must be documented. For incidents categorized as IMI-1, IMI-2, or IMI-3, a copy of the documentation must be forwarded to the Office of Security if not included in the inquiry report. Documentation of corrective actions for IMI-4 incidents does not have to be forwarded to the Office of Security.

4. INQUIRY OFFICIALS.

a. Inquiry officials will conduct inquiries to establish the pertinent facts and circumstances surrounding incidents of security concern.

b. Inquiry officials may be either Federal or contractor employees but must have previous investigative experience or Departmental inquiry training and must be knowledgeable of appropriate laws, Executive orders, Departmental directives, and/or regulatory requirements.

(1) Contractors may conduct inquiries into incidents of security concern; however, if a violation of law is determined or suspected, or the inquiry establishes information that a foreign power or an agent of a foreign power is involved, the contractor must stop further inquiry actions and notify the cognizant Departmental safeguards and security office, which will assume further notification and reporting responsibilities, to include coordination with OCI/ODNCI. In such instances, the contractor must document the known circumstances surrounding the incident of security concern and submit all accumulated data to the cognizant Departmental safeguards and security office.

(2) In all instances where the cognizant Departmental safeguards and security office disagrees with the contractor report, the cognizant Departmental safeguards and security office assumes supplemental inquiry responsibilities.

(3) When the inquiry into an incident of security concern necessitates communication with Agencies/organizations external to the Department (e.g., the U.S. Postal Service, the FBI, or other Federal agencies), a Federal employee must be responsible for performing all such communication.

(4) Contact with Federal, state, and local law enforcement officials may be made by contractors with the concurrence of the head of the field element.

c. Inquiry officials are not authorized to detain individuals for interviews nor to obtain sworn statements; however, they may conduct consensual interviews and obtain signed statements.

d. Inquiry officials must be appointed in writing by the head of the field element, the head of the Office of Headquarters Security Operations, or the Office of Security.

e. Inquiry officials are responsible for conducting the inquiry and maintaining records and documentation associated with the inquiry (e.g., logs of events, notes, recordings, and statements).

5. FEDERAL, STATE, OR LOCAL LAW ENFORCEMENT PERSONNEL.

a. Federal, state, or local law enforcement agency personnel requiring access to limited areas or higher for investigative actions must be escorted, have a current access authorization passed to DOE, or possess an active DOE access authorization. Such personnel will be approved for access to classified matter only if they possess the appropriate access authorization, the matter pertains directly to the investigation, and appropriate programmatic approvals have been granted if such approvals are required. Access to Restricted Data and Formerly Restricted Data will require a DOE Q or L or appropriate access authorization.

b. When authorized and approved Federal, state, or local law enforcement personnel are given access to classified information, they will be immediately advised of the classification level and category. They will also be informed of the protection and control requirements associated with the classified information they possess.

c. When an inquiry surrounding an incident of security concern establishes information indicating that fraud, waste, or abuse has occurred, the Office of the Inspector General must be notified for information and/or action.

d. The cognizant DOE safeguards and security office must make arrangements for the issuance of standard DOE security badges and any other necessary arrangements for Federal, State, or local law enforcement agencies involved in investigations.

6. CONDUCT OF INQUIRIES. The following actions must be taken when conducting inquiries into incidents of security concern and be reflected in the inquiry report. (See Chapter II for additional requirements.)

a. Data Collection.

(1) Collect all data/information relevant to the incident, such as operations logs, inventory reports, requisitions, receipts, photographs, signed statements, etc.

(2) Conduct interviews to obtain additional information regarding the incident.

(3) Collect physical evidence associated with the inquiry, if available. (Examples of physical evidence include, but are not limited to, recorder charts, computer hard drives, defective/failed equipment, procedures, readouts from monitoring equipment, etc.)

(4) Ensure physical evidence is protected and controlled and a chain-of-custody is maintained. (See Figure 2. Example Chain-of-Custody Form.)

b. Incident Reconstruction.

(1) Reconstruct the incident of security concern to the greatest extent possible using collected information and other evidence.

(2) Develop a chronological sequence of events that describes the actions preceding and following the incident.

(3) Identify persons associated with the incident.

c. Incident Analysis and Evaluation. This analysis will determine which systems/functions performed correctly or failed to perform as designed; it must provide the basis for determining the cause of the incident and subsequent corrective actions.

(1) Analyze the information collected during the inquiry process to determine whether it describes the incident completely and accurately.

(2) Collect additional data and reconstruct the incident if more information is required.

(3) Identify any collateral impact with other programs or security interests.

Figure 2. Example Chain of Custody Form

EVIDENCE/PROPERTY CUSTODY DOCUMENT **For use of this form see ISC-301 Conduct of Inquiries Course Manual.** **Proponent is the DOE Computer Forensics Laboratory.**	DOE TRACKING NUMBER: CFL CASE NUMBER

RECEIVING ACTIVITY	LOCATION	
NAME, GRADE AND TITLE OF PERSON FROM WHOM RECEIVED ☐ OWNER ☐ OTHER	ADDRESS *(Including Zip Code)*	
LOCATION FROM WHERE OBTAINED	REASON OBTAINED	DATE/TIME OBTAINED

ITEM NO.	QUANTITY	DESCRIPTION OF ARTICLES *(Include model, serial number, condition and unusual marks or scratches)*

CHAIN OF CUSTODY

ITEM NO.	DATE	RELEASED BY	RECEIVED BY	PURPOSE OF CHANGE OF CUSTODY
		SIGNATURE NAME, GRADE OR TITLE	SIGNATURE NAME, GRADE OR TITLE	
		SIGNATURE NAME, GRADE OR TITLE	SIGNATURE NAME, GRADE OR TITLE	
		SIGNATURE NAME, GRADE OR TITLE	SIGNATURE NAME, GRADE OR TITLE	
		SIGNATURE NAME, GRADE OR TITLE	SIGNATURE NAME, GRADE OR TITLE	
		SIGNATURE NAME, GRADE OR TITLE	SIGNATURE NAME, GRADE OR TITLE	

Figure 2. Example Chain-of-Custody Form (continued)

		CHAIN OF CUSTODY *(CONTINUED)*		
ITEM NO.	DATE	RELEASED BY	RECEIVED BY	PURPOSE OF CHANGE OF CUSTODY
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	
		SIGNATURE	SIGNATURE	
		NAME, GRADE OR TITLE	NAME, GRADE OR TITLE	

FINAL DISPOSAL ACTION

RELEASE TO OWNER OR OTHER (Name/Organization) _____

DESTROY _____

OTHER (Specify) _____

FINAL DISPOSAL AUTHORITY

ITEM(S)_____ON THIS DOCUMENT, PERTAINING TO THE INQUIRY/INVESTIGATION INVOLVING:

_____(IS)(ARE) NO LONGER
(Grade) *(Name)* *(Organization)*

REQUIRED AS EVIDENCE AND MAY BE DISPOSED OF AS INDICATED ABOVE. *(If articles must be retained do not sign, but explain in separate correspondence.)*

_____
(Typed/Printed Name, Grade, Title) *(Signature)* *(Date)*

WITNESS TO DESTRUCTION OF EVIDENCE

THE ARTICLE(S) LISTED AT ITEM NUMBER(S)_____(WAS) (WERE) DESTROYED BY THE EVIDENCE CUSTODIAN IN MY PRESENCE, ON THE DATE INDICATED ABOVE.

_____
(Typed/Printed Name, Grade, Title, Organization) *(Signature)* *(Date)*

7. INQUIRY REPORT CONTENT/CLOSURE CONSIDERATIONS. At a minimum, inquiry reports must describe the conduct and results of the inquiry and include the following information for the incident to be closed.

a. An executive summary.

b. A narrative, which must include the following.

(1) The date and time of incident discovery, any notifications, the incident inquiry, and other time-related actions pertaining to the incident (WHEN).

(2) 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 (WHERE).

(3) A complete discussion of the facts and circumstances surrounding the incident, including a description of all supporting information (WHAT), such as the following:

(a) detailed description of the incident of security concern;

(b) 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);

(c) identification of the causes for the incident (direct and contributing factors), descriptions of mitigating or aggravating factors that may reduce or increase the impact of the incident;

(d) descriptions of the actions that precipitated the incident;

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

(f) results of any interviews performed;

(g) descriptions of actions taken to minimize vulnerabilities created by the incident and prevent further loss/compromise of the security interest; and

(h) if the incident involves classified matter, the following must also be included:

1 a description of the potentially compromised classified matter, including but not limited to classification level, category, caveats (if any), and form (e.g., document title, date, and description). [A copy of the evidence (or photograph) must be retained and provided to HQ if requested.];

2 the classification guide and topic or source document, including date, of guide or source document;

3 known recipients of potentially compromised matter; and

4 owner of the classified matter (e.g., program office or other Government agency).

(4) An inquiry official's conclusion and the basis/facts that support the conclusion are essential.

(a) 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.

(b) The final report must also identify the management officials responsible for corrective actions and disciplinary actions.

c. The following must be included as attachments to the report of inquiry:

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

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

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

(4) a copy of the DOE F 471.1 and any other documents obtained during the data collection phase of the inquiry;

(5) a copy of DOE F 5639.3, or a form comparable in content, issued as a result of the inquiry; and

(6) a copy of DOE F 5639.2, "Reporting Unaccounted for Documents," or a form comparable in content, if applicable.

8. ADMINISTRATIVE ACTIONS.

a. Whenever possible, the responsibility for an incident of security concern must be assigned to an individual rather than to a position or office.

(1) 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.

(2) Security infractions are issued to document the assignment of responsibility for an incident of security concern. Individuals who do not possess an access authorization may be issued a security infraction.

b. Corrective actions taken in response to incidents of security concern must be documented, and for incidents categorized as IMI-1, IMI-2, or IMI-3, a copy of the documentation must be forwarded to the Office of Security. Documentation of corrective actions for IMI-4 incidents does not have to be forwarded to the Office of Security.

c. A copy of Part 1 of DOE F 5639.3 or similar form will be placed in the employee's DOE personnel security file. If an employee does not have an access authorization, it will be placed in his/her personnel file.

9. RECORDS RETENTION.

a. Records pertaining to incidents of security concern cannot be sent to Federal Records Centers.

b. Records must be dispositioned in accordance with an applicable General Records Schedule, published by the National Archives and Records Administration (NARA), or in accordance with a DOE Records Disposition Schedule approved by NARA, whichever is applicable.

c. The site records manager or similarly titled person should be routinely consulted regarding the maintenance and disposition of records.

CHAPTER II. INCIDENTS OF SECURITY CONCERN INVOLVING COMPROMISE OR POTENTIAL COMPROMISE OF CLASSIFIED INFORMATION

1. INQUIRIES INTO COMPROMISE OF, POTENTIAL COMPROMISE OF, OR MISSING CLASSIFIED INFORMATION. The following requirements are in addition to those contained in Chapter I of this CRD. Inquiry officials will perform, but not necessarily be limited to, the following actions.

   a. Query custodians and others having knowledge of the incident. When necessary, records must be audited for evidence of destruction, transmission, or other disposition.

   b. Ensure a DOE F 5639.2, or a form comparable in content, is completed if classified information is missing.

   c. Determine which Primary DOE Organization has programmatic responsibility for the information or whether the information was originated by another Government agency or a foreign government.

   d. Determine whether a compromise or potential compromise occurred. If there was a potential compromise, seek to determine the probability of compromise. The basis for such findings must be documented (i.e., potential compromise is defined as an incident of security concern where circumstances exist that cannot rule out the compromise of classified information).

   e. If an inquiry determines that a compromise or potential compromise has occurred, document the extent of the dissemination of the classified information and the actions taken to prevent further dissemination.

   f. When an inquiry establishes that classified information has been compromised by being published in the media, the questions contained in the Department of Justice Eleven-Point Criteria, which are listed below, must be answered and coordinated with the Office of Security. When completing the questions, provide all documentation and appropriate information to support affirmative responses. Each question must be answered affirmatively before the Department of Justice will initiate a formal investigation into the compromise; however, failure to affirmatively answer all the Department of Justice criteria does not preclude the Department of Justice from pursuing administrative or criminal action.

      (1) Could the date and identity of the article or articles disclosing the classified information be provided?

      (2) Could specific statements in the article which are considered classified be identified? Was the data properly classified?

(3) Is the classified data that was disclosed accurate? If so, provide the name of the person competent to testify concerning the accuracy.

(4) Did the data come from a specific document and, if so, what is the origin of the document and the name of the individual(s) responsible for the security of the classified data disclosed?

(5) Could the extent and official dissemination of the data be determined?

(6) Has it been determined that the data has not been officially released in the past?

(7) Has it been determined that prior clearance for publication or release of the information was not granted by proper authorities?

(8) Does review reveal that educated speculation on the matter cannot be made from material, background data, or portions thereof which have been published officially or have previously appeared in the press?

(9) Could the data be made available for the purpose of prosecution? If so, include the name of the person competent to testify concerning the classification.

(10) Has it been determined that declassification had not been accomplished prior to-the publication or release of the data?

(11) Will disclosure of the classified data have an adverse impact on national defense?