

Incident/Inquiry Report

The Incident/Inquiry Report is designed to provide a consistent reporting format to assist the Department of Energy (DOE) Complex in obtaining accurate and thorough information regarding an incident of security concern. Incident information collected will be input into the Incident Tracking & Analysis Capability (ITAC) Database to be used by the DOE, including the National Nuclear Security Administration (NNSA), to conduct analysis, modify policy, and provide value added feedback to the field.

This Report is to be completed by individual(s) with primary responsibility for incident Inquiries (i.e., the Inquiry Official). It is to be submitted to the Office of Security (SO) as part of the Inquiry process.

Every effort should be made to complete the report with as much detail as possible. All entries require completion to ensure each issue has been addressed. Where an entry is not applicable or the information is unknown, the field should be annotated as such (i.e., N/A or Unknown).

Please ensure the appropriate classification review is completed for this document. Enter the appropriate classification level and category (to include UCNI, OUO, etc.) at the top and bottom of all pages. Portion mark as appropriate. Include any caveats associated with this record.

Your timely completion and transmittal of the Incident/Inquiry Report to DOE/SO, is appreciated. After initial notification to the Headquarters Emergency Operations Center using DOE F 471.1, submission of a completed version of this report will serve to meet the requirement for the final inquiry report, as identified in DOE Order 471.4 *Incidents of Security Concern*, dated 3-17-04.

DOE HQ Tracking Number:

Locally Assigned Incident Tracking Number:

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

LRO for Facility where Incident Originated/Occurred:

Facility Abbreviation:

SSIMS Facility Code:

Facility where Incident Originated/Occurred:

Facility Abbreviation:

SSIMS Facility Code:

Location (Bldg./Rm.):

Facility responsible for conducting the Inquiry (if other than above):

SSIMS Facility Code:

Other Facilities/Location(s) affected by incident:

Location Name:

SSIMS Facility Code (if applicable).

Address:

City:

State:

Location (Bldg./Rm.):

Security area where incident occurred: (check all that apply)

Property Protection Area

Limited Area

Exclusion Area

Protected Area

Material Access Area

Vital Area

SCIF

SAPF/SSWA

Classified Information System Facility

Secure Communications Center

Non-Security Area (e.g., private residence, public areas, etc.)

2.0 Dates:

2.1 Reporting:

Time Zone (for the following times):

Incident Occurred

Date/Time:

Incident Discovered

Date/Time:

Inquiry initiated (determination that an incident has occurred)

Date/Time:

IMI Categorization made

Date/Time:

DOE F 471.1 transmitted to HQ EOC

Date/Time:

Incident contained to prevent further compromise

Date:

Inquiry Status Report transmitted to SO

Date:

Inquiry completed

Date:

Inquiry Report transmitted to SO

Date:

Incident officially closed

Date:

2.2 Follow-up:

Interim corrective actions implemented

Date:

Proposed corrective actions transmitted to SO

Date:

GEN-16 policy applied by Classification Office

Date:

Damage Assessment completed

Date:

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

3.1 Notifications

Initial Reporting Point of Contact (from DOE F 471.1):

Name:

Organization:

Phone:

Title:

Facility Security Officer:

Name:

Organization:

Phone:

Title:

DOE Cognizant Security Organization or HQ Representative:

Name:

Organization:

Phone:

Title:

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

Name:

Organization:

Phone:

Title:

3.2 Inquiry

Lead Organization and Inquiry Official:

Name:

Organization:

Phone:

Title:

Inquiry Official(s) at other affected sites:

Name:

Organization:

Phone:

Title:

Inquiry Participant(s)/Assistant Inquiry Officials:

Name:

Organization:

Phone:

Title:

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

Organization Name:

POC Name:

Phone:

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

Organization Name:

POC Name:

Phone:

3.3 Individuals Involved

Responsible Individual(s):

Name:

Organization:

Phone:

Title:

Was this individual interviewed? Yes No

Written statement available? Yes No

Is this individual a foreign national? Yes No

Was this individual appropriately cleared? Yes No
First Line Supervisor's Name:

Other Individual(s):

Name:

Organization:

Phone:

Title:

Was this individual interviewed? Yes No

Written statement available? Yes No

Is this individual a foreign national? Yes No

Was this individual appropriately cleared? Yes No

4.0 IMI Categorization: *(from the tables below, identify the incident)*

Reportable Categories of Incidents of Security Concern

4.1 Impact Measurement Index (IMI-1)

Actions, inactions, or events that pose the most serious threats to national security interests and/or critical DOE assets, create serious security situations, or could result in deaths in the workforce or general public. Report within 1 hour. [Topical Area (TA) shown within <>]

- 1.1 Confirmed or suspected loss, theft, or diversion of a nuclear device or components.
<Select the TA for this IMI category: NMC&A or PHYSEC>
- 1.2 Confirmed or suspected loss, theft, diversion, or unauthorized disclosure of weapon data. <IS>
- 1.3 Confirmed or suspected loss, theft, or diversion of Category I or II quantities of Special Nuclear Material (SNM). <NMC&A>
- 1.4 A shipper-receiver difference involving a loss in the number of items which total a Category I or II quantity of SNM.. <NMC&A>
- 1.5 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. <IS>
- 1.6 Confirmed or suspected intrusions, hacking, or break-ins into DOE computer systems containing TS information, SAP information, or SCI. <IS>
- 1.7 Confirmed or suspected physical intrusion attempts or attacks against DOE facilities containing nuclear devices and/or materials, classified information, or other national security related assets. <PHYSEC>
- 1.8 Confirmed or suspected attacks against DOE Federal and contractor employees that adversely impact a facility's or site's security posture. <PHYSEC>
- 1.9 Confirmed or suspected acts or attempts of terrorist-type actions. <PHYSEC>
- 1.10 Confirmed threats that immediately endanger personnel health or safety and may require immediate protective force/law enforcement intervention. <PHYSEC>

- 1.11 Dangerous weapons and firearms-related incidents involving protective force operations/personnel where an individual is killed, wounded, or an intentional discharge occurs. <PROFORCE>
- 1.12 Confirmed or suspected acts of sabotage, at any DOE facility, that place the safety or security of personnel, facilities, or the public at risk. <PHYSEC>
- 1.13 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. <IS>
- 1.14 Confirmed compromise of root/administrator privileges in DOE computer systems containing Secret or Confidential information. <IS>
- 1.15 Confirmed intrusions into information systems containing classified information. <IS>
- 1.16 Instances of malicious code that cause disruption, degradation, or compromise of information systems for an entire site/facility. <IS>
- 1.17 Instances of malicious code that allow unauthorized or undetected access to information systems containing classified information (Top Secret, Secret, Confidential, SAP information, or SCI). <IS>
- 1.18 Other (describe "Other"):
 <Select the TA for this "Other" IMI category:
 IS, NMC&A, PERSEC, PHYSEC, or PROFORCE>

4.2 Impact Measurement Index (IMI-2)

Actions, inactions, or events that pose threats to national security interests and/or critical DOE assets or that potentially create dangerous situations. Report within 8 hours. [Topical Area (TA) shown within <>]

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

- 2.9 Notifications, by any media or source, of validated threats that do not appear to immediately threaten personal safety or health. <PHYSEC>
- 2.10 Loss of classified information that must be reported to other Government agencies or foreign organizations. <IS>
- 2.11 Unsecured classified repositories of any type, including safes, doors, or other protective encasements, that contain Top Secret information, Special Access Program information, or Sensitive Compartmented Information. <Select the TA for this IMI category: IS or PHYSEC>
- 2.12 The loss of any DOE classified interest that requires state or local government or other Federal agency notification. <IS>
- 2.13 Confirmed compromise of root/administrator privileges in DOE unclassified computer systems. <IS>
- 2.14 Confirmed compromise of root/administrator privileges in DOE unclassified computer systems that have a significant possibility of being contaminated with Secret or Confidential information. <IS>
- 2.15 Potential compromise of root/administrator privileges in DOE computer systems containing classified information. <IS>
- 2.16 Instances of malicious code that cause disruption/degradation or compromise of information systems dedicated to safety, security, or critical operations. <IS>
- 2.17 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. <PHYSEC>
- 2.18 Other (describe "Other"):
 <Select the TA for this "Other" IMI category:
 IS, NMC&A, PERSEC, PHYSEC, or PROFORCE >

4.3 Impact Measurement Index (IMI-3)

Actions, inactions, or events that pose threats to DOE security interests or that potentially degrade the overall effectiveness of the Department's safeguards and security protection program. Report within 8 hours. [Topical Area (TA) shown within <>]

- 3.1 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). <NMC&A>
- 3.2 Bomb-related incidents at any DOE facility, including location of a suspected device. <PHYSEC>
- 3.3 Confirmed or suspected unauthorized disclosure, loss, or potential loss of Confidential matter by any medium, method, or action. <IS>
- 3.4 Confirmed or alleged noncompliance with laws or DOE directives/standards that jeopardizes protection of the facility or site security interests. <PHYSEC>
- 3.5 Demonstrators or protestors that cause site and facility damage. <PHYSEC>
- 3.6 Labor strikes that could degrade or impede the required protection of the facility or site. <Select the TA for this IMI category: PHYSEC or PROFORCE>
- 3.7 Physical violence or threat of retaliation against facility security personnel. <PHYSEC>
- 3.8 Dangerous weapons and firearms-related incidents involving protective force operations/personnel where an accidental weapon discharge occurs. <PROFORCE>

- 3.9 Loss or theft of DOE firearms, per DOE O 473.2, Protective Force Program, dated 6-30-00. <PROFORCE>
- 3.10 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. <PHYSEC>
- 3.11 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. <PHYSEC>
- 3.12 Confirmed or suspected malicious activities, including but not limited to stealing badges or vehicle licenses. <PHYSEC>
- 3.13 Discovery of malicious activities, disorderly conduct, or vandalism that disrupts facility activities or causes damage between \$10K and \$100K. <PHYSEC>
- 3.14 Circumvention of established access control procedures into a security area (excluding Property Protection Area). <PHYSEC>
- 3.15 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. <NMC&A>
- 3.16 A shipper-receiver difference involving a loss in the number of items which total a Category III or IV quantity of SNM. <NMC&A>
- 3.17 Confirmed or suspected loss, theft, or diversion of Category III or IV quantities of SNM. <NMC&A>
- 3.18 Intrusion attempts into information systems containing classified information. <IS>
- 3.19 Confirmed intrusions into unclassified information systems that are not publicly available (e.g., behind a firewall). <IS>
- 3.20 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). <IS>
- 3.21 Unauthorized network scans/probes on information systems possessing classified information. <IS>
- 3.22 Incidents of apparent surveillance of facilities or operations (studying, photographing, low over-flights, outsiders questioning employees or protective force, unusual calls for information, etc.). <PHYSEC>
- 3.23 Other (describe “Other”):
 - <Select the TA for this “Other” IMI category:
 - IS, NMC&A, PERSEC, PHYSEC, or PROFORCE >

4.4 Impact Measurement Index (IMI-4)

Actions, inactions, or events that could pose threats to DOE by adversely impacting the ability of organizations to protect DOE safeguards and security interests. Report monthly. [Topical Area (TA) shown within <>]

- 4.1 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. <NMC&A>

- 4.2 Significant shipper-receiver differences that exceed 200g of fissile material and the combined limit of error for the shipment. <NMC&A>
- 4.3 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. <NMC&A>
- 4.4 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. <NMC&A>
- 4.5 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. <IS>
- 4.6 Non-credible bomb threats at any DOE nuclear or non-nuclear facility. <PHYSEC>
- 4.7 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. <IS>
- 4.8 Peaceful demonstrations or protests that do not threaten facility or site security interests or activities. <PHYSEC>
- 4.9 Failure to adhere to established procedures contributing to the misuse or misprocessing of or failure to maintain security badges and passes. <Select the TA for this IMI category: PERSEC or PHYSEC>
- 4.10 Loss of security badges in excess of 5 percent of total issued during 1 calendar year. <PHYSEC>
- 4.11 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. <PERSEC>
- 4.12 Failure to adhere to established administrative procedures contributing to problems with foreign visitors. <Select the TA for this IMI category: IS, NMC&A, PERSEC, PHYSEC, or PROFORCE>
- 4.13 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. <IS>
- 4.14 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. <PHYSEC>
- 4.15 Circumvent established access control procedures into a Property Protection Area. <PHYSEC>
- 4.16 High rate/amount of loss (excluding natural disasters) or theft of Government property. <PHYSEC>
- 4.17 Other (describe "Other"):
 <Select the TA for this "Other" IMI category:
 IS, NMC&A, PERSEC, PHYSEC, or PROFORCE >

5.0 Classified Matter Description (to be completed for incidents involving classified matter):

5.1 Type

Incident Type: (check all that apply)

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

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

- Electronic Storage Media
- E-Mail
- Facsimile
- Hard Copy
- Internet
- Visual
- Audio/Verbal
- Other (describe "Other"):

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

Did the matter involve Work for Others?" Yes No

Did the matter involved belong to an "Other Government Agency?" Yes No

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

5.2 Classification

Classification Level: (check only one)

- Top Secret
- Secret
- Confidential

Category of Information: (check only one)

- Restricted Data
- Formerly Restricted Data
- National Security Information

Caveats: (check all that apply)

Weapons Data (WD)

Identify any SIGMA's (1-5, and 9-15) involved: _____

Special Access Program (SAP)

Sensitive Compartmented Information (SCI)

Foreign Government Information (FGI)

Naval Nuclear Propulsion Information (NNPI)

No Foreign Dissemination (NOFORN)

Other (describe "Other"):

5.3 Description

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

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

Classification Official(s) that verified the matter's classification (if applicable):

Name:

Organization:

Phone:

Title:

6.0 Narrative:

Describe the incident (including an executive summary, narrative, chronology of events, and conclusion, identifying who, what, when, where, why, and how) in accordance with DOE requirements for Inquiry Report Content identified in DOE Order 471.4 INCIDENTS OF SECURITY CONCERN, dated 3-17-04. (Specifics captured elsewhere in this report may be excluded):

7.0 Containment:

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

8.0 Mitigating/Aggravating Factors:

Identify any information that may be considered as a mitigating factor and reduces the

potential impact of the incident:

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

9.0 Determination of Inquiry:

9.1 Determination

Determination of Unauthorized Disclosure:(check only one)

- Loss/compromise did occur
- Probability of compromise is not remote
- Probability of compromise is remote
- Loss/compromise did not occur

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

Fundamental (root) cause(s) of the incident involves: (check all that apply)

- Equipment/Material Problem
- Management Problem
- Personnel Error
- Procedure Problem
- Training Deficiency
- Design Problem
- External Phenomena
- Other (describe "Other"):

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

How would the responsible individual(s) non-compliance be characterized: (check only one)

- Inadvertent
- Negligence
- Gross Negligence
- Willful

9.2 Summary

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

9.3 Damage Assessment

Has the Program Office requested a Damage Assessment be done? [] Yes [] No

Was a damage assessment completed (formal and/or informal)? [] Yes [] No

Summarize the results of the (formal and/or informal) damage assessment:

9.4 Documentation

Documentation included in inquiry report: (check all that apply. * indicates a required item.)

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

10.0 Corrective Actions:

Categorize Action(s) Taken: (check all that apply)

- [] Communication security system modification
- [] Cyber security system modification
- [] Disciplinary action
- [] Physical security system modification
- [] Policy/procedural change
- [] Training Modification
- [] Other (describe "Other"):

Summarize the proposed corrective actions identified to prevent recurrence (corrective actions identified in response to an incident of security concern must be documented and, for incidents categorized as IMI-1, 2, & 3 a copy forwarded to SO.):

Management Official(s) responsible for Corrective Actions:

Name:
 Organization:
 Phone:
 Title:

11.0 Disciplinary Actions:

Action taken: (check all that apply)

- Mandatory training
- Oral admonishment
- Personnel reassignment
- Suspension of access authorization
- Termination of access authorization
- Termination of employment
- Written reprimand
- Other (describe "Other"):

Are there mitigating factors affecting disciplinary action? Yes No

If "Yes", identify the factors: (check all that apply)

- Culpability of others
- Employee cooperativeness
- Enticements or provocations
- Possibility of genuine misunderstanding
- Other (describe "Other"):

Are there aggravating factors affecting disciplinary action? Yes No

If "Yes", identify the factors: (check all that apply)

- Employee willfulness
- Nature of other breaches
- Past breaches
- Series of breaches
- Other (describe "Other"):

Management Official(s) responsible for Disciplinary Actions:

Name:

Organization:

Phone:

Title:

12.0 Comments:

Include any comments associated with the incident:

Check here if this incident has or may result in increased media attention?

Check here if this incident has been rescinded (e.g., determination that an incident did not occur) based on the results of the inquiry?

Classification Official(s) who made the classification determination for this record:

Name:

Organization:

Phone:

Title: