

INCIDENT INQUIRY REPORT

The Incident/Inquiry Report is designed to provide a consistent reporting format to assist the Department of Energy (DOE) in obtaining accurate and thorough information regarding an incident of security concern. Information collected will be entered into the Safeguards and Security Information Management System (SSIMS) to be used by 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 Health, Safety and Security, Office of Security Technology and Assistance, Office of Security Assistance, HS-81 (hereafter DOE/HS), 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 (N/A) or the information is unknown (UNK), the field should be annotated as such (i.e., N/A or UNK).

Please ensure the appropriate classification and unclassified controlled information reviews are completed for this document. Enter the appropriate classification level and unclassified controlled information markings. Portion mark the Report as appropriate. Include any caveats associated with this Report.

Your timely completion and transmittal of the Report to DOE/HS is appreciated. After initial notification to the Headquarters Emergency Operations Center (EOC) using DOE F 471.1, submission of a completed Report will meet the requirement for the final inquiry report in DOE Manual 470.4-1, Safeguards and Security Program Planning and Management, Section N, *Incidents of Security Concern*, dated 8-26-05.

NOTE: If an incident/inquiry is an IMI 1.2, 1.5, 1.6, 1.7, 1.13, 1.14, 1.15, 1.16, 1.17, 2.6, 2.12, 2.13, 2.14, 2.15, 2.16, 3.3, 3.4, 3.11, 3.12, 3.18, 3.19, 4.5, 4.7, 4.9, 4.10, 4.11, or 4.13, information must be provided in the following sections in order to close an incident/inquiry: 7. Containment, 8. Factors, and 10. Corrective Actions. In addition, in 9. Determination, Documentation portion, a check must be placed in the "Corrective Action Plan," box. These IMIs are bolded in the text below, and Sections 7, 8, 10 and the relevant portion of 9 is in bold italics. When entering information into SSIMS concerning one of these IMIs, all fields must be completed before it will accept a closure date. It is recommended all sections of the report are completed regardless of the IMI.

Incident Inquiry Report

Incident Number:

Local Tracking Number:

1. Locations: (Complete with Facility Information as identified in SSIMS.)

Facility where Incident Originated/Occurred:

SSIMS Facility Code:
CSO:
Name:
Acronym:
Location (Building/Room):

Facility Responsible for Conducting the Inquiry (if other than above):

SSIMS Facility Code:
Name:

Other Facilities/Location(s) affected by the Incident:

SSIMS Facility Code (if applicable).
Name
Address:
City:
State:
Location (Building/Room):
DOE Facility Yes No

Security Area(s) where Incident Occurred: (check all that apply)

- | | | |
|---|---|---|
| <input type="checkbox"/> Property Protection Area | <input type="checkbox"/> Material Access Area | <input type="checkbox"/> Classified Information System Facility |
| <input type="checkbox"/> Limited Area | <input type="checkbox"/> Vital Area | <input type="checkbox"/> Secure Communication Center |
| <input type="checkbox"/> Exclusion Area | <input type="checkbox"/> SCIF | <input type="checkbox"/> Non-Security Area |
| <input type="checkbox"/> Protected Area | <input type="checkbox"/> SAPF/SSWA | |

2. Dates:

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 HQ	Date:
Inquiry completed	Date:
Inquiry Report transmitted to HQ	Date:
Incident officially closed	Date:

Follow-up:

Interim corrective actions implemented	Date:
Proposed corrective actions transmitted to HQ	Date:
GEN-16 policy applied by Classification Office	Date:
Damage Assessment completed	Date:

3. Identification:

Notifications

Initial Reporting Point of Contact (from DOE F 471.1)

Name:

Phone:

Organization:

Facility Security Officer:

Name:

Phone:

Organization:

DOE Cognizant Security Organization or HQ Representative:

Name:

Phone:

Organization:

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

Name:

Phone:

Organization:

Inquiry

Lead Organization and Inquiry Official:

Name:

Phone:

Organization:

Inquiry Official(s) at other affected sites:

Name:

Phone:

Organization:

Inquiry Participant(s)/Assistant Inquiry Officials: Check if inquiry lead

Name:

Phone:

Organization:

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

POC Name:

Phone:

Organization:

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

POC Name:

Phone:

Organization:

Individuals Involved

Responsible Individual(s):

Name:

Title:

Phone:

Organization:

Employer Facility Code and Name:

First Line Supervisor's Name:

Did this individual receive a written infraction for the incident? Yes No

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

Other Individual(s):

Name:

Title:

Phone:

Organization:

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. IMI Categorization

After selecting the correct IMI, the correct topical area must also be selected for some IMIs; when that is the case, select only the topical area that is most affected by the incident.

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

- 1.1 Confirmed or suspected loss, theft, or diversion of a nuclear device or components. < **NMC&A** or **PSS**>
- 1.2 Confirmed or suspected loss, theft, diversion, or unauthorized disclosure of weapon data. <IP>
- 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.** <IP>
- 1.6 **Confirmed or suspected intrusions, hacking, or break-ins into DOE computer systems containing TS information, SAP, or SCI.** <CSEC>
- 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.** <PSS>
- 1.8 Confirmed or suspected attacks against DOE Federal and contractor employees that adversely impact a facility's or site's security posture. <PSS>
- 1.9 Confirmed or suspected acts or attempts of terrorist-type actions. <PSS>
- 1.10 Confirmed reports of DOE or DOE contractor employees making threats against Departmental facilities, employees, or the U.S. Government <PSS>
- 1.11 Confirmed threats that immediately endanger personnel health or safety and may require immediate protective force/law enforcement intervention. <PSS>
- 1.12 Dangerous weapons and firearms-related incidents where an individual is killed wounded, or an intentional discharge occurs. <PF>
- 1.13 **Confirmed or suspected acts of sabotage, at any DOE facility, that places the safety or security of personnel, facilities, or the public at risk.** <PSS>
- 1.14 **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.** <CSEC>

- 1.15 **Confirmed compromise of root/administrator privileges in DOE computer systems containing Secret or Confidential information.** <CSEC>
- 1.16 **Confirmed intrusions into information systems containing classified information.** <CSEC>
- 1.17 **Instances of malicious code that cause disruption, degradation, or compromise of information systems for an entire site/facility.** <CSEC>
- 1.18 Instances of malicious code that allow unauthorized or undetected access to information systems containing classified information (Top Secret, Secret, Confidential, SAP information, or SCI). <CSEC>
- 1.19 Other (describe):
< IP, CSEC, NMC&A, PSP, PSS, PF, PMS or FVA>

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

- 2.1 Suspected loss, theft, or diversion of any radioactive material not categorized as special nuclear materials (SNM), or dangerous materials that could pose a health threat or endanger security. < NMC&A or PSS>
- 2.2 Confirmed or suspected intrusions, hacking, or break-ins into DOE computer systems containing Secret or Confidential classified information. <CSEC>
- 2.3 Any amount of SNM found in an exceptionally dangerous/hazardous unapproved storage environment, or unapproved mode of transportation/transfer. < NMC&A or PSS>
- 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.** <IP>
- 2.7 Actual or suspected technical interceptions of any level of classified information. <CSEC>
- 2.8 Actions, by electronic or physical means, that interfere with any DOE safeguards and security practices. < IP, CSEC, NMC&A, PSP, PSS, or PF>
- 2.9 Notifications, by any media or source, of validated threats that do not appear to immediately threaten personal safety or health. <PSS>
- 2.10 Loss of classified information that must be reported to other Government agencies or foreign organizations. <IP>
- 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. < IP or PSS>
- 2.12 **The loss of any DOE classified interest that requires State or local government or other Federal agency notification.** <IP>
- 2.13 **Confirmed compromise of root/administrator privileges in DOE unclassified computer systems.** <CSEC>
- 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.** <CSEC>
- 2.15 **Potential compromise of root/administrator privileges in DOE computer systems containing classified information.** <CSEC>
- 2.16 **Instances of malicious code that cause disruption/degradation or compromise of information systems dedicated to safety, security, or critical operations.** <CSEC>
- 2.17 Detection of activities involving individuals who have been confirmed as physically watching/casing/surveillance a site in an effort to gather information to aid in the conduct of a terrorist-type attack. <PSS>
- 2.18 Other (describe):
< IP, CSEC, NMC&A, PSP, PSS, PF, PMS or FVA>

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.

- 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. <PSS>
- 3.3 Confirmed or suspected unauthorized disclosure, loss, or potential loss of Confidential matter by any medium, method, or action.** <IP>
- 3.4 Confirmed or alleged noncompliance with laws or DOE directives/standards that jeopardizes protection of the facility or site security interests.** <PSS>
- 3.5 Demonstrators or protestors that cause site and facility damage. <PSS>
- 3.6 Labor strikes that could degrade or impede the required protection of the facility or site. < PSS or PF>
- 3.7 Physical violence or threat of retaliation against facility security personnel. <PSS>
- 3.8 Dangerous weapons and firearms-related incidents involving protective force operations/personnel where an unauthorized weapon discharge occurs. <PF>
- 3.9 Loss or theft of DOE firearms or ammunition, per DOE M 470.4-3, Protective Force. <PF>
- 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. <PSS>
- 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 unclassified controlled information.** <PSS>
- 3.12 Confirmed or suspected malicious activities, including but not limited to stealing badges or vehicle licenses.** <PSS>
- 3.13 Discovery of malicious activities, disorderly conduct, or vandalism that disrupts facility activities or causes damage between \$10K and \$100K. <PSS>
- 3.14 Circumvention of established access control procedures into a security area (excluding Property Protection Area). <PSS>
- 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.** <CSEC>
- 3.19 Confirmed intrusions into unclassified information systems that are not publicly available (e.g., behind a firewall).** <CSEC>
- 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). <CSEC>
- 3.21 Unauthorized network scans/probes on information systems possessing classified information. <CSEC>
- 3.22 Incidents of apparent surveillance of facilities or operations (studying, photographing, low overflights, outsiders questioning employees or protective force, unusual calls for information, etc.). <PHYSEC>
- 3.23 Other (describe):
< IP, CSEC, NMC&A, PSP, PSS, PF, PMS or FVA

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.

- 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.** <IP>
- 4.6 Non-credible bomb threats at any DOE nuclear or non-nuclear facility. <PSS>
- 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.** <IP>
- 4.8 Peaceful demonstrations or protests that do not threaten facility or site security interests or activities. <PSS>
- 4.9 Failure to adhere to established procedures contributing to the misuse or misprocessing of or failure to maintain security badges and passes.** < PSP or PSS>
- 4.10 Loss of security badges in excess of 5 percent of total issued during 1 calendar year.** <PSS>
- 4.11 Failure to adhere to established procedures contributing to the mismanagement or faulty application of the DOE Human Reliability Program.** <PSP>
- 4.12 Failure to adhere to established administrative procedures contributing to problems with foreign visitors. < IP, CSEC, NMC&A, PSP, PSS, or PF>
- 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.** <CSEC >
- 4.14 Unauthorized cellular phones and personal electronic devices (e.g., PDA's) introduced into a Limited Area, Protected Area, or Material Access Area, where there is no potential for compromise of classified or unclassified controlled information. <PSS>
- 4.15 Circumvent established access control procedures into a Property Protection Area. <PSS>
- 4.16 High rate/amount of loss (excluding natural disasters) or theft of Government property. <PSS>
- 4.17 Other (describe):
< IP, CSEC, NMC&A, PSP, PSS, PF, PMS or FVA>

5. Classified Matter Description. *Completed for incidents involving classified matter*

Type

Disclosure Type(s): (check all that apply)

- Unsecured/Improperly Secured
 - In Use
 - Reproduction
 - Storage
 - Destruction
- Unclassified Computer used to process/store

- Improper Transmission
 - o E-Mail
 - o Facsimile
 - o Hand Carry
 - o Mail/Shipping/Express Delivery
- Unapproved Facility (including private residences) used to process/store
- Verbal
- Media Leak
- Classification Issue
 - o Failure to Receive Classification Review
 - o Information Compilation
 - o Guidance Issue
 - o Classifier did not have Authority to Make Classification
 - o Misclassification
- Improper Escort
- Controlled Article
- Other (describe):

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

- Electronic Storage Media
- E-Mail
 - o Inside Firewall
 - o Outside Firewall
- Facsimile
- Hard Copy
- Internet
- Visual
- Multimedia
- Discussion (Audio/Verbal)
- Other (describe):

Identify the owner of the information:

Did the matter involved belong to an "Other Government Agency?" Yes No
If "Yes," Identify Other Government Agency(s) involved:

Did the matter involve Work for Others?" Yes No

Classification

Classification Level:

- Top Secret
- Secret
- Confidential

Classification Category:

- Restricted Data
- Formerly Restricted Data
- National Security Information

Caveats: (check all that apply)

- Weapons Data (WD) Identify SIGMAs (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):

Description

Describe the classified matter lost, compromised, or potentially compromised (e.g., document title and date, description of matter):

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:

Phone:

Organization:

6. Narrative:

Brief description of the incident (for incidents involving classified matter, identify classification level, category, and any identifiers):

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 in DOE Manual 470.4-1, Safeguards and Security Program Planning and Management, Section N, *Incidents of Security Concern*, dated 8-26-05. (Specifics captured elsewhere in this report may be excluded):

7. Containment:

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

8. Factors:

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

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

9. Determination:

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):

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
- None

Summary.

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

Damage Assessment

Has the Program Office requested a Damage Assessment? Yes No

Was the damage assessment completed (formal and/or informal)? Yes No
If you chose "Yes," you must insert a date in 2. Dates - Follow-Up – Damage Assessment Completed.

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

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
- 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):

10. Corrective Actions:

Corrective Action Taken

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 must be forwarded to DOE/HS):

Management Official(s) responsible for Corrective Actions:

Name:

Organization:

Phone:

Corrective Action Process

Describe corrective action steps:

Describe the results achieved:

Remedial actions which will be taken to prevent recurrence:

The date by which full compliance will be achieved:

11. Disciplinary Actions:

Action(s) 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):

Are there mitigating factors affecting disciplinary action? Yes No

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

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

Are there aggravating factors affecting disciplinary action? Yes No

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

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

Management Official(s) responsible for Disciplinary Actions:

Name:

Phone:

Organization:

12. Comments:

Other Comments

Include any comments associated with the incident:

Security Enforcement Screener/Analyst:

Name:

Date:

Security Enforcement Reviewed/Approved:

Name:

Date:

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

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

Describe media attention:

Check here if this incident has any association with a foreign national(s):

Record Classification

Classification/Marking Official who made the classification/marketing determination for the DOE F 471.1:

Name:

Phone:

Marking of DOE F 471.1

- Secret Formerly Restricted Data (S/FRD)
- Secret Restricted Data (S/RD)
- Secret National Security Information (S/NSI)
- Confidential Formerly Restricted Data (C/FRD)
- Confidential Restricted Data (C/RD)
- Confidential National Security Information (C/NSI)
- Official Use Only (OUO)
- Unclassified Naval Nuclear Propulsion Information (UNNPI)
- Unclassified Controlled Nuclear Information (UCNI)
- Unclassified

Classification/Marking Official who made the classification/marketing determination for this record:

Name:
Phone:

Marking of this Record:

- Secret Formerly Restricted Data (S/FRD)
- Secret Restricted Data (S/RD)
- Secret National Security Information (S/NSI)
- Confidential Formerly Restricted Data (C/FRD)
- Confidential Restricted Data (C/RD)
- Confidential National Security Information (C/NSI)
- Official Use Only (OUO)
- Unclassified Naval Nuclear Propulsion Information (UNNPI)
- Unclassified Controlled Nuclear Information (UCNI)
- Unclassified

Record Caveats (check all that apply)

- Weapons Data (WD) Identify SIGMAs (1-5, and 9-15) involved: _____
- Foreign Government Information (FGI)
- Naval Nuclear Propulsion Information (NNPI)
- No Foreign Dissemination (NOFORN)

Time and Funds Expended on Incident:

Total Hours:
Total Costs:
Comments: