



**NOT MEASUREMENT
SENSITIVE**

DOE-STD-1210-2012
September 2012

DOE STANDARD

Incidents of Security Concern



U.S. Department of Energy
Washington, D.C. 20585

AREA SANS

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

INTENTIONALLY BLANK

TABLE OF CONTENTS

<u>PARAGRAPH</u>	<u>PAGE</u>
FOREWORD	IV
INCIDENTS OF SECURITY CONCERN.....	1
1. SCOPE	1
2. PURPOSE	1
3. APPLICABILITY	1
4. REFERENCES	1
5. ACRONYMS AND DEFINITIONS	1
6. DUTIES, RESPONSIBILITIES AND TRAINING	1
6.1 Inquiry Official	1
7. IOSC PROCESS STEPS	2
7.1 IOSC Initiation	2
7.2 Containment/Mitigation	2
7.3 Preliminary Inquiry	2
7.4 Categorization	3
7.5 Initial Notification and Reporting	3
7.6 Main Inquiry	3
7.7 Incident Assessment and Risk Ranking	5
7.8 Corrective Action	6
7.9 Effectiveness Reviews.....	7
7.10 Incident Tracking	7
7.11 Incident Trending	8
7.12 Lessons Learned	8
7.13 Integration	9
7.14 Close-out Documentation.....	9
7.15 Final Reporting.....	11
APPENDIX A. TABLES.....	A.1
APPENDIX B. DECISION TREES	B.1
APPENDIX C. DOE O 470.4B SSIMS NOTIFICATION AND INQUIRY OUTLINES	C.1
APPENDIX D. IOSC SCENARIOS.....	D.1
8. CONCLUDING MATERIAL	37

FOREWORD

This Department of Energy Technical Standard is for use by all DOE elements.

Comments (recommendations, additions, and deletions) and any other pertinent data that may improve this document should be mailed to the U.S. Department of Energy; Office of Health, Safety, and Security; Office of Security Policy, GTN/HS-51; 1000 Independence Ave., SW; Washington, DC 20585-1290, or emailed to Sabeena Khanna at sabeena.khanna@hq.doe.gov.

DOE Technical Standards do not establish requirements. However, all or part of the provisions in this Standard can become requirements under the following circumstances:

1. They are explicitly stated to be requirements in a DOE requirements document (e.g., a purchase requisition);
2. The organization makes a commitment to meet a Standard in a contract, implementation plan, or program plan; or
3. When incorporated into a contract.

Throughout this Standard, the word “shall” is used to denote actions to be performed if the objectives of this Standard are to be met. If the provisions in this Standard are made requirements through one of the three ways discussed above, then the “shall” statements would become requirements. Goals or intended functionality are indicated by “should.” It is not appropriate to consider that “should” statements would automatically be converted to “shall” statements as this action would violate the consensus process used to approve this standard.

This Standard was prepared following requirements for due process, consensus, and approval as required by the U.S. Department of Energy Standards Program. Consensus is established when substantial agreement has been reached by all members of the writing team and the Standard has been approved through the DOE directives approval process (REVCOM). Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made toward their resolution.

INCIDENTS OF SECURITY CONCERN

1. SCOPE

This Technical Standard describes establishing and maintaining a quality incident of security concern (IOSC) program. Each site/facility establishes an IOSC program to ensure that the occurrence of a security incident prompts the appropriate graded response including an assessment of the potential impacts, appropriate notifications/reporting, extent of condition, and corrective actions. The long-term management of incidents serves as an effective safeguards and security (S&S) program planning and management tool for enhancing site-specific implementation of security policies, as well as preventing the reoccurrence of IOSCs and improving S&S performance.

Under DOE O 470.4B, Safeguards and Security Program, site/facility operators have many alternatives with regard to how their IOSC program is designed, managed, and operated. This Technical Standard describes one method, commonly used throughout the U.S. Department of Energy (DOE)/National Nuclear Security Administration (NNSA) that can be used to achieve the desired compliance.

2. PURPOSE

The purpose of this technical standard is to provide site/facility operators with a compliance-based means that is acceptable in meeting DOE standards for IOSC policy requirement objectives.

3. APPLICABILITY

This technical standard can be used by all site/facility operators within the DOE and NNSA complex.

4. REFERENCES

References commonly used in the DOE S&S Program to include the IOSC Policy within DOE O 470.4B and other S&S directives are located in the S&S Policy Information Resource (PIR) website located at (<http://pir.pnl.gov>).

5. ACRONYMS AND DEFINITIONS

Acronyms and definitions commonly used in the DOE S&S Program are located in the S&S PIR website located at (<http://pir.pnl.gov>). In addition to the PIR, pertinent IOSC definitions can be found in Table A.1, Definitions Associated with the DOE IOSC Program.

6. DUTIES, RESPONSIBILITIES AND TRAINING

6.1 INQUIRY OFFICIAL

Inquiry officials are responsible for conducting the inquiry and maintaining all documentation associated with the inquiry. Inquiry officials may be either Federal or contractor employees and shall be appointed in writing by the designated Federal entity(s). At a minimum, inquiry officials shall have previous investigative experience or Departmental inquiry official training (preferably both) and be knowledgeable of appropriate laws, executive orders, Departmental S&S directives, and/or regulatory requirements. Inquiry officials should be trained in conducting causal analyses. Inquiry officials and members of inquiry teams should be well trained and able to demonstrate their proficiency or working knowledge of a variety of skills necessary to conduct effective inquiries. These skills include, but are not limited to, investigative techniques, conducting interviews, report writing, causal and trending analyses, and human performance assessments.

6.1.1 Training

Individuals who conduct inquiries should enhance and maintain their competency by completing other courses relevant to conducting inquiries, periodic in-house training, and membership in associations of security professionals. Examples of additional training courses beneficial to an inquiry official include:

- Physical Security Systems course offered through the DOE National Training Center (NTC).
- Information Security courses offered through the NTC.
- International Association of Computer Investigative Specialists (IACIS) offers a 2-week basic course in computer forensics.

7. IOSC PROCESS STEPS

The IOSC process generally involves a series of steps starting with the IOSC initiation and concluding with final reporting. The appendices section of this Standard contains resource tools to be used throughout the IOSC process.

- Table A.1, Definitions Associated with the DOE IOSC Program
- Table A.2, IOSC Categorization Matrix
- Table A.3, IOSC Risk Ranking Score Sheet
- Figure B.1, Improper Storage of Classified Matter
- Figure B.2, Processing Classified Information on an Unapproved Computer System
- Figure B.3, Unauthorized Introduction of Controlled Articles
- Figure B.4, Unauthorized Network-Based Transmission of Information
- Appendix D, IOSC Scenarios

7.1 IOSC INITIATION

The IOSC initiation process is the point in time when an event is brought to the attention of management. Preliminary inquiry should immediately be initiated to determine if a security incident has or has not occurred and include the need for classification determination.

7.2 CONTAINMENT/MITIGATION

Upon notification of a potential IOSC, the reporting party and/or the inquiry official initiates the appropriate immediate action to stabilize and/or place the security related item(s) in a secure and safe location/condition (e.g., collection/storage of potentially classified documents; obtain classification review; isolation of contaminated systems, back-ups, or other information storage devices; etc.) to preclude further potential compromise. When necessary, engage appropriate technical personnel. Notifications, via secure means, to affected sites/entities should be made as soon as possible. Immediate actions should be taken to preserve conditions and protect potential evidence for further inquiry.

7.3 PRELIMINARY INQUIRY

The preliminary inquiry consists of gathering facts to determine if an IOSC has occurred. Verbal interviews, gathering of potential evidence, and documentation of an IOSC should be conducted. If the inquiry official determines that sufficient evidence/facts exist to conclude that an IOSC has occurred, the

next step is categorization of the incident. If the inquiry official determines that an IOSC has not occurred, no further action is necessary.

7.4 CATEGORIZATION

DOE/NNSA uses a graded approach for the identification and categorization of IOSCs. Based on the preliminary inquiry and determination that an IOSC has occurred, DOE O 470.4B should be referred to for the reporting criteria and determination of the significance level category and incident type. While not all incidents fit neatly into any one category, it is the responsibility of the reporting organization¹ to determine which level and incident type best describes the incident. Justification for the categorization (i.e., significance level and type) of the incident should be included in the initial notification. Consultation with the local site office or DOE HQ is a viable option for accurately determining the significance level/type of atypical incidents. Procedures for determining the significance level and type of incidents shall be contained in the IOSC program plan.

7.5 INITIAL NOTIFICATION AND REPORTING

The reporting organization has a maximum of 5 calendar days to categorize IOSCs. Once the IOSC is categorized it should be reported through approved methods. If uncertainty still exists at the end of 5 days, the incident should be tentatively reported as a Category A incident. If additional facts or details about the incident are discovered through the inquiry, the incident can be re-categorized.

Once a decision has been made that a reportable incident has occurred and has been categorized, an inquiry shall be initiated. The reporting organization should immediately notify all stakeholders (e.g., Federal Site Office CSO, site/facility management, etc.) in addition to entering the appropriate details in SSIMS. SSIMS is the designated system for notification and reporting to Headquarters for all Category A incidents. If SSIMS is unavailable, an appropriate secure fax notification to the DOE Emergency Operations Center is acceptable. In extreme cases where SSIMS or the DOE Emergency Operations Center fax line is not available, an appropriate secure telephonic notification to the DOE Emergency Operations Center with a fax or SSIMS follow-up is also acceptable. Appendix C.1, DOE 470.4B S&S Information Management System (SSIMS) Notification Outline, identifies the SSIMS process for initial notification.

Category B incidents shall be entered in SSIMS or a local system identified in the site's/facilities IOSC program plan. The local system shall contain enough data to track issues and support trending and analysis. The reporting organization should notify all stakeholders (i.e., site management and site management CSO, field office IOSC program manager, etc.), as applicable.

7.6 MAIN INQUIRY

7.6.1 Data Collection

Collect all data/information relevant to the incident, such as operations logs, inventory reports, requisitions, receipts, photographs, signed statements, documents, etc. Conduct interviews to obtain additional information regarding the incident. 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, access logs, and readouts from monitoring equipment, etc. Ensure physical evidence is protected and controlled and a chain of custody be maintained. Original exhibits should be maintained in the case file.

¹ The reporting organization is the Contractor cognizant security office (CSO) and/or their designee.

7.6.2 Incident Reconstruction

Reconstruct the incident to the greatest extent possible using collected information and evidence. Develop a chronological sequence of events that describes the actions preceding and following the incident. Identify persons associated with the incident.

7.6.3 Reporting and Documentation

Inquiry reports shall describe the conduct and results of the inquiry. The information captured shall meet the requirements as outlined in DOE O 470.4B. Additionally, inquiry reports should include at least an executive summary and a narrative that includes the following:

- The pertinent information to the location, building/room numbers, date and time information, notifications made, the incident inquiry, detailed description of the incident and other time related actions pertaining to the incident;
- A complete discussion of the facts and circumstances surrounding the incident, including a description of all supporting information, such as the following:
 - Documentation and evidence of information obtained to mitigate the likelihood of compromise;
 - Identification of all personnel involved in the incident, including those associated with the inquiry process, and when they were notified;
 - Identification of the causes and corrective actions for the incident and descriptions of mitigating or aggravating factors that may reduce or increase the impact of the incident;
 - Descriptions of the actions that precipitated the incident;
 - Descriptions of all physical evidence, including all records/documents reviewed;
 - Results of any interviews performed to include copies of any signed statements of involved individuals.
 - Descriptions of actions taken to minimize vulnerabilities created by the incident and prevent further loss/compromise of the security interest;
 - Results of the extent of conditions review.
- If the incident involves classified matter, the following should also be included:
 - A description of the potentially compromised classified matter, including but not limited to classification level, category, caveats, and its physical form. A copy of the evidence or photograph should be maintained and provided to DOE HQ if requested;
 - The classification guide and topic or source document including date of guide or source document;
 - Known recipients of the potentially classified matter;
 - Owner of the classified matter, (e.g., program office or other Government agency);
 - The reporting organization's conclusion and the basis/facts that support the conclusion and the potential risk to security.
 - The inquiry report shall contain supporting documentation of factors used to determine that loss, theft, compromise or suspected compromise did not occur or the likelihood of compromise is remote.

7.7 INCIDENT ASSESSMENT AND RISK RANKING

An incident assessment facilitates development of a set of corrective actions that will reduce the likelihood of the incident recurring, and establishes the criteria for measuring the effectiveness of those actions. The level of effort and detail for these assessment activities needs to be commensurate with the level of risk associated with the incident being assessed.

The incident assessment process begins with a risk ranking, which then drives the graded approach to causal analysis, corrective actions and follow up effectiveness reviews and tracking/trending of incident data. Table A.3, IOSC Risk Ranking Score Sheet, describes a risk ranking process that can be used to objectively determine the level of risk caused by an incident.

Incidents are ranked as High, Medium or Low risk. The ranking is determined by scoring a predetermined number of incident elements and adding up the scores. Based on the final total, the incident is then graded as High, Medium, or Low.

The specific elements that are ranked and the scoring criteria used should be established in the IOSC program plan. Typical elements that are included in risk ranking include classification of material involved, location of incident, likelihood of compromise, intent (i.e., willful, negligence, inadvertent), management involvement, mission impact, external reaction (i.e., publicity), and resource loss/damage.

Risk ranking is done early in the incident inquiry process and before the causal analysis is completed. It is possible that as more information is uncovered during the inquiry and/or causal analysis that the risk ranking could change. In this case, a new risk ranking should be performed using the new data. If this results in a change in risk, the causal analysis, corrective actions, and effectiveness review activities should be modified accordingly.

7.7.1 High Risk Incidents

For all incidents ranked High risk, a formal causal analysis should be performed in accordance with the organization's cause analysis process. High risk incidents require a thorough and in-depth causal analysis that gives senior management a high degree of certainty that the root causes are properly identified, and that effective corrective actions are put in place to address those causes. The causal analysis for High risk incidents should be chartered (sponsored) by the organization's senior management. At a minimum, the causal analysis should:

- be conducted by an analysis team led by a qualified Causal Analyst (determined by organizational qualification requirements).
- include all data collected by the inquiry official during the inquiry and/or critique. Additional data (physical evidence, interviews, documentation) should be gathered as needed.
- use at least one structured causal analysis method (change analysis, barrier analysis, tree analysis, events & causal factors charting, Management Oversight and Risk Tree (MORT)). In most cases, additional methods should be used to validate the causes. The choice of methods should be chosen by the lead analyst, and will probably be driven (to some extent) by the significance of the incident.
- identify direct, contributing, and root causes, as appropriate. Depending on the complexity of the event, it is not uncommon to identify several causes that all should be addressed in order to minimize likelihood of incident recurrence.
- incorporate Human Performance Improvement analysis (when human errors are identified as causes).
- include extent of condition/extent of cause analysis as appropriate.

7.7.2 Medium Risk Incidents

For all incidents ranked Medium risk, a formal causal analysis should be performed in accordance with the organization's cause analysis process. Medium risk incidents require a thorough cause analysis to give management confidence that the root causes are properly identified and that corrective actions are put in place to address those causes. The causal analysis for Medium risk incidents should be chartered (sponsored) by the department/division manager responsible for the incident. At a minimum, the causal analysis should:

- be conducted by a qualified Causal Analyst (determined by organizational qualification requirements). Depending on the complexity of the incident, a causal analysis team may be necessary rather than a single individual.
- include all data collected by the inquiry official during the inquiry and/or critique. Additional data (physical evidence, interviews, documentation) should be gathered as needed.
- use at least one structured causal analysis method (change analysis, barrier analysis, tree analysis, events & causal factors charting, MORT). The choice of methods should be chosen by the lead analyst, and will probably be driven (to some extent) by the significance of the incident.
- identify direct, contributing, and root causes, as appropriate. Depending on the complexity of the event, it is not uncommon to identify several causes that all should be addressed in order to minimize likelihood of incident recurrence.
- incorporate Human Performance Improvement analysis (when human errors are identified as causes).
- include extent of condition/extent of cause analysis if warranted by circumstances of the incident.

7.7.3 Low Risk Incidents

For all incidents ranked as Low risk, an informal causal analysis, conducted by a causal analyst (preferably formally qualified by the organization) should be performed in accordance with the organization's cause analysis process. Informal techniques that are typically used include the "Five Whys" Human Performance Improvement (for incidents involving human error) or use of intuition/experience with the organization's processes.

All causal analysis activities and results should be documented, either within the inquiry report, or as an attachment.

7.8 CORRECTIVE ACTION

Once causes (direct, contributing, root) are identified, a set of corrective actions are developed to specifically address the causes. Organizations should choose whether to have the causal analyst (or team) recommend a set of corrective actions that are included in the causal analysis report. It is also acceptable to have a separate group or person develop corrective actions.

Overall ownership of the corrective action plan belongs to the organization's division/directorate responsible for the incident. The corrective action plan should be approved by that group's manager.

Each cause identified in the causal analysis should have at least one corresponding corrective action. In some cases, it is appropriate for a single action to satisfactorily address more than one cause. For all High risk incidents, and when deemed appropriate for Medium and Low risk incidents, a matrix that cross walks actions to causes should be included in the corrective action plan.

Corrective actions should be assigned to specific individuals. Individuals should be assigned actions based on the risk ranking of the incident and their roles, responsibilities, authorities, and accountabilities. A common error in corrective action planning is to assign an action to an individual who does not have the authority and/or resources necessary to successfully complete the action.

Corrective actions should be as specific as possible, with clearly defined deliverables and due dates that are commensurate with the level of effort required and the urgency to get the action completed.

Once approved, corrective actions should be tracked to completion using the organization's issues management/action management processes, typically in an action tracking system. Regular review of action status should be conducted for open actions. In the event that an action will not be completed on time, the action owner should work with the responsible manager to determine if the action plan should be updated to reflect a change in the action activity and/or due date.

All actions, once completed, should be validated. Validation consists of an independent review of the action that assures it was completed. A validation may include an interview of the action owner, review of documentation, spot check of records, or any other activity that demonstrates the action was completed. For High risk and Medium risk incidents, validation activities should be documented, either within the organization's issues/action tracking system, or in the incident report file. Low risk incident action validations should be noted as completed in the incident report file.

7.9 EFFECTIVENESS REVIEWS

Effectiveness reviews are conducted after corrective actions are completed to determine if the corrective actions have had the desired effect. Effectiveness reviews should not be confused with action validation; validation is confirmation that an action was completed- effectiveness reviews confirm that the actions are effective and are having the intended effect.

Effectiveness reviews should be scheduled after the corrective action has been implemented, allowing sufficient time for the actions to take effect.

When conducting an effectiveness review, the organization should refer to the original incident and causal analysis for context. The reviewer should then conduct interviews, review documents, evaluate system performance and/or complete other assessment tasks that measure the effectiveness of the action.

If an action is determined to be ineffective or unsustainable (i.e., the action taken does not have the desired effect of mitigating the likelihood of an incident recurring), additional corrective actions should be developed and approved by the responsible manager. These additional actions should be documented in the incident report file.

The results of effectiveness reviews should be included in the incident report files.

Effectiveness reviews should be conducted for all actions associated with High risk incidents. For Medium and Low risk incidents, effectiveness reviews should be considered and completed on a case by case basis.

7.10 INCIDENT TRACKING

Tracking of IOSCs is necessary to assure all associated activities (e.g., critiques, inquiries, causal analyses, corrective actions, effectiveness reviews, reporting) are completed in a timely manner.

Organizations should establish an incident tracking system that assigns unique numbers to each reported incident. The tracking system could be electronic or paper based, and should include fields such as description, date of critique, date of causal, corrective action plan submittal, closeout information, etc. The tracking system should be used as a tool to verify that all required activities associated with each event are completed satisfactorily and in a timely manner.

The sensitivity and classification of incident data is such that it is likely that the tracking system will contain classified information. Organizations should consider keeping the tracking system on a classified computer/network, or limit the detail of data in the tracking system to avoid classification issues.

NOTE: Limiting the detail of data to avoid classification issues can severely degrade the effectiveness of the tracking system.

7.11 INCIDENT TRENDING

Trending of incident data serves two primary purposes: 1) it assists an organization in identifying programmatic and/or systemic issues that might not be noticeable when data is reviewed separately and independently, and 2) it assists with identifying potential areas of weakness exposed by lesser incidents (precursor activities) before a more significant event occurs.

Trending of incidents should be a continuous, ongoing activity by contractor organizations. Noted trends should be shared with the organization, and appropriate actions developed. At a minimum, organizations should complete an annual formal trend analysis of all incidents, with a timeframe that overlaps previous trend reports to provide continuity.

It is acceptable for the trending of incidents to be included in an organization's overall security trend report in support of its security regulatory program (i.e., 10 CFR Part 824). In addition to incident data, contractor organizations should trend assessment results, findings, performance assurance data, and operational feedback ('find-it-fix-its') from various security program elements.

An effective trend analysis includes both statistical (when sufficient numbers of data points exist) and empirical analysis.

The trend analysis should not focus on just the number of incidents. It should include trending of factors such as the types of incidents, responsible organizations, location, dates, and causes. Tables and charts should be used to aid in viewing the data to help spot potential trends.

The analysis should give contextual consideration to organizational characteristics such as the number of cleared employees, amount and location of classified holdings, types and numbers of classified projects and programs, and other relevant characteristics.

7.12 LESSONS LEARNED

The organization's security education and awareness program should work closely with the IOSC program to identify topics where the lessons learned as a result of incidents can be shared with staff members in a proactive and timely manner. Every incident should be evaluated for potential lessons learned material, and if deemed appropriate, development of a Lessons Learned article should be included as a corrective action.

7.13 INTEGRATION

Integration of the site IOSC program with the larger S&S program management function will influence other functional areas as well as enhance site-specific implementation of security policies. The IOSC program is generally reactive, in that it is responsible for effectively managing incidents after they have already occurred. However, a narrowly focused, reactive approach in managing IOSCs is not sufficient in meeting DOE's expectations for protection of classified information and high value assets.

The IOSC program should be fully integrated into the organization's program planning and management function, and proactively integrate incident awareness into everyday operations by keeping lines of communication open. Inquiry personnel should be available to answer questions, provide guidance, and assist in identifying potential security risks and incident precursors. Two way communications between the two programs should provide feedback from recent IOSCs and IOSC trends that help direct program priorities such as:

- prioritizing funding and planning of protection strategy projects,
- focusing self-assessments on current topics of interest,
- sharing lessons learned and other awareness and education activities with organization staff.
- apprising the IOSC program of organizational goals, mission activities, and operational status that can facilitate incident response, causal analyses and corrective action planning.

7.14 CLOSE-OUT DOCUMENTATION

7.14.1 Category A Incidents

Category A inquiry reports should clearly describe the conduct and results of the inquiry and include the following information for the incident to be closed (the information captured needs to meet the requirements as outlined in DOE O 470.4B).

- An executive summary.
- A narrative, which includes the following:
 - The date and time of incident, any notifications, the incident inquiry, and other time related actions pertaining to the incident.
 - All data pertinent to the location of an incident, including the facility name and facility code, 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.
 - A complete discussion of the facts and circumstances surrounding the incident, including a description of all supporting information, such as the following:
 - Detailed description of the incident of security concern.
 - Identification of all personnel involved in the incident and when they were notified, including those associated with the inquiry process.
 - Identification of the causes and corrective actions for the incident, descriptions of mitigating or aggravating factors that may reduce or increase the impact of the incident.
 - Descriptions of the actions that precipitated the incident.
 - Descriptions of all physical evidence, including all records/documents reviewed.

- Results of any interviews performed.
- Descriptions of actions taken to minimize vulnerabilities created by the incident and prevent further loss/compromise of the security interest.
- If the incident involves classified matter, the following should also be included:
 - A description of the potentially compromised classified matter, including but not limited to classification level, category, caveats, and form. A copy of the evidence or photograph needs to be maintained for future reference.
 - The classification guide and topic or source document including date of guide or source document.
 - Known recipients of the potentially classified matter.
 - Owner of the classified matter, (e.g., program office or other Government agency).
- An Inquiry Official's conclusion and the basis/facts that support the conclusion. This conclusion needs to address the potential risk to the security interest based upon the documented evidence and a subjective analysis of the facts and circumstances surrounding the incident of security concern.
- The final report needs to identify the management officials responsible for corrective and disciplinary actions.
- The following shall be included as attachments to the inquiry report:
 - A copy of any signed statements of involved individuals.
 - A description of the compromised or potentially compromised information as appropriate.
 - Documents obtained during the data collection phase of the inquiry.
 - For incidents involving compromise or potential compromise of classified information, ensure that the additional requirements of DOE O 470.4B are followed and included in the inquiry and final report.
 - If applicable, the results of the Extent of Condition Review.

7.14.2 Category B Incidents

Category B inquiry reports shall be documented at a level that appropriately captures the situation in the entirety of the event and meets the requirements as outlined in DOE O 470.4B.

- Inquiry reports need to describe the conduct and results of the inquiry and include the following information for the incident to be closed:
 - Location,
 - Dates and times,
 - Names, titles of persons contacted or involved, including a record of prior incidents for which the individual had been determined to be responsible
 - Events leading up to the IOSC
 - Narrative describing the facts and circumstances of the IOSC
 - If applicable, the results of the Extent of Condition Review.

- Ensure that documented evidence has been obtained that rules out, or mitigates, the likelihood of compromise (i.e., mitigating/aggravating factors - omni lock audit, access authorization and need to know).
- Reason for cause
- Corrective action, to include disciplinary action, if applicable

7.15 FINAL REPORTING

7.15.1 Category A Incidents

Prior to closure the DOE/NNSA CSO shall review all category A incidents and determine if the incident warrants a damage assessment.

Category A incidents are considered closed upon completion of the inquiry report, review by DOE/NNSA CSO, and entry into SSIMS. Appendix C.2, DOE O 470.4B SSIMS Inquiry Outline describes the SSIMS process. The final closure report shall be submitted within 90 calendar days of preliminary incident notification. Extensions for closure can be submitted as outlined in the site IOSC program plan.

7.15.2 Category B Incidents

Category B incidents can be closed using SSIMS, or a locally approved system identified in the IOSC program plan. The inquiry report shall contain supporting documentation of factors used to determine that loss, theft, compromise or suspected compromise did not occur or the likelihood of compromise is remote.

INTENTIONALLY BLANK

APPENDIX A. TABLES

Table A.1. Definitions Associated with the DOE IOSC Program

Arrest	Any act—including taking, seizing, or detaining of a cleared DOE or DOE contractor enrolled in the Human Reliability Program—that indicates an intention to take a person into custody and that subjects the person to the control of law enforcement personnel.
Compromising Emanations	Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by telecommunications or automated information systems equipment.
Cyber Incident Resulting in Compromise of Information	Cyber-related incidents/events where a compromise of information occurred in conjunction with an Enterprise Incident Capability incident. If an Enterprise Incident Capability incident does not involve the compromise of information as outlined in the Information Security table, the reporting process remains within the OCIO program.
Degradation of Security	Facility wide disruption/degradation of the security posture resulting from a natural or man-made event.
Demonstrations/Protest	A peaceful demonstration (20 or more participants) of disapproval, complaint, or display of unwillingness usually to an idea or course of action. Note: This assumes it is peaceful; if not, then it falls under the <i>hostile act</i> entry in this table.
Extent of Condition	The extent to which the actual condition exists in other areas within the organization.
Gross Negligence	An act that shows recklessness or willful disregard for the protection of DOE security interests. Gross negligence requires more than just neglect of ordinary care toward a security interest or just inadvertence. For example, a person may circumvent prescribed procedures with full knowledge of the security requirements and associated penalties but does so for personal convenience with little concern for the compromise or potential compromise of the security interest. Although the individual may not intend to lose or compromise the security interest, a reasonable person would recognize that the act or omission has a high probability of such results. This type of noncompliance constitutes a violation of 18 USC 793 (f).
Hostile Act	An act directed against Departmental assets or personnel that, whether successful or unsuccessful, could result in damage or loss of Departmental property/assets, the environment, injury to Departmental or contractor employees, or the public.
Improper Access Control	Not following the proper process for permitting or denying access to information, facilities, or other types of security interests.
Improper Handling	Unauthorized movement from a material balance area within the designated security area boundary. Improper destruction, not in accountability, improper transporting, unapproved packaging (e.g., not double wrapped), marking issues, improper material surveillance requirements (e.g., two person rule), failure to obtain classification review, classifying information without authority or outside authority, discussion in an unapproved location.

Table A.1. (contd)

Improper Storage	An approved storage facility or container (e.g., vault, VTR, security container, etc.) for the protection of SNM, classified information, and/or other security interests that is not properly secured (e.g., locked and/or alarmed, or in a facility or container that is not approved for the storage of the particular security interest).
Inadvertent	An act during which a person carefully follows the prescribed procedures as he or she understands them, but the security interest is mishandled anyway. This type of noncompliance situation arises without any kind of risk/benefit analysis and is generally the result of ignorance of requirements or a systematic or procedural failure.
Inventory Difference	The difference between the nuclear material book inventory and the corresponding physical inventory within a material balance area that exceeds unresolved alarm limits.
Investigation	The conduct of an official inquiry that pertains to a criminal felony investigation.
Labor Strike	Strike or threat of strike that may impact the site's/facility's security posture.
Loss	The inability to locate classified matter, SNM, or other Departmental interest.
Media Event	A security event that results in interest by the media.
Negligence	An act during which (a) a person attempts to follow procedures in good faith but through carelessness or neglect mishandles a security interest, or (b) a person circumvents prescribed procedures with full knowledge of the security requirements and associated penalties but does so with a good faith expectation of an overriding programmatic gain without expectation of any compromise or potential compromise of the security interest. In the latter situation, the noncompliance arises with some degree of risk/benefit analysis, and the person assumes the risk without management's knowledge or approval. This type of noncompliance represents any knowing, willful, or negligent action contrary to the requirements of applicable DOE orders or regulations that does not constitute a violation or result in the actual loss of a security interest. Normally, this type of noncompliance is elevated above administrative and/or disciplinary actions when it results in the actual compromise or potential compromise of the security interest.
Non-Willful Intrusion	The inadvertent or unintended penetration of a security boundary by the public. This does not include authorized visitors.
On-Site Arrest	Any act, including taking, seizing or detaining of an employee or non-employee on DOE property, excluding public access areas, that indicates an intention to take a person into custody and that subjects the person to the control of law enforcement personnel.
Process Difference	An unresolved process difference that exceeds the MC&A-established limits.
Processing Information on an Unapproved Computer System	Processing classified information on an unapproved computer system.
Shipper-Receiver Difference	The unresolved difference between the measured quantity of nuclear material stated by the shipper as having been shipped and the measured quantity stated by the receiver as having been received that exceeds (i.e., gain or loss) established limits results.

Table A.1. (contd)

Significant Nuclear Defense Intelligence Losses	Defined by 50 USC 2656 as “any national security or counterintelligence failure or compromise of classified information at a facility of the Department of Energy or operated by a contractor of the Department that the Secretary considers likely to cause significant harm or damage to the national security interests of the United States.”
Suspicious Activity	Incidents determined or suspected to be apparent surveillance of facilities or operations (studying, photographing, low over-flights, outsiders questioning employees to include protective force, unusual calls for information, etc.).
Theft	The removal of Government property and/or materials from a DOE or contractor operated facility without permission or authorization and contrary to law. Note: Theft also encompasses the act of <i>diverting</i> materials and/or property.
Threats	Information suggesting the intent to attack or cause harm.
Transmission of Information on an Unauthorized Communication System	Transmission of classified (verbal or text) on an unapproved fax, phone, PDA, cell phone, etc.
Unauthorized Discharge	The discharge of a firearm under circumstances <u>other than</u> (1) during firearms training with the firearm properly pointed down range (or toward a target), or (2) the intentional firing at a hostile party when deadly force is authorized by 10 CFR 1047.7.
Unauthorized Introduction of Controlled Articles	Unauthorized carrying, transporting, or otherwise introducing or causing the introduction of any articles controlled because of their potential to be used to record or transmit information without authorization. Examples are recording equipment (audio, video, optical, or data), cellular phones, radio frequency transmitting equipment, etc.
Unauthorized Introduction of Prohibited Articles	Per 10 CFR 860, an “unauthorized carrying, transporting, or otherwise introducing or causing the introduction of any dangerous weapon, explosive, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property, into or upon any facility, installation, or real property subject to” 10 CFR 860.
Unauthorized Movement	From a material balance area where the removal crosses outside the designated security boundary (e.g., boundaries of a property protection area, LA, PA, or an MAA).
Unauthorized Network Based Transmission of Information	Email or other text message sent via an unclassified system/network/intranet that contains classified or controlled unclassified information not properly encrypted when required.
Unauthorized Recipient of Information	This event results in the disclosure of information to an <i>identifiable</i> recipient(s) who does not have the appropriate clearance level and/or the need to know. The disclosure can occur by a variety of possible mediums (e.g., verbal, hardcopy, visual, electronic, etc.).
Vital Area	A type of security area that is located within a PA and that has a separate perimeter and access controls to afford layered protection, including intrusion detection, for vital equipment.
Willful	An act during which a person, with full knowledge of the security requirements and associated penalties disregards or circumvents prescribed procedures with intent to remove a security interest from its proper place of custody or to conceal the loss, theft, abstraction, or destruction of said interest.

Table A.2. IOSC Categorization Matrix

Type	Category A	Category B
Security Interest (SI)	Generally includes loss, theft, compromise or suspected compromise of the following assets	
	Special Nuclear Materials (SNM)	
	All classified matter	Official Use Only, Official Use Only/Export Controlled Information (Ex 3), Unclassified Controlled Nuclear Information, Naval Nuclear Propulsion Information
	Radiological, chemical, or Biological materials indentified in DOE O 473.3	
	Security key or keycard based on the significance of the asset being protected (level I or II security keys)	Level III security keys
	Protective Force firearms, ammunition, explosives, and equipment identified in DOE O 473.3	
	DOE security badge that is the target of the theft	
	Matter of a foreign government that requires reporting based on established agreements and required protocols	
	Other assets determined by the DOE/NNSA CSO and/or contractor CSO	Other assets as determined by the DOE/NNSA CSO and/or contractor CSO
Management Interest (MI)	Generally does not involve Departmental assets but may have potential undesirable impacts requiring management notification. These incidents should be specified In the ISOC program plan	
	Incidents significant enough to warrant notification to the DOE/NNSA CSO	Incidents requiring notification to the contractor CSO
	Could include work stoppages, labor strikes affecting site security	Peaceful demonstrations of over 20 persons that require assistance from outside law enforcement agencies
	Arrest of an employee enrolled in the Human Reliability Program	
Procedural Interest (PI)	Generally associated with failure to adhere to security procedures and warrant notification to the DOE/NNSA CSO and where incidents do not result in loss, theft, compromise, or suspected compromise of the asset	
	Unauthorized discharge of a firearm	Improper handling, or storage of classified matter where evidence supports that compromise did not occur or the likelihood of compromise is remote
	Other incidents determined by the DOE/NNSA CSO and/or contractor CSO	Failing to properly secure a VTR (e.g., combination dial locked but the alarm is not secured) where evidence supports that unauthorized access and compromise did not occur or the likelihood of compromise is remote
		Unprotected classified document in a security area where evidence supports that compromise did not occur or the likelihood of compromise is remote (e.g., all personnel are cleared to the level of the document and have a need to know)
		Failure to follow two-person rule

Table A.3. IOSC Risk Ranking Score Sheet

INCIDENT ELEMENT		SCORE
Highest Classification Level	5: Top Secret	
	3: Secret	
	2: Confidential	
	0: No classified information directly involved	
Highest Classification Category	2: Restricted Data	
	1: Formerly Restricted Data	
	0: National Security Information, or no classification category directly involved	
Caveats	5: Sensitive Compartmented Information (SCI)	
	5: Special Access Program (SAP)	
	3: Nuclear Weapon Data (NWD)	
	2: Other	
	0: Not Applicable	
Location	5: Offsite	
	3: In Property Protection Area	
	1: In Limited Area	
	1: in Protected Area	
	1: In Material Access Area	
	0: Physical Location not directly involved	
Disclosure Status (Loss or Compromise of classified)	5: Did occur	
	3: Likely occurred	
	1: Unlikely to have occurred	
	0: Did not occur, or classified information not directly involved	
Intent	5: Willful	
	3: Gross negligence	
	1: Negligence	
	0: Inadvertent	
Management Involvement	5: Upper –level management involved/contributed	
	2: Front-line management involved/contributed	
	1: Management aware	
	0: Management unaware	
Mission Impact	5: Significant program or project interruption	
	3: Failure to meet DOE or client milestone	
	1: Failure to meet internal milestone	
	0: No significant mission impact	
External Reaction	5: National headlines; high level DOE involvement in investigation/enforcement action	
	2: Regional headlines; official inquiries from high level DOE	
	1: Local headlines; no significant inquiries from DOE	
	0: Little or no public interest; no DOE inquiries	
Resource Loss/Damage	5: Loss or damage to equipment/facilities >\$1M	
	3: Loss or damage to equipment/facilities \$100K to \$1M	
	1: Loss or damage to equipment/facilities \$10K to \$100K	
	0: Loss or damage to equipment/facilities <\$10K	

Table A.3. (contd)

INCIDENT ELEMENT		SCORE
Additional Contributing Factors (Choose all that apply)	1, 3, 5: Programmatic Issue (usually involves issues in administrative or management controls)	
	1, 3, 5: Repetitive Event (usually involve multiple instances of different types of issues that include substantially similar conditions, locations, organizations or programs)	
	1, 3, 5: Recurrence (usually involve multiple instances of the same type of issue)	
	2: Electronic transmission outside firewall	
	1: Electronic transmission inside firewall	
	3: Foreign national involved from sensitive country	
	1: Foreign national involved from non-sensitive country	
Total Score/Risk Ranking High: ≥ 16 Medium: 8-15 Low: < 8		

DOF-STD-1210-2012

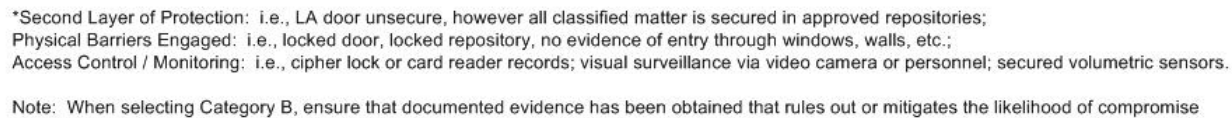
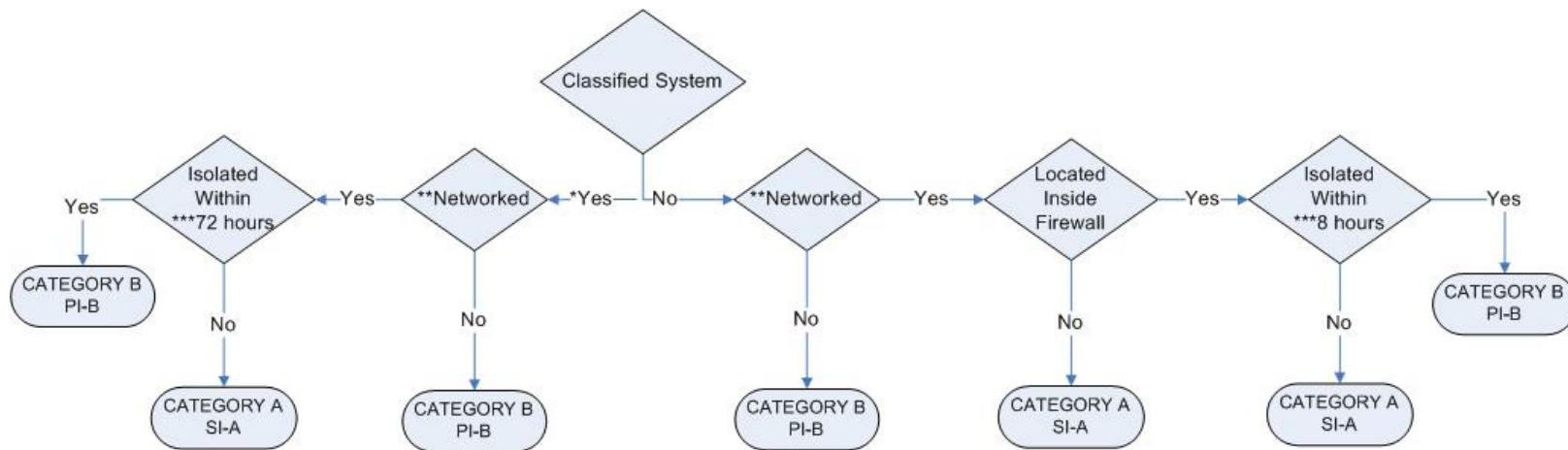


Figure B.1. Improper Storage: Classified Matter



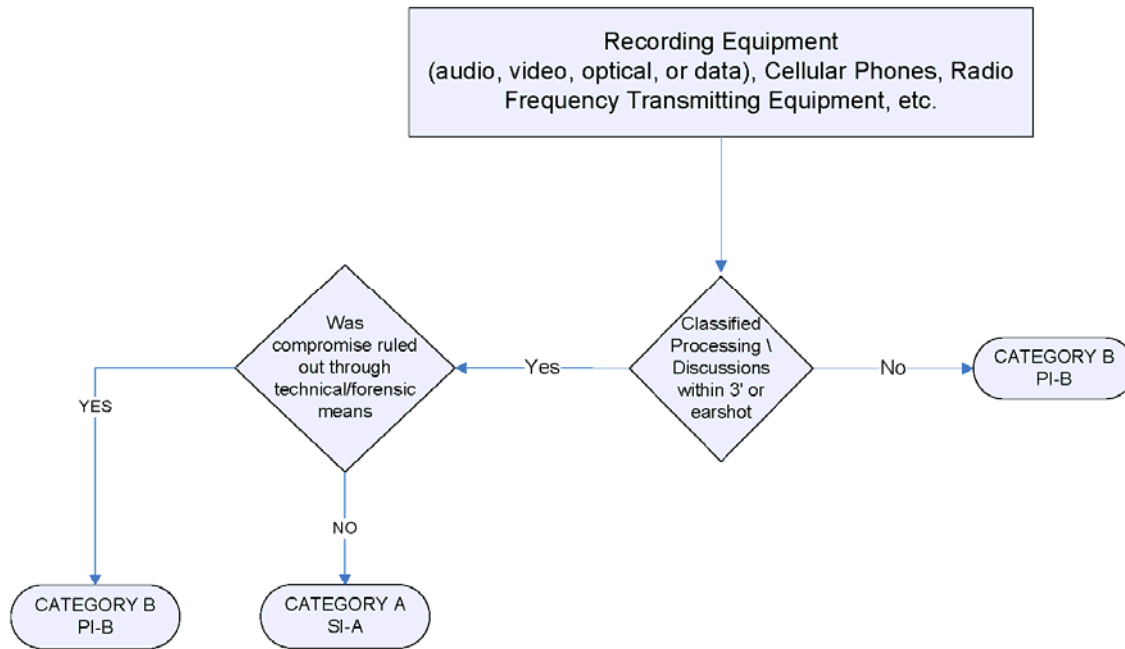
*Category and / or Level of Information Exceeds the Approved Level of System Accreditation

**Computer networks can be interpreted according to the hardware and software technology that is used to interconnect the individual devices in the network, such as optical fiber, Ethernet, wireless LAN, HomePNA, power line communication or G.hn.

*** Within the number of hours from occurrence: System Taken Off-Line; Appropriately Stored Pending Sanitization; Affected Systems Identified

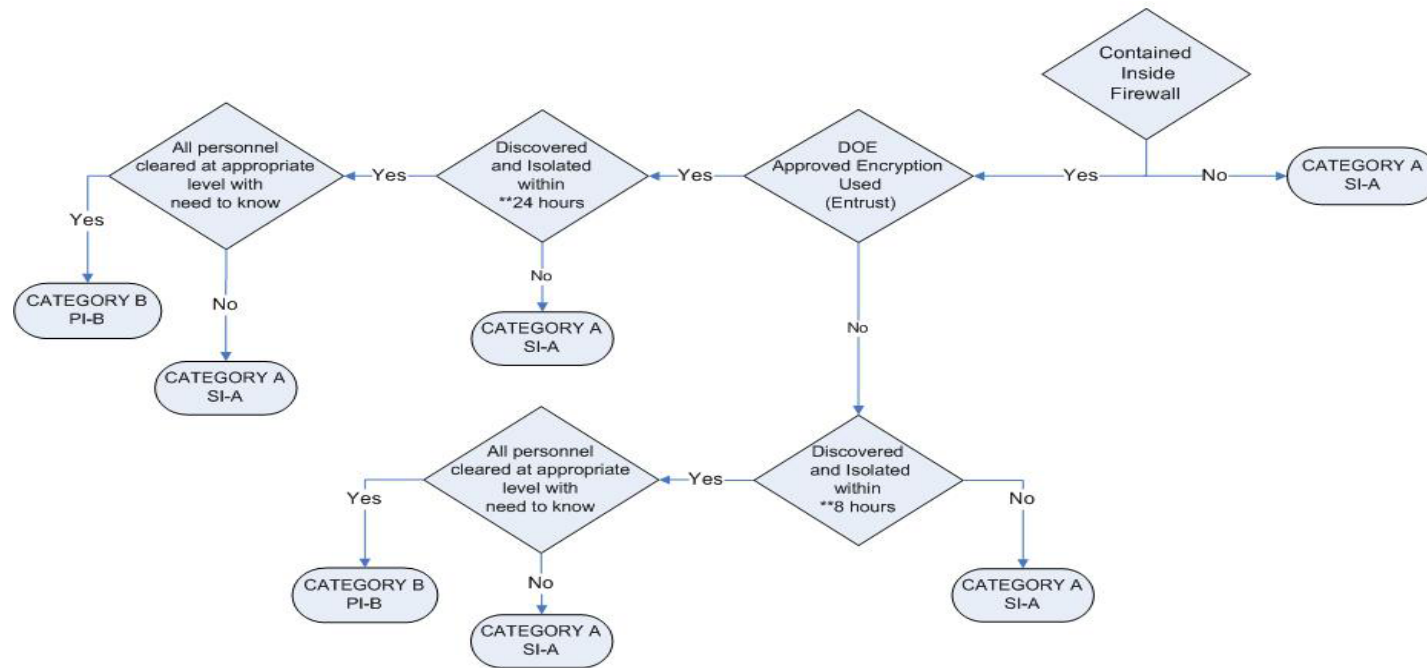
Note: When selecting category B, ensure that documented evidence has been obtained that rules out or mitigates the likelihood of compromise

Figure B.2. Processing Classified Information on an Unapproved Computer System



Note: When selecting category B, ensure that documented evidence has been obtained that rules out or mitigates the likelihood of compromise

Figure B.3. Unauthorized Introduction of Controlled Articles



** Within 8 hours from occurrence: System Taken Off-Line; Appropriately Stored Pending Sanitization; Affected Systems Identified

Note: When selecting category B, ensure that documented evidence has been obtained that rules out or mitigates the likelihood of compromise

Figure B.4. Unauthorized Network-Based Transmission of Information

APPENDIX C. DOE O 470.4B SSIMS NOTIFICATION AND INQUIRY OUTLINES

C.1 DOE O 470.4B SSIMS NOTIFICATION OUTLINE

1. Facility Code
 - a. Facility Name (Auto-populated based on facility code)
 - b. Facility Local Address or Unclassified Mailing Address (Auto-populated based on facility code)
 - c. Location (Building/Room Number)
2. Incident Discovery Date
3. Incident Number (System Generated)
4. Local Tracking Number (Local Incident Number)
5. Classification/marketing of the notification form.
6. Incident Categorization
 - a. Significance Level
 - i. Category A
 - ii. Category B
 - b. Interest Type
 - i. Security Interest (SI)
 - ii. Management Interest (MI)
 - iii. Procedural Interest (PI)
 - c. Topical Area
 - i. Program Planning and Management (PPM)
 - ii. Protective Force (PF)
 - iii. Physical Security (PS)
 - iv. Nuclear Material Control & Accountability (MCA)
 - v. Information Protection (IP)
 - d. Incident type (Available options will be limited based on the above)
 - i. Arrest
 - ii. On-site Arrest
 - iii. Investigation
 - iv. Hostile Act
 - v. Threats
 - vi. Suspicious Activity
 - vii. Demonstrations/Protests
 - viii. Labor Strikes
 - ix. Non-willful Intrusion
 - x. Degradation of Security
 - xi. Media Event
 - xii. Loss
 - xiii. Improper Storage
 - xiv. Unauthorized Discharge
 - xv. Unauthorized Introduction of Prohibited Articles

- xvi. Improper Access Controls
 - xvii. Process Difference
 - xviii. Inventory Difference
 - xix. Shipper/Receiver Difference
 - xx. Unauthorized Movement
 - xxi. Improper Handling
 - xxii. Cyber Incident Resulting in Compromise or Suspected Compromise of Information
 - xxiii. Unauthorized Network Based Transmission of Information
 - xxiv. Transmission of Information on an Unauthorized Communications System
 - xxv. Processing Information on an Unapproved Computer System
 - xxvi. Unauthorized Recipient of Information
 - xxvii. Unauthorized Introduction of Controlled Articles
 - xxviii. Improper Handling
7. Brief Description of the Incident
 8. Incident has or may result in media attention (Yes/No)
 - a. If yes describe the media attention
 9. Incident involves foreign nationals (Yes/No)
 10. If incident involves classified matter
 - a. Classification level of matter
 - b. Category of matter
 - c. Applicable identifiers (caveats)
 - d. Forms of matter involved
 11. Notification Point of Contact
 - a. Name
 - b. Phone
 - c. Secure Fax
 12. Notification Classification Official
 - a. Name
 - b. Phone
 - c. Classification Guide
 13. Closure Date (MI incidents only)

C.2 DOE O 470.4B SSIMS INQUIRY OUTLINE

1. Incident Number from notification
2. Classification/markings of the inquiry report (Level and Category)
3. Facility Where Incident Occurred/Originated (Auto-populated from notification)
 - a. Facility Code
 - b. Facility Local Address or Unclassified Mailing Address
 - c. Location (Building/Room)
 - d. Cognizant Security Office
 - e. Program Office
4. Facility Conducting the inquiry (if different from above)
 - a. Facility Code
 - b. Facility Name (Auto-populated based on facility code)
 - c. Cognizant Security Office
 - d. Program Office
5. Other Locations
 - a. Facility Code (if location is in SSIMS)
 - b. Name (Auto-populate if facility code is supplied)
 - c. Address (Auto-populate if facility code is supplied)
 - d. Location (Building/Room)
 - e. DOE Facility (Yes/No)
6. Security Areas involved
7. Dates
 - a. Discovery Date (Auto-populate from notification)
 - b. Inquiry Completion Date
 - c. Closure Date
8. Individuals
 - a. Facility Security Officer (at facility where incident occurred)
 - i. Name
 - ii. Title
 - iii. Organization
 - iv. Phone
 - b. DOE Cognizant Security Organization or HQ Representative
 - i. Name
 - ii. Title
 - iii. Organization
 - iv. Phone
 - c. Inquiry Officials
 - i. Name
 - ii. Title
 - iii. Organization
 - iv. Phone
 - d. Other Departmental Elements, Field/Operations Offices, Site Offices, Government Agencies, Foreign Government Agencies, or Contractors Involved in the Inquiry

- i. Name
 - ii. Title
 - iii. Organization
 - iv. Phone
 - e. Case Released to Other Agency or Agencies outside of DOE/NNSA
 - i. Agency Name
 - ii. Case/Tracking Number
 - iii. Date Released
 - iv. Closure Date from Other Agency (if available)
 - f. Responsible Individuals
 - i. Name
 - ii. Title
 - iii. Organization
 - iv. Phone
 - v. Employer Facility Code (if available)
 - vi. Employer Name (Auto-populate if facility code is supplied)
 - vii. Written Infraction issued (Yes/No)
 - viii. Interviewed (Yes/No)
 - ix. Written Statement available (Yes/No)
 - x. Foreign National (Yes/No)
 - xi. Properly Cleared (Yes/No)
 - g. Other Individuals
 - i. Name
 - ii. Title
 - iii. Organization
 - iv. Phone
 - v. Employer Facility Code (if available)
 - vi. Employer Name (Auto-populate if facility code is supplied)
 - vii. Interviewed (Yes/No)
 - viii. Written Statement available (Yes/No)
 - ix. Foreign National (Yes/No)
 - x. Properly Cleared (Yes/No)
- 9. Incident Categorization (Auto-populate from notification but may be changed)
 - a. Significance Level
 - i. Category A
 - ii. Category B
 - b. Incident Type
 - i. Security Interest (SI)
 - ii. Management Interest (MI)
 - iii. Procedural Interest (PI)
 - c. Topical Area
 - i. Program Planning and Management (PPM)
 - ii. Protective Force (PF)
 - iii. Physical Security (PS)

- iv. Nuclear Material Control & Accountability (MCA)
 - v. Information Protection (IP)
- d. Incident type (Available options will be limited based on the above)
 - i. Arrest
 - ii. On-site Arrest
 - iii. Investigation
 - iv. Hostile Act
 - v. Threats
 - vi. Suspicious Activity
 - vii. Demonstrations/Protests
 - viii. Labor Strikes
 - ix. Non-willful Intrusion
 - x. Degradation of Security
 - xi. Media Event
 - xii. Loss
 - xiii. Improper Storage
 - xiv. Unauthorized Discharge
 - xv. Unauthorized Introduction of Prohibited Articles
 - xvi. Improper Access Controls
 - xvii. Process Difference
 - xviii. Inventory Difference
 - xix. Shipper/Receiver Difference
 - xx. Unauthorized Movement
 - xxi. Improper Handling
 - xxii. Cyber Incident Resulting in Compromise or Suspected Compromise of Information
 - xxiii. Unauthorized Network Based Transmission of Information
 - xxiv. Transmission of Information on an Unauthorized Communications System
 - xxv. Processing Information on an Unapproved Computer System
 - xxvi. Unauthorized Recipient of Information
 - xxvii. Unauthorized Introduction of Controlled Articles
 - xxviii. Improper Handling
- 10. Description of Classified Matter Involved
 - a. Disclosure Type
 - b. Forms of Matter (Auto-populate from notification but may be changed)
 - c. Owner of the Information
 - d. Classification Level (Auto-populate from notification but may be changed)
 - e. Category (Auto-populate from notification but may be changed)
 - f. Caveats (Auto-populate from notification but may be changed)
 - g. Sigma Levels (Auto-populate from notification but may be changed)
 - h. Description of the matter (Auto-populate from notification but may be changed)
 - i. Classification Guide
 - j. Official Verifying the matter's classification
 - i. Name

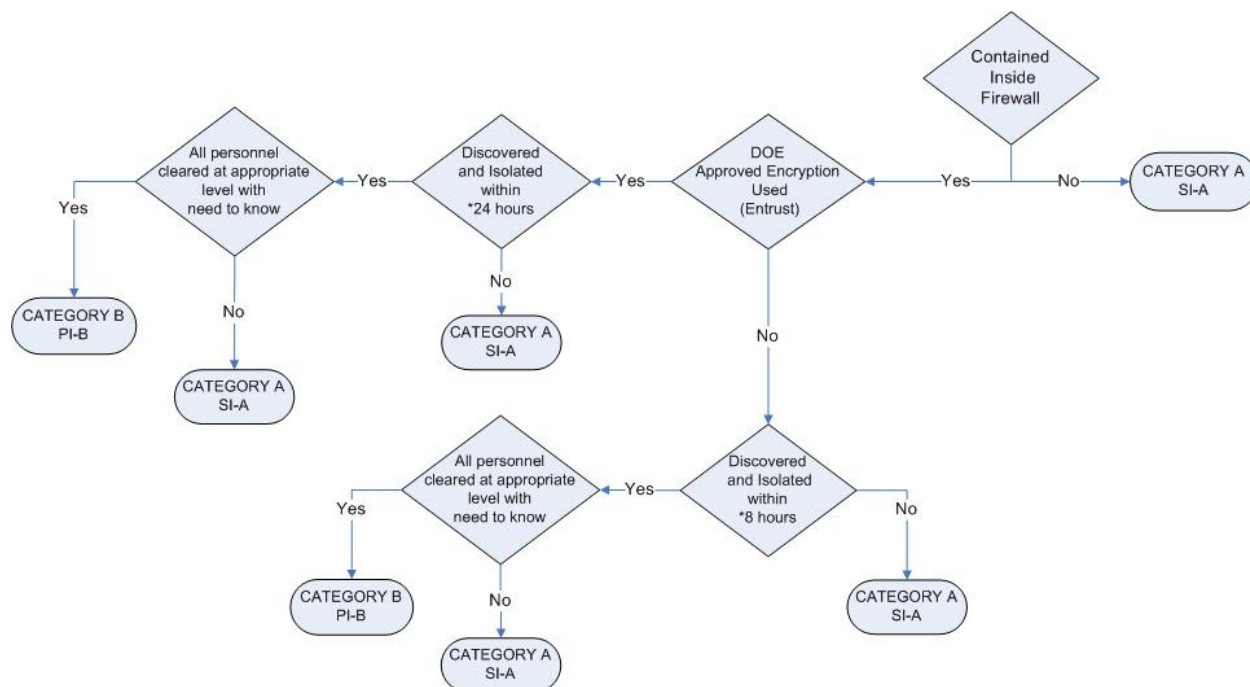
- ii. Title
 - iii. Organization
 - iv. Phone
- 11. Detailed Narrative
- 12. Determination of the Inquiry
 - a. Loss/Compromise
 - i. Compromise
 - ii. Suspected Compromise
 - iii. Likelihood of Compromise is Remote
 - iv. Compromise Did Not Occur
 - v. Significant Nuclear Defense Intelligence Loss
 - b. Rationale
 - c. Root cause
 - d. Characterization
 - e. Damage assessment
- 13. Corrective Actions
 - a. Actions taken to prevent recurrence
 - b. Management officials responsible for corrective actions
 - i. Name
 - ii. Title
 - iii. Organization
 - iv. Phone
- 14. Other Comments
- 15. Caveats (that apply to the inquiry report not the matter involved)
- 16. Sigma levels (that apply to the inquiry report not the matter involved)
- 17. Media Attention (Yes/No) (Auto-populate from notification – can be changed)
 - a. If Yes Describe the attention (Auto-populate from notification – can be changed)
 - b. Foreign National involvement (Yes/No) (Auto-populate from notification – can be changed)
- 18. Has this incident been rescinded (Yes/No)
- 19. Classification official for the inquiry
 - a. Name
 - b. Organization
 - c. Phone
 - d. Classification Guide
- 20. Local Tracking Numbers (Auto-populate from notification – can be changed)
- 21. Inquiry Costs
 - a. Total hours
 - b. Total costs
 - c. Comments

APPENDIX D. IOSC SCENARIOS

- On Monday at 3:00 p.m., a staff member receives an email from another staff member. The receiving staff member is an Authorized Derivative Classifier (ADC), and the sending staff member is requesting a classification review of an attached PowerPoint presentation. At 8:00 a.m. on Tuesday, the ADC staff member reviews the presentation and determines the attachment contains information at the S/RD level. At approximately 9:00 a.m., the ADC staff member reports the potential incident of security concern (IOSC) to management. At 10:00 a.m., management reports the potential IOSC to the Safeguards and Security IOSC team.

The IOSC team learns that the email was sent within the site's firewall, unencrypted, and included two additional staff members. There was no further dissemination of the presentation, to include hardcopies, or CDs, etc. All receiving staff members are appropriately cleared with a need to know. The presentation was created and sent on an unclassified computer. The IOSC team was able to contain the incident by 3:00 p.m. the day of notification (Tuesday). After reviewing the facts and circumstances, the IOSC team determines to report this incident as a category "SI-A."

The most appropriate decision tree for this incident is "Unauthorized Network-Based Transmission of Information." The first decision point on the decision tree is if the emailed presentation was contained within the firewall, this decision is "Yes." If an email is contained within a firewall, the next decision point is if "DOE Encryption Used," this decision is "No." The next decision point is if the email was "Discovered and Isolated within 8 hours." The email was sent 24 hours prior to official containment of the classified information, this decision is "No," concluding that the appropriate classification of this incident is a category "SI-A."



* Within 8 hours from occurrence: System Taken Off-Line; Appropriately Stored Pending Sanitization; Affected Systems Identified
 Note: When selecting category B, ensure that documented evidence has been obtained that rules out or mitigates the likelihood of compromise

Figure D.1. Unauthorized Network-Based Transmission of Information

Table D.1. IOSC Risk Ranking Score Sheet

INCIDENT ELEMENT		SCORE
Highest Classification Level	5: Top Secret	3
	3: Secret	
	2: Confidential	
	0: No classified information directly involved	
Highest Classification Category	2: Restricted Data	2
	1: Formerly Restricted Data	
	0: National Security Information, or no classification category directly involved	
Caveats	5: Sensitive Compartmental Information (SCI)	0
	5: Special Access Program (SAP)	
	3: Nuclear Weapon Data (NWD)	
	2: Other	
	0: Not Applicable	
Location	5: Offsite	0
	3: In Property Protection Area	
	1: In Limited Area	
	1: In Protected Area	
	1: In Material Access Area	
	0: Physical Location not directly involved	
Disclosure Status (Loss or Compromise of classified)	5: Did occur	1
	3: Likely occurred	
	1: Unlikely to have occurred	
	0: Did not occur, or classified information not directly involved	
Intent	5: Willful	0
	3: Gross negligence	
	1: Negligence	
	0: Inadvertent	
Management Involvement	5: Upper –level management involved/contributed	0
	2: Front-line management involved/contributed	
	1: Management aware	
	0: Management unaware	
Mission Impact	5: Significant program or project interruption	0
	3: Failure to meet DOE or client milestone	
	1: Failure to meet internal milestone	
	0: No significant mission impact	

Table D.1. (contd)

INCIDENT ELEMENT		SCORE
External Reaction	5: National headlines; high level DOE involvement in investigation/enforcement action	0
	2: Regional headlines; official inquiries from high level DOE	
	1: Local headlines; no significant inquiries from DOE	
	0: Little or no public interest; no DOE inquiries	
Resource Loss/Damage	5: Loss or damage to equipment/facilities >\$1M	0
	3: Loss or damage to equipment/facilities \$100K to \$1M	
	1: Loss or damage to equipment/facilities \$10K to \$100K	
	0: Loss or damage to equipment/facilities <\$10K	
Additional Contributing Factors (Choose all that apply)	1, 3, 5: Programmatic Issue (usually involves issues in administrative or management controls)	1
	1, 3, 5: Repetitive Event (usually involve multiple instances of different types of issues that include substantially similar conditions, locations, organizations or programs)	
	1, 3, 5: Recurrence (usually involve multiple instances of the same type of issue)	
	2: Electronic transmission outside firewall	
	1: Electronic transmission inside firewall	
	3: Foreign national involved from sensitive country	
	1: Foreign national involved from non-sensitive country	
Total Score/Risk Ranking High: >=16 Medium: 8-15 Low: <8		7

D.1 EXPLANATION

The information involved was Secret, with a category of Restricted Data. This gives us scores of ‘3’ and ‘2’ for the first two elements. There are no caveats associated with the information, so the caveats score is ‘0’. These first three elements are very straightforward as far as scoring.

Location does not apply in this case. Generally, the location element is used when the event involves easily recognized information or matter that is left unsecured, as the effect on risk ranking gets reduced if the information is in a more secure location during the event. In this case, a score of ‘0’ is appropriate.

Based on information provided, a disclosure status of ‘unlikely’ is appropriate. All involved personnel have clearances. The email was sent over the unclassified network, so we can’t rule out compromise, but there are no indications that any uncleared persons did in fact access it while it was on the servers, and the timeframe is fairly short. A score of ‘1’ is appropriate. In a real event, you need to make sure you collect enough information to be able to justify whatever score you choose. For example, a document left on an unclassified server for a long period of time (weeks or months) will be harder to justify an ‘unlikely’ score than one which is taken down within a certain number of hours or days.

There is no indication that there was negligence or willful noncompliance, so Intent is scored '0'.

Management involvement is likely a '0' for this scenario. This element is usually hard to score above zero early in an event. It is usually during the cause analysis that enough information is gathered to make a determination that management involvement was material to the event. Again, make sure you have sufficient evidence to defend your score.

Mission Impact and External Reaction are somewhat subjective, but there are indicators that can be used to assist in scoring. The affected project/organization can tell you if the event is creating an impact, and if so, what the level is. Your communications department can tell you if there is media attention. For this event, the likely scores are '0' for both Mission Impact and External Reaction.

No equipment/facility damage has occurred in this event, so '0' is the correct score.

Under Additional Contributing Factors, there is significant leeway provided to the screener to add risk factors based on repetitiveness, programmatic issues or any other factor that they deem appropriate. This is intentional because there is always the chance that an event does not neatly fit into the checklist as written, but it is clear to the screener that it needs a higher score so it gets appropriate treatment from management for causal analysis. In this case, no information is provided to indicate any additional factors except for the fact that it involved internal email.

The total score for this event is 7, which puts it in the Low category. It is important to note that the category result is not absolute; this score of 7 is high enough that the screener may consider calling it a medium even though it is technically below 8. In this case, because the information was on an unclassified system overnight, we might have scored it '3' (likely compromise) which would have made it a Medium for categorization. The screener could also have left it a '1' (unlikely compromise) but still categorized it as medium, citing the risks associated with the information being on an unclassified network overnight, or other intangible factors that they felt warranted more formality in the causal analysis.

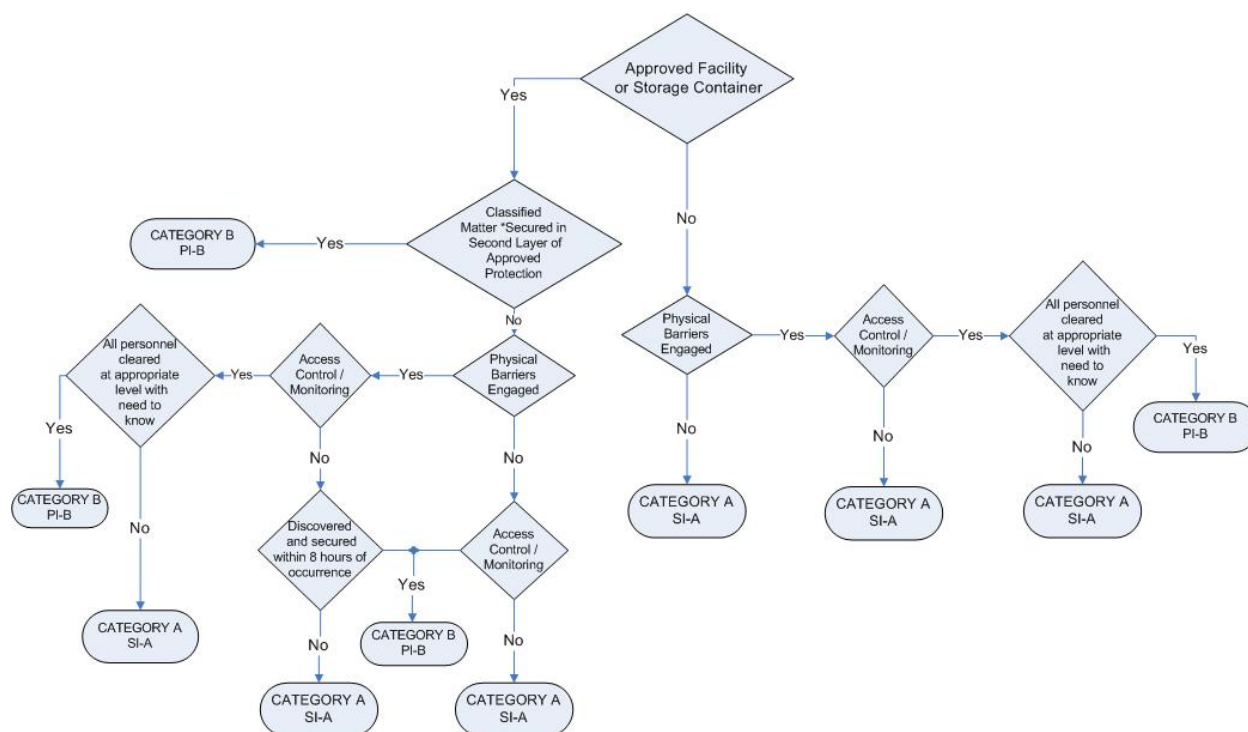
Similarly, a result could be downgraded if the screener had a borderline score that they felt did not merit the higher category. In either case, the screener needs to make sure they have sufficient documentation to justify adjusting the category.

2. On Friday at 4:00 p.m. a staff member conducting "end of day checks" discovers an unsecured GSA approved safe containing classified information up to the C/RD level. The staff member secures the safe and reports the potential IOSC immediately to management. At approximately 4:30 p.m. management reports the potential IOSC to the Safeguards and Security IOSC team.

The IOSC team learns that the safe is located within a limited area that resides within a property protection area. The office that contains the safe is controlled by an auditable cipher lock, which was engaged at the time of the incident. The audit from the lock indicates that the space owner entered the office at 1:00 p.m. that day, and no one else entered the office until 4:00 p.m. that same day when conducting "end of day checks." The staff member conducting "end of day checks" has a need to know and all the classified is accounted for. The IOSC team also notes that there are no signs of forced entry through the door, walls, windows, etc. After reviewing the facts and circumstances, the IOSC team determined to report this incident as a category "PI-B."

The most appropriate decision tree for this incident is "Improper Storage: Classified Matter." The first decision point on the decision tree is if the classified matter is contained within an approved facility or storage container. Since the office resides within a limited area, this decision is "Yes."

The next decision point is if the classified matter is secured in a second layer of approved protection, such as a GSA approved safe. In this situation the classified matter was in an unsecured safe, this decision point is “No.” Since the documents are not in a second layer of approved protection the next decision point is if the area in question had physical barriers engaged. The safe was located within a room behind a locked door, so this decision point is “Yes.” Because the safe was behind a locked door the next decision point is if the engaged barriers had access-control monitoring. In this case the limited door was controlled with an auditable lock, so this decision point is “Yes.” The next decision point is if all personnel who entered the area during the time the classified matter was unsecured are appropriately cleared and have the need to know. The audit from the lock indicated that the staff member who discovered the open safe was the only person to enter the room during the time in question. This particular staff member is appropriately cleared with a need to know, so this decision point is “Yes,” concluding that the appropriate classification of this incident is a category “PI-B.”



*Second Layer of Protection: i.e., LA door unsecure, however all classified matter is secured in approved repositories;

Physical Barriers Engaged: i.e., locked door, locked repository, no evidence of entry through windows, walls, etc.;

Access Control / Monitoring: i.e., cipher lock or card reader records; visual surveillance via video camera or personnel; volumetric sensors.

Note: When selecting Category B, ensure that documented evidence has been obtained that rules out or mitigates the likelihood of compromise

Figure D.2. Improper Storage: Classified Matter

Table D.2. IOSC Risk Ranking Score Sheet

INCIDENT ELEMENT		SCORE
Highest Classification Level	5: Top Secret	2
	3: Secret	
	2: Confidential	
	0: No classified information directly involved	
Highest Classification Category	2: Restricted Data	2
	1: Formerly Restricted Data	
	0: National Security Information, or no classification category directly involved	
Caveats	5: Sensitive Compartmented Information (SCI)	0
	5: Special Access Program (SAP)	
	3: Nuclear Weapon Data (NWD)	
	2: Other	
	0: Not Applicable	
Location	5: Offsite	1
	3: In Property Protection Area	
	1: In Limited Area	
	1: In Protected Area	
	1: In Material Access Area	
	0: Physical Location not directly involved	
Disclosure Status (Loss or Compromise of classified)	5: Did occur	0
	3: Likely occurred	
	1: Unlikely to have occurred	
	0: Did not occur, or classified information not directly involved	
Intent	5: Willful	0
	3: Gross negligence	
	1: Negligence	
	0: Inadvertent	
Management Involvement	5: Upper –level management involved/contributed	0
	2: Front-line management involved/contributed	
	1: Management aware	
	0: Management unaware	
Mission Impact	5: Significant program or project interruption	0
	3: Failure to meet DOE or client milestone	
	1: Failure to meet internal milestone	
	0: No significant mission impact	

Table D.2. (contd)

INCIDENT ELEMENT		SCORE
External Reaction	5: National headlines; high level DOE involvement in investigation/enforcement action	0
	2: Regional headlines; official inquiries from high level DOE	
	1: Local headlines; no significant inquiries from DOE	
	0: Little or no public interest; no DOE inquiries	
Resource Loss/Damage	5: Loss or damage to equipment/facilities >\$1M	0
	3: Loss or damage to equipment/facilities \$100K to \$1M	
	1: Loss or damage to equipment/facilities \$10K to \$100K	
	0: Loss or damage to equipment/facilities <\$10K	
Additional Contributing Factors (Choose all that apply)	1, 3, 5: Programmatic Issue (usually involves issues in administrative or management controls)	0
	1, 3, 5: Repetitive Event (usually involve multiple instances of different types of issues that include substantially similar conditions, locations, organizations or programs)	
	1, 3, 5: Recurrence (usually involve multiple instances of the same type of issue)	
	2: Electronic transmission outside firewall	
	1: Electronic transmission inside firewall	
	3: Foreign national involved from sensitive country	
	1: Foreign national involved from non-sensitive country	
Total Score/Risk Ranking High: >=16 Medium: 8-15 Low: <8		5

D.2 EXPLANATION

The information involved was Confidential, with a category of Restricted Data with no other caveats. This gives us scores of ‘2’, ‘2’ and ‘0’ for the first three elements.

In this event, location is important, because the information/material is obviously marked as classified, and its presence in a location makes it susceptible to anyone who has access to that location. In this event, the location is a limited area. So a score of ‘1’ is appropriate.

Based on information provided, a disclosure status of ‘0’ (did not occur) is appropriate for disclosure. There is sufficient evidence provided that no one without need to know and clearance ever had access to the safe and information in it. A screener could argue that we can’t rule out compromise, because a surreptitious entry might have occurred—a score of ‘1’ (unlikely) is not wrong, but probably not warranted in this case.

There is no indication that there was negligence or willful noncompliance, so Intent is scored ‘0’.

Management involvement is likely a '0' for this scenario.

For this event, the likely scores are '0' for both Mission Impact and External Reaction.

No equipment/facility damage has occurred in this event, so '0' is the correct score.

Under Additional Contributing Factors, there is no information provided to indicate any additional risk factors need to be added. This might be different if the group or person involved is a repeat offender, or if previous incidents indicated that this was another related programmatic issue. In this case, a score of '0' is appropriate.

The total score for this event is 5. In this case, the score clearly results in a Low categorization. It is not likely that the screener would want to push this up to the Medium level. Again, it is up to the screener to make the final determination of categorization, using the risk ranking sheet as a tool to help make that decision.

8. CONCLUDING MATERIAL

Review Activity:

EM

HSS

NE

NNSA

SC

Preparing Activity:

Office of Security Policy (HS-51)

Project Number:

SANS-0011

Field and Operations Offices

ID

NNSA Service Center

ORO

RL

Site Offices:

LASO

LLSO

OR

RLSO

SRSO

YSO

External Agency

None