

APPENDIX C - INCIDENTS OF SECURITY CONCERN

1. **OBJECTIVE.** To ensure the occurrence of a security incident prompts the appropriate graded response, to include an assessment of the potential impacts, extent of condition, and corrective actions. The long-term management of incidents serves as an effective Program Planning and Management tool for enhancing site-specific implementation of security policies.
2. **PURPOSE.** To set forth requirements for the Department of Energy (DOE) Incidents of Security Concern process, including timely identification, notification, inquiry, reporting, and closure of incidents of security concern. The Incident Program serves multiple purposes to include:
 - a. Ensure incidents are communicated to DOE/National Nuclear Security Administration (NNSA) line management, and, as necessary, other agencies and foreign governments
 - b. Meet regulatory reporting requirements
 - c. Ability to track and trend the health of the security program at the site and overall Department
 - d. Ensure incidents are assessed relative to impact to National Security and collateral impact with other programs and security interests
 - e. Mechanism to support performance assurance, self-assessment, oversight, and other key security functions
 - f. Ability to influence policy development and site security implementation, and
 - g. Ability to ensure the identification of safeguards and security (S&S) programmatic successes are communicated internally/externally
3. **DEFINITION.** Security incidents encompass a broad range of events and assets. These incidents include actions ranging from accidental to intentional (i.e., willful), failure to adhere to established security requirements (i.e., properly marking a document) to an actual compromise of information, loss of an asset to theft, involvement of a foreign national to a cleared Departmental employee, security deficiencies to security successes (e.g., detection of suspicious activity), etc. While incidents include an array of events, the resulting response to the incident is graded relative to notification, inquiry, and closure requirements.

The subject policy defines two general categories of incidents.

- a. Category A incidents are generally defined as incidents involving high level of National Security assets and unacceptable consequences. Category A incidents require the involvement of the Cognizant Secretarial Officer or their designee(s)

and the contractor security authority. The involvement of the Cognizant Secretarial Officer or their designee(s) is imperative for assessing impacts, coordinating with external agencies, and/or keeping senior leadership apprised of significant events.

- b. Category B incidents are reflective of procedural-based incidents or involve lower level National Security assets such as Controlled Unclassified Information versus Classified Information. The management and resolution of Category B incidents is the primary function of the Contractor Security Authority; however, this does not preclude the Cognizant Secretarial Officer or their designee(s) from exercising their oversight responsibilities. The monitoring of Category B incidents by the Contractor Security Authority is essential as it allows management to proactively address reoccurring incidents, thereby minimizing the occurrence of potentially more significant events.

4. REFERENCES.

- a. 18 United States Code (U.S.C.) 923 (g)(6), each licensee shall report the theft or loss of a firearm from the licensee's inventory or collection, within 48 hours after the theft or loss is discovered, to the Attorney General and to the appropriate local authorities.
- b. 42 U.S.C. 2271 to 2181 (Sections 221 to 233 as amended, AEA), gives the FBI the authority to investigate alleged or suspected criminal violations of the Act, makes violations of the Act criminal, and provides for injunction and contempt proceedings.
- c. 42 U.S.C. 2282b (Section 234B, as amended, AEA), establishes civil penalties for violations of directives regarding protection of classified information by contractors or their employees.
- d. 50 U.S.C. 402a, *Coordination of Counterintelligence Activities*, states that the Federal Bureau of Investigation is advised immediately of any information, regardless of its origin, which indicates that classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power.
- e. 50 U.S.C. 2656 requires the Secretary of Energy to notify the Committees on Armed Services of the Senate and House of Representatives of each "significant nuclear defense intelligence loss."
- f. Energy Reorganization Act of 1974: Sec. 307, requires investigating suspected, attempted, or actual thefts of special nuclear materials in the licensed sector and developing contingency plans for dealing with such incidents.

- g. Executive Order 13526, *Classified National Security Information*, if the Director of the Information Security Oversight Office finds that a violation of this order or its implementing directives has occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.
- h. National Security Decision Directive 84, requires that unauthorized disclosures of classified information be evaluated to determine information disclosed and extent of dissemination, and discusses coordination with Department of Justice (DOJ).
- i. 10 Code of Federal Regulations (CFR) Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*, establishes rules to assess a penalty for violation of a directive relating to the protection of classified information pursuant to 42 U.S.C. 2282b (Section 234B, as amended, of the *Atomic Energy Act of 1954*) or for violation of a compliance order that directs action for the protection of classified information.
- j. 10 CFR 1016, *Restricted Data*, requires the permittee to report any infractions, losses, compromises, or possible compromise of Restricted Data.
- k. 10 CFR 1045, *Nuclear Classification and Declassification*, addresses “Nuclear Classification and Declassification”, to include sanctions for knowing, willful, or negligent actions contrary to the requirements of the CFR that results in the misclassification of information.
- l. 32 CFR Part 2001.47, *Reporting Loss of Classified Information*, mandates reporting, inquiry, etc. for the loss, possible compromise, or unauthorized disclosure of classified information. If the incident entails a criminal violation, coordination is required with legal counsel and DOJ.
- m. 48 CFR Chapter 9, *Department of Energy Acquisitions Regulation (DEAR)*, supplements 48 CFR Chapter I, *Federal Acquisition Regulations*, and includes the security clauses to be used in DOE solicitations and contractors or agreements involving access to classified information and/or a significant quantity of SNM.
- n. NISPOM 1-303, *Reports of Loss, Compromise, or Suspected Compromise*, requires any loss, compromise or suspected compromise of classified information, foreign or domestic, to be reported to the CSA. Classified material that cannot be located within a reasonable period of time shall be presumed to be lost until an investigation determines otherwise.
- o. DOE O 151.1C, *Comprehensive Emergency Management System*, establishes policy and assigns roles and responsibilities for the Department of Energy (DOE) Emergency Management System.
- p. DOE O 206.1, *Department of Energy Privacy Program*, establishes Departmental implementation of agency statutory and regulatory requirements for privacy,

specifically those provided in the Privacy Act of 1974, as amended at Title 5 United States Code (U.S.C.) 552a, Section 208 of the E Government Act of 2002, and Office of Management and Budget directives.

- q. DOE O 221.1A, establishes requirements and responsibilities for reporting fraud, waste, abuse, misuse, corruption, criminal acts, or mismanagement to the DOE, Inspector General.
- r. DOE O 231.1A, Chg 1, *Environment, Safety, and Health Reporting*, requires a timely collection, reporting, analysis, and dissemination of information on environment, safety, and health issues as required by law or regulations or as needed to ensure that the Department of Energy (DOE) and National Nuclear Security Administration are kept fully informed on a timely basis about events that could adversely affect the health and safety of the public or the workers, the environment, the intended purpose of DOE facilities, or the credibility of the Department.
- s. DOE M 231.1-1A, Chg 2, *Environment, Safety, and Health Reporting Manual*, establishes requirements categorizing occurrences related to ES&H or operations (“Reportable Occurrences”); notifying DOE of these occurrences; and developing and submitting documented follow-up reports. These occurrence reporting directives further require that the notifications be timely in accordance with the significance of the occurrence.
- t. Former Deputy Secretary Clay Sell memorandum dated June 22, 2007. Requires notifying Congress of various losses, and in particular, classified material that may compromise national security. The determination of compromise must be made by the Program Office.
- u. 50 U.S.C. 2656 requires the Secretary of Energy to notify the Committees on Armed Services of the Senate and House of Representatives of each “significant nuclear defense intelligence loss.”

5. ROLES AND RESPONSIBILITIES.

- a. Cognizant Secretarial Officer. The Secretarial Officer must define the designee(s) (i.e., Program Office and/or Site Office) responsible for executing the subsequent roles and responsibilities. Note: Reference to the cognizant Secretarial Officer in the remainder of the policy implies either the Secretarial Officer or their Federal designee(s).
 - (1) As the element with programmatic responsibility for the information, coordinate formal reviews of incidents involving the loss, theft, compromise, or suspected compromise of Top Secret, Sensitive Compartmented Information (SCI), Special Access Program (SAP), and Restricted Data (RD) Weapons Data to render a “significant nuclear defense intelligence loss” and damage assessment determinations. The

Defense Authorization Act defines “significant nuclear defense intelligence loss” as “any national security or counterintelligence failure or compromise of classified information at a facility of the Department or operated by a contractor of the Department that the Secretary considers likely to cause significant harm or damage to the national security interest of the United States.” This requirement is stipulated in 50 United States Code (USC) 2656.

If it’s determined that the incident meets the “significant nuclear defense intelligence loss” criteria, the appropriate Federal entity(s), after consultation with the Director, Central Intelligence, and the Director, Federal Bureau of Investigation (FBI), must provide notification to Congress. The notification of Congress must occur within 30 days of categorizing the event as a 50 USC 2656 reportable incident.

The element with programmatic responsibility for the information must also determine if the incident warrants a damage assessment. Damage assessments determine potential damage to national security, and are performed to evaluate and document possible countermeasures and conduct actions to limit potential damage.

- (2) Serve as the liaison to Congress, the Secretary, and other Government agencies, the FBI, the Inspector General for incidents under their purview.
- (3) Track and trend incidents for the purpose of assessing program strengths and weaknesses across programmatic sites.
- (4) Where noted in the policy, specify to the contractor security authority the Federal “designee(s)” responsible for executing an applicable Federal requirement (e.g., entity(s) responsible for approving the contractor security authority (CSA) developed Incidents of Security Concern (IOSC) Program Plan.
- (5) Provide guidance/direction to the contractor security authority relative to specific expectations for executing various elements of the program, to include, but not limited to, the mechanism for providing notification, particular incidents requiring Federal line management notification, etc.
- (6) Perform oversight of the contractor security authority’s implementation of the IOSC Program, to include, but not limited to reviewing inquiries, determinations of compromise, tracking and trending, integration of the data into the larger Program Planning and Management (PPM) function, etc.
- (7) Ensure the contractor security authority complete the actions necessary to resolve incidents of security concern, including actions necessary to prevent recurrence.

- (8) Ensure that the IOSC Program Plan thoroughly addresses all elements of the program and sufficient resources are provided to conduct inquiries and damage assessments and to implement corrective actions.
- (9) Utilize the incident program as a feedback mechanism to assist management in evaluating programmatic performance across all security disciplines.
- (10) Coordinate with the Deputy Director, Counterintelligence Directorate concerning incidents that indicate a deliberate compromise of classified information or involve foreign persons, governments, or activities.

b. Contractor Security Authority.

- (1) Develop an IOSC Program Plan that addresses each component (i.e., initial notification, inquiry, etc.) of the subject policy.
- (2) Identify the occurrence of both Category A and B incidents.
- (3) Assess and categorize all incidents, as these steps determine the appropriate level of notification and influence the consideration for external notification, corrective actions, damage assessments, etc. For example, the subsequent response/requirements vary significantly between an incident where the information was deemed to be compromised or suspected of compromise versus compromise did not occur or the likelihood is remote.
- (4) Integrate the IOSC Program with the larger PPM function for the purpose of influencing other functions and enhancing site-specific implementation of security policies.
- (5) Perform tracking and trending analyses on the collective set of incidents for the purpose of monitoring security program performance and modifying site security policies accordingly.
- (6) Assess the impacts of incidents relative to other site programs and security interests and coordinate, as necessary, with the programmatic element responsible for the information that is stolen, lost, compromised, or suspected of compromise. The latter is required to render a “significant nuclear defense intelligence loss” and damage assessment determinations.
- (7) Assess if corrective actions are warranted for a given incident.

c. Office of Health, Safety and Security (HSS).

- (1) Establish the Incidents of Security Concern Program based on National policies and best business practices.

- (2) Oversee, maintain, and provide training to the Safeguards and Security Information Management System (SSIMS).
- (3) Assess incident data for the purpose of reviewing and enhancing security policies.
- (4) Provide technical incident and causal analysis expertise to site and program offices as requested.

CHAPTER I. IDENTIFICATION AND REPORTING REQUIREMENTS

1. GENERAL

- a. Each incident requires categorization, an initial report, an inquiry, and a closure report. The level of effort associated with the latter three steps is graded based on the incident category and factors (severity, asset, etc.) surrounding the incident.
- b. Policy implementation requires diligence on the part of the contractor security authority to ensure incidents are appropriately categorized, as the subsequent steps/requirements determine the level of notification and influence the consideration for external notification, corrective actions, damage assessments, etc. For example, the requirements vary significantly between an incident where the information was deemed to be compromised or suspected of compromise versus compromise did not occur or the likelihood is remote.
- c. Effective execution of policy requires the development of an IOSC Program Plan by the contractor security authority. The plan must address the various sections of the policy, to include, incident identification and notification; initial reporting; inquiry process; and closure of incidents.
- d. The contractor security authority must appropriately respond and manage both individual incidents and, over a span of time, the collective set of incidents. The former ensures the potential impacts of incidents are addressed, and the latter serves as a Program Planning and Management tool for monitoring the effectiveness of particular security topical areas or the larger site security program and avoiding the reoccurrence of incidents by implementing corrective actions.
- e. The contractor security authority developed IOSC Program Plan requires implementation guidance from the cognizant Secretarial Officer with respect to their expectations associated with the various elements of the policy. These elements include, but are not limited to, particular incidents requiring Federal notification, specific Federal offices and entities requiring notification, and the mechanism for notifying entities within line management.
- f. Initial and final reporting is imperative as the cognizant Secretarial Officer has specific responsibilities for notifying and/or coordinating with other agencies, governments, Departmental leadership, and Congress for select incidents.
- g. The element with programmatic responsibility for the information involved with the loss, theft, compromise, or suspected compromise of Top Secret, SCI, SAP, and RD Weapons Data must assess the incident to render a “significant nuclear defense intelligence loss” and damage assessment determination.
- h. Incidents include a range of possible actions, inactions, or events that have occurred at a site that:

- (1) pose threats to National Security interests and/or critical DOE assets,
- (2) create potentially serious or dangerous security situations,
- (3) potentially endanger the health and safety of the workforce or public (excluding safety-related items),
- (4) degrade the effectiveness of the Safeguards & Security (S&S) program,
- (5) adversely impact the ability to protect DOE S&S interests,
- (6) warrant notification to the cognizant Secretarial Officer due to media interest or due to the general significance of the event,
- (7) reflect the failure to adhere to security procedures, or
- (8) illustrate the system functioning as designed by identifying and/or mitigating potential threats (e.g., detecting suspicious activity, hostile act, etc.).

2. INCIDENT IDENTIFICATION AND CATEGORIZATION. DOE uses a graded approach for the identification and categorization of incidents of security concern. This approach provides a framework for the requirements of reporting time-lines and the level of detail for inquiries into, and root cause analysis of, specific security incidents. By establishing a graded approach, line management can effectively allocate the resources necessary to implement this section based on the severity of security incidents. The incident program is comprised of two general categories of incidents described below:

- a. Category A incidents are generally defined as incidents involving high level National Security assets and unacceptable consequences. Category A incidents require the involvement of the cognizant Secretarial Officer and the contractor security authority. The involvement of the cognizant Secretarial Officer for Category A incidents is imperative for assessing impacts, coordinating with external agencies, and/or keeping senior leadership apprised of significant events.
- b. Category B incidents are generally defined as reflective of procedural-based incidents or involve lower level National Security assets (Controlled Unclassified Information versus Classified Information). The management and resolution of Category B incidents is the primary function of the contractor security authority; however, this does not preclude the cognizant Secretarial Officer from exercising their oversight responsibilities. The monitoring of Category B incidents by the contractor security authority is essential as it allows management to proactively address reoccurring incidents, thereby minimizing the occurrence of potentially more significant events. The following subsections provide the framework for identifying and categorizing incidents of security concern.

- c. The three general types of Category A incidents include:
- (1) The loss, theft, compromise, or suspected compromise of assets involving significant National Security interests.
 - (2) Events of Management Interest
 - (3) Incidents with special organizational interest
- d. The criteria for Category A incidents includes the following:
- (1) “Loss, theft, compromise, or suspected compromise” involving assets of significant National Security interests.
 - (a) These incidents are associated with more severe consequences (e.g., unauthorized disclosure) versus incidents based on the failure to adhere to security procedure where the supporting facts suggest compromise did not occur or the likelihood is remote.
 - (b) The compromise or suspected compromise can occur through unauthorized disclosure (i.e., identifiable recipient) and/or several types of medium such as, but not limited to computer, verbal, facsimile, phone, etc. The latter is described in NISPOM as “Improper Transmission”. Also, the latter type of incidents may not be associated with a specific unauthorized recipient, but rather result in a compromise or suspected compromise determination due to the inherent vulnerabilities of the transmission [reference the technical standard for the type of “improper transmission” incidents that constitute a compromise or suspected compromise (i.e., Category A incident)].
- e. This criterion must be assessed/applied to incidents involving the following assets:
- Special Nuclear Material and nuclear material (Note: “Loss” does not include quantities that are within established shipping, processing, and inventory limits).
 - Classified Matter (Note: Subsequent sections will differentiate the reporting requirements for Top Secret, SCI, SAP, and RD Weapons Data information versus lower categories and levels of classified information).
 - Radiological, Biological and Chemical materials as defined in DOE M 470.4-2A.

- Security keys based on the significance of the asset being protected and the degree (i.e., direct versus access impeded by other layers/measures) of access provided by the key.
- Protective Force firearms, ammunition, explosives, and other equipment per the reporting requirements in DOE M 470.4-3A and DOE M 470.4-8.
- Credentials that are the target of the theft for the purpose of gaining unauthorized access to a DOE/NNSA facility or site.
- Matter of a foreign government that requires reporting based on established agreements and required protocol.

f. Events of Management Interest

- (1) These events may include, but are not limited to incidents with media interest or other significant incidents such as, on-site arrest; hostile act; threat; non-willful or unauthorized intrusion; introduction of prohibited articles; unacceptable degradation of a facility's security posture; a facility inadvertently receiving an asset that exceeds security authorization thresholds; a gain in the number of SNM items; and unauthorized discharge resulting in injury or fatality.
- (2) The IOSC Program Plan must define those potential incidents that are considered Events of Management Interest.
- (3) In addition to the defined Category A incidents specified in the subject policy, Federal line management must specify other incidents that they deem warrant an elevated reporting.

g. Incidents with special organizational interest.

- (1) Security incidents involving any credible information that a non-U.S. citizen or an agent of a foreign power is involved, the geographically closest element of the Office of Counterintelligence (OCI)/Office of Defense Nuclear Counterintelligence (ODNCI) must be notified, which in turn will notify the FBI in accordance with 50 U.S.C. 402a.
- (2) If a violation of law has occurred and the preservation of evidence requires immediate notification of Federal (including FBI), State, or local law enforcement agencies (e.g., theft of SNM, homicide, assault, location or detonation of an explosive device), the Federal designee(s) within line management must perform all necessary referrals and notifications.

- (3) When an inquiry surrounding an incident of security concern establishes information indicating that fraud, waste, or abuse has occurred, the Office of the Inspector General must be notified for information and/or action
 - (4) When the inquiry into an incident of security concern necessitates communication with Agencies/organizations external to the Department (e.g., the U.S. Postal Service, the FBI, or other Federal agencies), a Federal designee(s) must be responsible for performing all such communication.
 - (5) Whenever a compromise involves the classified matter of another Government agency, the Federal designee(s) within line management must coordinate with the Other Government Agencies (OGA), as appropriate.
 - (6) Whenever a compromise involves the matter of a foreign government that requires protection [e.g., Confidential Foreign Government Information Modified Handling (C/FGI-Mod)], the Federal designee(s) within line management must coordinate with the Department of State and the foreign government, as appropriate. The foreign government, however, will not normally be advised of any Departmental security system vulnerabilities that allowed or contributed to the compromise.
 - (7) If a compromise of SCI has occurred, the Director, Office of Intelligence and Counterintelligence, must consult with the designated representative of the Director, Central Intelligence, and other officials responsible for the information involved.
- h. The two general types of Category B incidents include:
- (1) The loss, theft, compromise, or suspected compromise of an asset other than those identified in section 2.e.
 - (2) Procedural-based Incidents
- f. The criteria for Category B incidents include the following:
- (1) The loss, theft, compromise, or suspected compromise of an asset other than those identified in section 2.e.
 - a. While the criterion (loss, theft, compromise, or suspected compromise) is the same as Category A, the assets are considered to have less of an impact to National Security. Examples of assets this criterion must be assessed/applied to include, but not limited to, OUO (Ex 2) OUO/ECI (Ex 2 or 3), UCNI, U-NNPI.

- (a) This does not include hard copy or electronic based incidents involving PII as this is the function of the CIO.
 - (b) The compromise or suspected compromise can occur through unauthorized disclosure (i.e., identifiable recipient) and/or several types of medium such as, but not limited to computer, verbal, facsimile, phone, etc. The latter is described in NISPOM as “Improper Transmission”.
- (2) Procedural-based Incidents
- (c) This encompasses incidents associated with the failure to adhere to security procedures and where the supporting facts suggest compromise did not occur or the likelihood was remote. This also includes those incidents where it’s initially believed that there was a “compromise or suspected compromise”, but the subsequent inquiry determines compromise did not occur or the likelihood was remote. An example of procedural-based incident would be the improper marking, handling, and/or storage of classified matter, including Top Secret, SCI, SAP, etc., and where the supporting inquiry suggest compromise did not occur or the likelihood was remote.
 - (d) Accounting for procedural-based incidents is considered a general function of Program Planning and Management, as it provides a mechanism for monitoring the effectiveness of the respective security discipline/program and understanding if the occurrence was an isolated incident or part of a larger systemic issue.

3. INITIAL INQUIRY, CATEGORIZATION, AND REPORTING REQUIREMENTS

- a. The “clock starts” when an incident is brought to the organizations attention. At that point, the site has a maximum of five days to conduct the preliminary inquiry, make the initial categorization, and perform the initial notification(s). The categorization is based on subject policy and any additional criteria as specified in the site plan. Initial reporting and categorization specifications include:
 - (1) Although a maximum of five days are provided, sites are required to report the incident as soon as the incident is categorized. The five days provides flexibility for those incidents requiring additional fact gathering such as classification review, inventory check to locate a potentially lost/missing item versus incidents where there is less ambiguity such as a hostile act or unauthorized discharge. This reporting timeframe is consistent with the recent NISPOM updates.

- (2) Technical Standard XXX can be used to assist sites with incident categorization as it illustrates how mitigating factors can provide assurance that compromise did not occur or the likelihood is remote.
 - (3) If there is still uncertainty at the five day mark, with respect to if there is an incident or the categorization of the incident, the site must make the initial notification based on the more conservative categorization criteria.
 - (4) The contractor security authority will examine and document the pertinent facts and circumstances regarding the incident. If it is determined that an incident of security concern did not occur, no further action is required.
 - (5) If the final inquiry reveals additional details and facts, the policy provides a mechanism to re-categorize the incident as appropriate.
 - (6) Each incident must be assigned a unique local site tracking number.
- b. Category A specific requirements:
- (1) Incidents must be entered into SSIMS; however, additional and/or specific notification requirements must be defined in the approved IOSC Program Plan.
 - (2) The Federal designee(s) within line management must be notified of all Category A incidents.
 - (3) The content provided in the initial notification must be pre-established by the site in their approved IOSC Program Plan. For example, if the incident involves classified matter, it's imperative that the Departmental element with programmatic responsibility for the information be identified. Notification must include if origination was by another agency or foreign government, and a description of the compromised or suspected compromised information. Note: reference Incident Closure section for additional content considerations for the initial report.
 - (4) The approved IOSC Program Plan must document the personnel and organizations in the notification chain.
- c. Category B specific requirements:
- (1) Incidents must be input into SSIMS or a local system identified in the approved IOSC Program Plan. The local system must enable tracking and trending capabilities in support of other PPM functions.
 - (2) While notification and reporting of Category B incidents does not extend beyond the site contractor organization(s), the site must document their internal notification process in their approved IOSC Program Plan.

d. The loss, theft, compromise, or suspected compromise for Top Secret, SCI, SAP, and RD Weapons Data classified information. If the site determines that an incident involving this specific information meets the criterion of loss, theft, compromise, or suspected compromise, then the incident like other Category A incidents must be reported to the cognizant Secretarial Officer, or their designee(s). Once reported, the designee(s) (or element with programmatic responsibility of the information) must review the incident and render two additional determinations.

- (1) The element with programmatic responsibility for the information must determine if the incident constitutes a “significant nuclear defense intelligence loss”, which is defined in the Defense Authorization Act as “any national security or counterintelligence failure or compromise of classified information at a facility of the Department or operated by a contractor of the Department that the Secretary considers likely to cause significant harm or damage to the national security interest of the United States.” This requirement is stipulated in 50 USC 2656.

If it’s determined that the incident meets the “significant nuclear defense intelligence loss” criteria, the appropriate Federal entity(s), after consultation with the Director, Central Intelligence, and the Director, FBI, must provide notification to Congress. The notification of Congress must occur within 30 days of categorizing the event as a 50 USC 2656 reportable incident.

- (2) The element with programmatic responsibility for the information must also determine if the incident warrants a damage assessment. Damage assessments determine potential damage to national security, and are performed to evaluate and document possible countermeasures and conduct actions to limit potential damage. Note: Damage assessments are generally considered for Top Secret, SCI, SAP, and RD Weapons Data classified information; however, they can also be conducted for other incidents involving other levels and categories of classified information. In addition to the specific information compromised or suspected of compromise, some of the other considerations for conducting a damage assessment are, but not limited to, if the incident is associated with a violation of law, if the information was compromised to a wide audience, etc.

e. Reporting Incidents Associated with Sensitive Programs. Incidents of security concern involving activities associated with sensitive programs must follow the same initial reporting process but may omit details because of programmatic controls. These programs include the Sensitive Compartmented Information (SCI) Program, Special Access Program (SAP), the Technical Surveillance Countermeasures (TSCM) Program, the Counterintelligence (CI) Program, or other programs identified by the appropriate Federal designee(s). All subsequent

reporting must be handled within channels until such time as the inquiry report has been closed within the sensitive program. The closure date of the inquiry report must be entered into SSIMS or a locally approved system.

- f. Multi-Program Reporting. An event that meets the criteria for reporting as an incident of security concern does not negate the responsibility to report through other related reporting chains such as, but not limited to the below:
- (1) Occurrence Reporting Processing System (ORPS). Incidents involving an event that affects both safety and security are reportable through DOE O 231.1A, Chg 1, *Environment, Safety, and Health Reporting*.
 - (2) DOE O 151.1C, *Comprehensive Emergency Management System*. Incidents that are reportable under the provisions of DOE O 151.1C, must continue to be reported in accordance with that Order and this policy.
 - (3) Personally Identifiable Information (PII). Incidents involving PII must be reported to the Office of Chief Information Officer in accordance with DOE O 206.1, *Department of Energy Privacy Program*.
 - (4) National Nuclear Security Administration (NNSA) "Flash Reporting" procedures are not affected by requirements in this section.
 - (5) DOE O 475.1, *Counterintelligence Program*. The geographically closest element of the Office of Counterintelligence (OCI)/Office of Defense Nuclear Counterintelligence (ODNCI) must be notified of security incidents involving any credible information that a non-U.S. citizen or an agent of a foreign power is involved.
 - (6) DOE O 221.1A, *Reporting Fraud, Waste and Abuse to the Office of Inspector General*. When an inquiry surrounding an incident of security concern establishes information indicating that fraud, waste, abuse, misuse, corruption, criminal acts, or mismanagement has occurred, the Office of the Inspector General must be notified for information and/or action.
- g. Cyber Security Reporting Requirements. When a cyber related event meets the categorization criteria (e.g., loss, theft, compromise, or suspected compromise of classified information) for reporting as an incident of security concern, it should be reported to the Computer Incident Response Center (CIRC) and the subject policy. However, if the information was not compromised or suspected of compromise then it does not require reporting through the IOSC program.
- h. Special Reporting Situations. Under certain circumstances, related incidents of security concern that are anticipated to recur over a long period of time may be consolidated from a reporting and documentation perspective. This situation will be handled on a case-by-case basis between the contractor security authority and

the Federal designee(s). Specific plans for this reporting process must be documented in the approved IOSC Program Plan.

4. INQUIRY.

a. Conduct of Inquires.

- (1) If an incident affects more than one site/facility, the following criteria must be used in determining the lead organization responsible for conducting the inquiry:
 - (a) If the sites/facilities fall under the purview of a single Program and/or Site Office, that Office must assign responsibility to a lead organization.
 - (b) If the sites/facilities fall under the purview of multiple Program Offices, those Offices must, by mutual agreement, decide on a lead organization with responsibility for the inquiry.
- (2) The following actions must be considered when conducting inquiries into both Category A and B incidents:
 - (a) The scope of the inquiry should reflect both the severity (e.g., procedural versus compromise) and nature (e.g., event of management interest versus security failure) of the incident. For example, if an unauthorized cell phone is brought into an area but immediately discovered and removed, the scope of the inquiry and associated documentation would be far less than where an unauthorized cell phone is “powered on” and physically present during classified discussions.
 - (b) The specific inquiry process established by the contractor security authority must be addressed in their approved IOSC Program Plan. The results of the inquiry and the resulting documentation will help establish the final categorization of the incident, cause of the incident, and subsequent corrective actions.
 - (c) Data Collection
 - Collect all data/information relevant to the incident, such as operations logs, inventory reports, requisitions, receipts, photographs, signed statements, etc.
 - Identify persons associated with the incident and conduct interviews to obtain additional information regarding the incident.

- Ensure physical evidence is protected and controlled and a chain-of-custody is maintained.
 - If available, collect physical evidence associated with the inquiry, such as recorder charts, computer hard drives, defective/failed equipment, procedures, and readouts from monitoring equipment.
- (d) Incident Reconstruction
- Reconstruct the incident of security concern to the greatest extent possible using collected information and other evidence.
 - Develop a chronological sequence of events that describes the actions preceding and following the incident.
- (c) Incident Analysis and Evaluation. Analysis and evaluation determines which systems/functions performed correctly or failed to perform as designed. It provides the basis for determining the cause of the incident and subsequent corrective actions. Inquiry officials must:
- analyze the information collected during the inquiry to determine whether it describes the incident completely and accurately;
 - collect additional data and reconstruct the incident if more information is required;
 - identify any collateral impact with other programs or security interests.
- (3) When an inquiry establishes that classified matter has been compromised by being published in the media, the questions contained in the Department of Justice (DOJ) Eleven-Point Criteria must be answered and coordinated with the programmatic element responsibility for the classified matter. When completing the questions, provide all documentation and appropriate information to support affirmative responses. Each question must be answered affirmatively before the DOJ will initiate a formal investigation into the compromise; however, failure to affirmatively answer all the DOJ criteria does not preclude the DOJ from pursuing administrative or criminal action.
- (a) Could the date and identity of the article or articles disclosing the classified information be provided

- (b) Could specific statements in the article that are considered classified be identified? Was the data properly classified?
 - (c) Is the classified data that was disclosed accurate? If so, provide the name of the person competent to testify concerning the accuracy.
 - (d) Did the data come from a specific document, and, if so, what is the origin of the document and the name of the individual(s) responsible for the security of the classified data disclosed?
 - (e) Could the extent and official dissemination of the data be determined?
 - (f) Has it been determined that the data has not been officially released in the past?
 - (g) Has it been determined that prior clearance for publication or release of the information was not granted by proper authorities?
 - (h) Does review reveal that educated speculation on the matter cannot be made from material, background data, or portions thereof which have been published officially or have previously appeared in the press?
 - (i) Could the data be made available for the purpose of prosecution? If so, include the name of the person competent to testify concerning the classification.
 - (j) Has it been determined that declassification had not been accomplished prior to the publication or release of the data?
 - (k) Will disclosure of the classified data have an adverse impact on the national defense?
- b. Inquiry Officials
- (1) Inquiry officials must conduct inquiries to establish the pertinent facts and circumstances surrounding incidents of security concern.
 - (2) Inquiry officials may be either Federal or contractor employees and must have previous investigative experience or Departmental inquiry official training. Inquiry officials must be knowledgeable of appropriate laws, executive orders, Departmental directives, and/or regulatory requirements.
 - (a) Contractors may conduct inquiries into incidents of security concern; however, if a violation of law is determined or suspected

or the inquiry establishes information that a foreign power or an agent of a foreign power is involved, the contractor must stop further inquiry actions and notify the designated Federal designee(s), which will assume further notification and reporting responsibilities, to include coordination with OCI. In such instances, the contractor must document the known circumstances surrounding the incident of security concern and submit all accumulated data to the Federal designee(s).

- (b) In all instances where the Federal designee(s) disagrees with the contractor report, the Federal designee(s) must assume supplemental inquiry responsibilities.
 - (c) When the inquiry into an incident of security concern necessitates communication with Agencies/organizations external to the Department (e.g., the U.S. Postal Service, the FBI, or other Federal, State, or local agencies), a Federal employee must be responsible for performing all such communication.
 - (d) Contact with Federal, State, and local law enforcement officials may be made by contractors with the written concurrence of the Federal designee(s).
- (3) Inquiry officials are not authorized to detain individuals for interviews or obtain sworn statements; however, they may conduct consensual interviews and obtain signed statements.
 - (4) Inquiry officials must be appointed in writing by the designated Federal entity(s). DOE Headquarters inquiry officials must be appointed in writing by the head of the Office of Headquarters Security Operations.
 - (5) Inquiry officials are responsible for conducting the inquiry and maintaining all documentation associated with the inquiry.
 - (6) When inquiry officials discover suspected or confirmed violations of law, they must immediately notify the designated Federal entity(s).

5. INCIDENT CLOSURE

- a. Once the incident inquiry is completed, a final report must be submitted within 30 days. The final report serves as the basis for closing Category A and B incidents, and similar to inquiries, the level of detail provided in the final report will vary by the category of the incident. The contractor security authority must identify the format and closure report details for the various types of incidents in their approved IOSC Program Plan.
 - (1) All supporting documentation must be retained with the final report.

- (2) The timeframe for completing inquiries and the process for seeking extensions must be addressed in the site IOSC Program Plan.
- (3) Category A incidents must be input and closed via SSIMS, and Category B incidents can be closed using SSIMS or a locally approved system.
- (4) The mechanisms i.e., SSIMS, facsimile, e-mail, etc. for notifying all vested entities must be defined in the approved IOSC Program Plan.
- (5) The plan must document the personnel/organizations in the notification chain.
- (6) The content of the report must be defined by the site in their IOSC Program Plan, but at a minimum it must include:
 - (a) Material and relevant information (i.e., who, what, when, and where) that was not included in the initial report;
 - (b) The name and social security number of the individual(s) who was primarily responsible for the incident, including a record of prior incidents for which the individual had been determined responsible;
 - (c) If applicable, address if the unauthorized disclosure was willful (i.e., intentional);
 - (d) A statement of the corrective action taken to preclude recurrence and the disciplinary action taken against the responsible individual(s), if any;
 - (e) If applicable, specific reasons for reaching the conclusion the theft, loss, compromise, suspected compromise, compromise did not occur, or the likelihood of compromise was remote;
 - (f) Identify any collateral (i.e., extent of condition) impact with other programs or security interests;
 - (g) If the incident involves the compromise or suspected compromise of information, the extent of the dissemination (i.e., number of individuals and their citizenship; global disclosure via cyber mediums, open source publication, etc.) must be identified;
 - (h) Identify specific impacts (i.e., degree of damage, ref. 32 CFR 2001.47) of the incident to the Department and/or National Security. Whenever an incident involves classified matter or interests of more than one Government agency, each agency is

responsible for conducting the damage assessment resulting from its compromised matter.

6. ADMINISTRATIVE ACTIONS

- a. Whenever possible, the responsibility for an incident of security concern must be assigned to an individual rather than to a position or office. When individual responsibility cannot be established and the facts show that a responsible official allowed conditions to exist that led to an incident of security concern, responsibility must be assigned to that official.
- b. Security infractions are issued to document the assignment of responsibility for an incident of security concern. Security infractions may be assigned to individuals who do not possess a security clearance.