Classified Information Security Noncompliance Reporting Criteria

January 2012

MANDATORY SECURITY INCIDENT REPORTING

Classified information security noncompliances are categorized according to the disclosure or potential disclosure of DOE classified information placed at risk. There are two categories of noncompliances that are based on the relative severity of a classified information security incident. The categories are identified by an event category and type. Each of the two categories is further subdivided into three types based on the type of interest (security interest, management interest, and procedural interest).

(NOTE: Security incidents involving the protection and control of classified information categorized as a B requires documented evidence to support the determination that a compromise has not occurred or the likelihood of potential compromise is remote).

Classified Information Security Reportable Noncompliances based on DOE Order 470.4B

This table contains information pertaining to reportable noncompliances involving classified information security. Consult DOE Order 470.4B for complete information about the reporting categories and types.

Significance Level Category	
A	**B**
Category A incidents, which meet a designated level of significance relative to the potential impact on the Department and/or national security, require notification to DOE/NNSA Cognizant Security Officer (CSO), contractor CSO, and reporting in SSIMS.	Category B incidents, which do not meet the Category A criteria, are managed and resolved by the contractor CSO; however, this does not preclude the DOE/NNSA CSO from exercising its oversight responsibilities. The monitoring of Category B incidents by the contractor CSO is essential as it allows management to proactively address reoccurring incidents, thereby minimizing the occurrence of potentially more significant incidents. Category B incidents must be reported in a locally approved system or may be reported in SSIMS.

Incident Type	
Security Interest (SI) This type of incident results in the loss, theft, compromise, or suspected compromise of classified matter.	**Security Interest (SI)** Not Applicable to Part 824
Management Interest (MI) Not Applicable to Part 824	**Management Interest (MI)** Not Applicable to Part 824
Procedural Interest (PI) Not Applicable to Part 824	**Procedural Interest (PI)** This type of incident is associated with the failure to adhere to security procedures that does not result in the loss, theft, compromise, or suspected compromise of classified matter and all evidence surrounding the incident suggests the classified matter was not compromised or the likelihood of compromise is remote.

VOLUNTARY SECURITY REPORTING GUIDANCE

One of the goals of the Department's Security Enforcement Program is to encourage contractor organizations to develop internal assessment processes that can identify deficiencies and noncompliances with classified information security requirements. In addition to self-identifying security concerns, contractors need to be able to report noncompliances and provide the status of corrective actions to the Office of Security Enforcement. This voluntary reporting process is in addition to the mandatory security incident reporting requirements outlined above and contained in DOE O 470.4B.

To ensure a consistent approach in self-reporting security noncompliances by contractor organizations, the Office of Security Enforcement has developed the criteria below. It is suggested that contactor organizations in coordination with their Enforcement Coordinators review the results of assessments to identify any programmatic deficiencies or noncompliances involving classified information protection requirements. If deficiencies or noncompliances are identified that meet a criterion below, these self-identified issues should be entered into the "SA" survey type within the SSIMS survey screens along with the corrective actions that were developed as a result of the causal/root cause analysis to prevent recurrence. The type of reportable condition

(i.e., Repetitive Noncompliances, Programmatic Issue, or Intentional Violation or Misrepresentation) should be reflected in the SSIMS finding comments with an explanation of the self-identified security concern.

Noncompliances that do not meet the reporting requirements contained in DOE O 470.4B or the voluntary security reporting criteria should be reported into the contractor's internal issues tracking systems and trended to timely identify potential recurring or programmatic issues.

Other Classified Information Security Reportable Conditions

The Office of Security Enforcement expects the following types of noncompliances resulting from self-assessments or other internal reviews/trending to be reported in SSIMS for screening purposes and possible mitigation of civil penalties for contractors that self-identify/report security noncompliances.

- Repetitive Noncompliances: Generally, repetitive noncompliances involve two or more different security deficiencies that include substantially similar conditions, locations, organization, program, classification level, classified information/matter, or individual(s). It is reasonable to assume that circumstances should have been appropriately addressed by the contractor's corrective actions resulting from the previous noncompliant condition.

- Programmatic Issue: Typically, programmatic issues are discovered through a review of multiple events or conditions with a common cause, however; may also be identified through a causal analysis or a single security event/incident. Programmatic issues usually involve some weaknesses in administrative or management controls (i.e., security plans, standard operating procedures, physical security configuration) or the implementation of these controls. Additionally, when management determines conditions exist requiring broad corrective actions to improve management or process controls, management has concluded that the problem is programmatic.

- Intentional Violation or Misrepresentation: An intentional violation or misrepresentation may involve, for example, accountable classified matter inventory records or inventory results that are falsified intentionally. A noncompliance should be reported as intentional or willful only if there is supporting evidence that the individual intentionally or negligently falsely reported, or otherwise disregarded classified information security requirements.