

**OFFICE OF SECURITY ENFORCEMENT
VOLUNTARY SECURITY REPORTING
THRESHOLDS GUIDANCE**

April 28, 2009

As previously stated in the email provided to the enforcement community on December 8, 2008, 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 the classified information security requirements. In addition to self-identifying security concerns, contractors need to be able to report noncompliances and provide status of corrective actions to the Office of Security Enforcement. This voluntary reporting process is in addition to the mandatory security incident reporting requirements contained in DOE M 470.4-1, Section N, *Incidents of Security Concern*.

Currently, contractor organizations have the ability to report nuclear safety and worker safety and health self-identified noncompliances through the Noncompliance Tracking System, however; until recently there was not a similar system to self report security noncompliances. As a result, in December 2008 this capability was made available through enhancements to the Safeguard and Security Information Management System (SSIMS), which has been the principle system used by organizations throughout the DOE complex for requisite reporting of security incidents (i.e., IMI-1,-2,-3 and -4) as well as containing DOE audits, survey, and inspection results.

To ensure a consistent approach in self reporting security noncompliance by contractor organizations, the Office of Security Enforcement has developed the below list of thresholds. It is suggested that contractor organizations in coordination with their Enforcement Coordinators review the results of their assessments to identify any programmatic deficiencies or noncompliances involving classified information protection requirements. If deficiencies or noncompliances are identified, suggest these self identified issues 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 specific Management Issues Noncompliance (i.e., Repetitive Noncompliance, Programmatic Issue, and Intentional Violation or Misrepresentation) should be reflected in the SSIMS finding comments with an explanation of the self identified security concern.

Circumstances that do not meet the requirements contained in DOE M 470.4-1, Section N, *Incidents of Security Concern* or the security reporting thresholds should be reported into the contractor's internal issues tracking systems and trended to timely identify potential recurring or programmatic issues.

Classified Information Security Noncompliances Associated with Occurrences/Events

These types of security events would be considered mandatory security incident reporting as defined in DOE M 470.4-1, Section N, *Incidents of Security Concern* and required to be reported in SSIMS.

Management Issues Noncompliances

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

- Repetitive Noncompliance: 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 inventory records or inventory results that are falsified intentionally, such as classified removable electronic media inventory activities. 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.