





- (2) This CRD must be included in all contracts that involve National Security Systems that are used or operated by a contractor or other organization on behalf of DOE, including NNSA, to collect, process, store, display, create, disseminate, or transmit information.
- (3) The heads of Departmental Elements are responsible for notifying contracting officers of affected site/facility management contracts to incorporate this directive into those contracts. Once notified, contracting officers are responsible for incorporating the CRD into each affected contract via the *Laws, Regulations, and DOE Directives* clause of the contracts within 90 days.
- (4) A violation of the provisions of the CRD relating to the safeguarding or security of Restricted Data or other classified information may result in a civil penalty pursuant to subsection a. of section 234B of the Atomic Energy act of 1954 (42 U.S.C. 228b.). The procedures for assessment of civil penalties are set forth in Title 10, Code of Federal Regulations (CFR), Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*, (10 CFR 824).
- (5) As stated in DEAR clause 970, 5204-2, titled *Laws, Regulations, and DOE Directives*, regardless of the performer of the work, site/facility contractors with the CRD incorporated into their contracts are responsible for compliance with the CRD. Affected site/facility management contractors are responsible for flowing down the requirements of the CRD to subcontracts at any tier to the extent necessary to ensure compliance with the requirements. In doing so, contractors must not unnecessarily or imprudently flow down requirements to subcontracts. That is, contractors must both ensure that they and their subcontractors comply with the requirements of this CRD and only incur costs that would be incurred by a prudent person in the conduct of competitive business.
- (6) This Manual does not automatically apply to other than site/facility management contracts. Application of any of the requirements of this Manual to other than site/facility management contracts will be communicated as follows:
  - (a) Heads of Field Elements and Headquarters Departmental Elements. Review procurement requests for new non-site/facility management contracts that involve National Security Systems and contain DEAR clause 952.204-2, *Security Requirements*. If appropriate, ensure that the requirements of the CRD of this Manual are included in the contract.
  - (b) Contracting Officers. Assist originators of procurement requests who want to incorporate the requirements of the CRD of this























**Table 5. Security Audit Controls**

Security Audit Controls								
Control Identifier	Control Name	Protection Index						
		PI-1	PI-2	PI-3	PI-4	PI-5	PI-6	PI-7
AU-1	Security Alarms	AU-1	AU-1	AU-1	AU-1	AU-1	AU-1	AU-1
AU-2	Auditable Events	AU-2	AU-2	AU-2	AU-2	AU-2 (1)	AU-2 (1)	AU-2 (1)
AU-3	Audit Record Contents	AU-3	AU-3	AU-3	AU-3	AU-3 (1) (2)	AU-3 (1) (2)	AU-3 (1) (2)
AU-4	Profile Based Anomaly Detection	N/A	N/A	AU-4	AU-4	AU-4 (1)	AU-4 (1)	AU-4 (1)
AU-5	Complex Attack Heuristics	AU-5	AU-5	AU-5	AU-5	AU-5	AU-5	AU-5
AU-6	Audit Review	AU-6	AU-6	AU-6	AU-6	AU-6 (1)	AU-6 (1)	AU-6 (1)
AU-7	Guarantees of Audit Data Availability	AU-7	AU-7	AU-7	AU-7	AU-7 (1)	AU-7 (1)	AU-7 (1)

**AU-1 SECURITY ALARMS**

The information system security controls shall include or exclude auditable events from the set of audited events based on the user identity and role and shall automatically alert the Information System Security Officer (ISSO) and take [*list of actions (e.g., automatically lock out the system, isolate the system, no additional actions)*] upon detection of a potential security violation.

**AU-2 AUDITABLE EVENTS**

The information system shall provide the capability to compile audit records from multiple components throughout the system into a system-wide (logical or physical), time-correlated audit trail. The information system shall provide the capability to manage the selection of events to be audited by individual components of the system.

The information system security controls shall generate an audit record of the following events:

- Start-up and shutdown of the audit functions

































administrators. The information system security controls shall restrict the ability to modify the authentication data to authorized system administrators and those users explicitly authorized to modify their own authentication data (e.g., passwords).

Control Enhancement (1): For PI-5 through PI-7, the information system security controls shall restrict the ability to modify the information system and object representation of time to ISSOs and authorized system administrators.

### **MT-5 REVOCATION**

The information system security controls shall restrict the ability to revoke security attributes associated with the users within the information system's control to the ISSO and authorized system administrators. The information system security controls shall enforce the immediate revocation of security-relevant authorizations (e.g., next login, next attempt to open the file, within a fixed time). Upon revocation of security-relevant authorizations (e.g., disable subject) the system must [*list of authorized actions (e.g., reassign ownership of objects, disable access to objects)*] to ensure control of objects owned by subject. The information system security controls shall restrict the ability to revoke the security attributes associated with objects within the information system's control to users authorized to modify the security attributes by DAC or MAC security policies. The information system security controls shall enforce the access rights associated with an object when an access check is made.

Control Enhancement (1): For PI-5 through PI-7, the rules of the MAC security policy (DP-6) are enforced on all future operations.

### **MT-6 RESTRICTIONS ON SECURITY ROLES**

The information system security controls shall be able to associate users with roles and shall maintain the roles of ISSO, authorized system administrator, and users explicitly authorized by the DAC security policy to modify object security attributes and their own authentication data (e.g., passwords). The information system security controls shall ensure that the conditions of [*list conditions for the different roles (e.g., least privilege for each use to perform the assigned role; a user assigned as an ISSO cannot also be assigned the system administrator role and vice versa)*] are satisfied.

Control Enhancement (1): For PI-5 through PI-7, the information system security controls shall also maintain the role of users authorized by the MAC security policy to modify object security attributes.

























































