§ 147.15 Guideline M—Misuse of Information technology systems.

(a) *The concern.* Noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. Information Technology Systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

(b) *Conditions that could raise a security concern and may be disqualifying include:* (1) Illegal or unauthorized entry into any information technology system;

(2) Illegal or unauthorized modification, destruction, manipulation or denial of access to information residing on an information technology system;

(3) Removal (or use) of hardware, software, or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;

(4) Introduction of hardware, software, or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations.

(c) *Conditions that could mitigate security concerns include:* (1) The misuse was not recent or significant;

(2) The conduct was unintentional or inadvertent;

(3) The introduction or removal of media was authorized;

(4) The misuse was an isolated event;

(5) The misuse was followed by a prompt, good faith effort to correct the situation.

Subpart B—Investigative Standards

§ 147.18 Introduction.

The following investigative standards are established for all United States Government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information, to include Sensitive Compartmented Information and Special Access Programs, and are to be used by government departments and agencies as the investigative basis for final clearance determinations. However, nothing in these standards prohibits an agency from using any lawful investigative procedures in addition to these requirements in order to resolve any issue identified in the course of a background investigation or reinvestigation.

§ 147.19 The three standards.

There are three standards (Attachment D to this subpart part summarizes when to use each one):

(a) The investigation and reinvestigation standards for ''L'' access authorizations and for access to confidential and secret (including all secret-level Special Access Programs not specifically approved for enhanced investigative requirements by an official authorized to establish Special Access Programs by section in 4.4 of Executive Order 12958) (60 FR 19825, 3 CFR 1995 Comp., p. 33);

(b) The investigation standard for''Q'' access authorizations and for access to top secret (including top secret Special Access Programs) and Sensitive Compartmented Information;

(c) The reinvestigation standard for continued access to the levels listed in paragraph (b) of this section.

§ 147.20 Exception to periods of coverage.

Some elements of standards specify a period of coverage (e.g. seven years). Where appropriate, such coverage may be shortened to the period from the subject's eighteenth birthday to the present or to two years, whichever is longer.

§ 147.21 Expanding investigations.

Investigations and reinvestigations may be expanded under the provisions of Executive Order 12968 (60 FR 40245, 3 CFR 1995 Comp., p. 391) and other applicable statutes and Executive Orders.