

# **COUNTERESPIONAGE.US**

## **Protecting Classified & Sensitive Information Is Our Business**

**The following is a list of the statutory policy and regulatory mandates, regarding Security, Education, Training and Awareness (SETA) for the U.S. Federal Government.**

The Federal Information Security Management Act of 2002 (FISMA) states that each Federal department and agency must include security awareness training within an agency-wide information security program. The security awareness training must inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of information security risks associated with their activities, and their responsibilities in complying with agency policies and procedures to reduce risks. The FISMA also requires each agency to include as part of its performance plan a description of the resources, including budget, staffing, and training, that are necessary to implement the program.

The Computer Security Act of 1987 requires that each Federal agency provide “mandatory periodic training in computer security awareness and accepted computer security practices of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency.”

The OMB Circular A-130, Appendix III, Management of Federal Information Resources, states that personnel be trained in their responsibilities and be addressed in the security plan for each information system. Federal departments and agencies must implement policies, standards, requirements, and procedures that are consistent with standards and guidance issued by NIST. The OMB A-130, Appendix III also requires that: “The head of each agency must ensure that the agency develops a well-trained staff of information resource professionals.”

The Office of Personnel Management (OPM) Regulation 5 CFR Subpart C 930.301, Information Security Responsibilities for Employees who manage or Use Federal Information Systems, provides specific direction regarding the nature and content of the training for categories of information technology users and supports the requirements established by FISMA.

**According to the 5 CFR Part 930, OPM requires that Federal agencies identify employees responsible for the management or use of computer systems that process sensitive information and to provide training to the following groups:** executives, program and functional managers, chief information officers (CIO), Information Technology (IT) security program managers, auditors, other security-oriented personnel, IT function management and operations personnel, and end users.

**In addition, OPM requires that employees in these groups receive their required training within 60 days of their appointment in accordance with 5 CFR Subpart C 930.301.** The OPM also requires that additional training be provided whenever there is a significant change in the agency ISS environment or procedures or when an employee enters a new position involving the handling of sensitive information. The FAA requires annual training to constitute computer security refresher training.

**COUNTERESPIONAGE.US**

**Office: 888-363-7241 / Cell: 561-809-6800**

**[training@counterespionage.us](mailto:training@counterespionage.us)**