General Principles of NISPOM Compliance for Cleared Contractors
Defense Security Service
May 2007, Reposted 7/31/07

The following is provided by the Defense Security Service (DSS) to inform contractors of the principles that DSS will apply in administering its industrial security oversight mission.

- By signing the DoD Security Agreement (DD Form 441), contractors agree to comply with the provisions of the "National Industrial Security Program Operating Manual" (NISPOM). Defense Security Service (DSS) oversees contractor compliance with the NISPOM on behalf of the Department of Defense and 23 other Federal agencies.

- DSS expects that every contractor will comply with the terms of the NISPOM, and DSS will hold every contractor accountable for compliance. Consequences of non-compliance depend upon the severity of the security breach. Depending on specific circumstances, DSS may:

    - Issue Marginal and Unsatisfactory security ratings, and provide appropriate notifications to government contracting activities.
    - Invalidate the contractor's facility security clearance, rendering the contractor ineligible to receive new classified contracts or material.
    - Revoke the facility security clearance.

- Processing classified information on unaccredited information systems is an example of non-compliance with the terms of the NISPOM. DSS will direct contractors who are processing classified information on unaccredited systems to discontinue processing and will take other actions as appropriate.

- DSS representatives are available to advise and assist contractors on security matters. However, DSS has neither the authority nor the resources to carry out the contractor's security responsibilities. The ultimate obligation to comply with the terms of the NISPOM rests with the contractor and its personnel.

- Under certain circumstances, the NISPOM requires contractors to certify to the accuracy of information. The Certificate Pertaining to Foreign Interests (SF-328) and the Information System Security certification are examples. DSS expects that each certification is true when made. DSS will hold the certifier accountable for the validity of the certification. DSS will seek appropriate sanctions against individuals who make false or misleading certifications related to security matters.

- DSS expects that contractor personnel will comply with the terms of user agreements and other applicable published laws, regulations, policies and notices governing access to automated information systems maintained by DSS or other Federal agencies.

- DSS will suspend the access of any person who has violated the terms of user agreements or other applicable rules. (Sharing a JPAS username and password with another person is an example of non-compliance with a user agreement.)

- DSS considers deliberate or willful violations of NISPOM security requirements to be a matter of grave concern. Violations may result not only in the invalidation or revocation of the facility security clearance, but may also lead to the suspension or revocation of the responsible individual's personnel security clearance. Compelling business needs do not justify such behavior.