DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

SRS Criteria Reference Card

Appointed Personnel Duties Job Aid

The Senior Management Official (SMO) will:

- □ Ensure the contractor maintains a system of security controls in accordance with the requirements of the NISPOM.
- □ Appoint an FSO and ITPSO in writing.
- □ Remain fully informed of the facility's classified operations.
- □ Make decisions based on classified threat reporting and their thorough knowledge, understanding, and appreciation of the threat information and the potential impacts caused by a loss of classified information.
- □ Retain accountability for the management and operations of the facility (or legal entity) without delegating that accountability to a subordinate manager.
- □ Annually certify to DCSA, in writing, that a self-inspection was conducted, that other KMP were briefed on the results of the self-inspection, that appropriate corrective actions were taken, and that management fully supports the security program at the cleared facility.
- □ Complete annual security training.
- □ Be listed on the KMP list.
- □ Maintain eligibility for access to classified information at the level of the FCL. Refer to NISPOM 117.9(g) exclusion for changed conditions and temporarily exclusions.

The Facility Security Officer (FSO) will:

- □ Supervise and direct security measures necessary for implementing the applicable requirements of the NISPOM and related USG security requirements to ensure the protection of classified information. This includes, at a minimum:
  - Ensure a system of controls are in place to protect, control, and safeguarding classified information from loss or compromise, and access to classified information is afforded only to cleared and authorized persons.
  - Ensure written security procedures are documented when required by DCSA.
  - Ensure security training is provided to cleared employees consisting of initial briefings, refresher briefings, debriefings, and special briefings (when required).
  - Ensure personnel security clearance eligibility and access records are adequately maintained in the system of record.
  - Ensure a formal self-inspection is conducted at least annually (once a calendar year).
- □ If a FOCI facility under a VT, PA, SSA, or SCA, be the principal advisor to the Government Security Committee (GSC) and attend GSC meetings.
- □ Complete annual security training.
- □ Complete FSO training within 6 months of appointment.
- □ Be listed on the KMP list.
- □ Maintain eligibility for access to classified information at the level of the FCL.

The Insider Threat Program Senior Official (ITPSO) will:

- Establish and execute an insider threat program to gather, integrate, and report relevant and available information indicative of a potential or actual insider threat.
- Ensure the FSO is an integral member of the contractor’s insider threat program.
- Ensure contractor program personnel assigned insider threat program responsibilities and all other cleared employees complete required training.
- Complete annual security training.
- Complete ITPSO training.
- Be listed on the KMP list.
- Maintain eligibility for access to classified information at the level of the FCL.

The Information Systems Security Manager (ISSM) will:

- Be appointed when the contractor is or will be processing classified information on an information system located at the contractor facility.
- Maintain eligibility for access to classified information to the highest level of the information processed on the system(s) under their responsibility.
- Complete training and possess technical competence commensurate with the complexity of the contractor’s classified information system.
- Oversee development, implementation, and evaluation of the contractor’s classified information system program for contractor management, information system personnel, users, and others as appropriate.
- Coordinate with the ITPSO so that insider threat awareness is addressed in the contractor’s information system security program.
- Develop, document, and monitor compliance of the contractor’s information system security program.
- Verify self-inspections are conducted at least every 12 months on the contractor’s information systems that process classified information, and that corrective actions are taken for all identified findings.
- Certify to DCSA in writing that the systems security plan is implemented for each authorized information systems, specified in the SPP; the specified security controls are in place and properly tested; and the information system continues to function as described in the SPP.
- Brief users on their responsibilities with regard to IS security and verify that contractor personnel are trained on the security restrictions and safeguards of the IS prior to access to an authorized information system.
- Develop and maintain security documentation of the security authorization request to DCSA.