

Job Descriptions As Per The Joint DODIIS/Cryptologic SCI Information Systems Security Standards

Information Systems Security Manager (ISSM)

The ISSM is appointed in writing by the authority at a site responsible for information system security. ISSM responsibilities should not be assigned as collateral duties, if at all possible. The ISSM shall:

- Be a U.S. citizen;
- Hold U.S. Government security clearance/access approvals commensurate with the level of information processed by the system; and
- Attend ND-225 training or equivalent.

The ISSM responsibilities include:

- Forwarding a copy of his/her appointment letter to the DAA Rep/SCO.
- Developing and maintaining a formal IS security program.
- Implementing and enforcing IS security policies.
- Reviewing and endorsing all IS accreditation/certification support documentation packages.
- Overseeing all ISSOs to ensure they follow established IS policies and procedures.
- Ensuring ISSM/ISSO review weekly bulletins and advisories that impact security of site information systems to include, AFCERT, ACERT, NAVCIRT, IAVA, and DISA ASSIST bulletins.
- Ensuring that periodic testing (monthly for PL-5 systems) is conducted to evaluate the security posture of the ISs by employing various intrusion/attack detection and monitoring tools (shared responsibility with ISSOs).
- Ensuring that all ISSOs receive the necessary technical (e.g., operating system, networking, security management, SysAdmin) and security training (e.g., ND-225 or equivalent) to carry out their duties.
- Assisting ISSOs to ensure proper decisions are made concerning the levels of concern for confidentiality, integrity, and availability of the data, and the protection levels for confidentiality for the system.
- Ensuring the development of system accreditation/certification documentation by reviewing and endorsing such documentation and recommending action to the DAA Rep/SCO.
- Ensuring approved procedures are in place for clearing, purging, declassifying, and releasing system memory, media, and output.
- Maintaining, as required by the DAA Rep/SCO, a repository for all system accreditation/certification documentation and modifications.
- Coordinating IS security inspections, tests, and reviews.
- Investigating and reporting (to the DAA/DAA Rep/SCO and local management) security violations and incidents, as appropriate.

- Ensuring proper protection and corrective measures have been taken when an IS incident or vulnerability has been discovered.
- Ensuring data ownership and responsibilities are established for each IS, to include accountability, access and special handling requirements.
- Ensuring development and implementation of an effective IS security education, training, and awareness program.
- Ensuring development and implementation of procedures in accordance with configuration management (CM) policies and practices for authorizing the use of hardware/software on an IS. Any changes or modifications to hardware, software, or firmware of a system must be coordinated with the ISSM/ISSO and appropriate approving authority prior to the change.
- Developing procedures for responding to security incidents, and for investigating and reporting (to the DAA Rep/SCO and to local management) security violations and incidents, as appropriate.
- Serving as a member of the configuration management board, where one exists (however, the ISSM may elect to delegate this responsibility to the ISSO.)
- Working knowledge of system functions, security policies, technical security safeguards, and operational security measures.
- Accessing only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.

Information Systems Security Officer (ISSO)

The ISSO shall:

- Be a U.S. citizen and
- Hold U.S. Government security clearance/access approvals commensurate with the level of information processed by the system.

Responsibilities of the ISSO shall include:

- Ensuring systems are operated, maintained, and disposed of in accordance with internal security policies and practices as outlined in the accreditation/certification support documentation package.
- Attending required technical (e.g., operating system, networking, security management, SysAdmin) and security (e.g., ND-225 or equivalent) training relative to assigned duties.
- Ensuring all users have the requisite security clearances, authorization, need-to-know, and are aware of their security responsibilities before granting access to the IS.
- Ensuring that proper decisions are made concerning levels of concern for confidentiality, integrity, and availability of the data, and the protection level for confidentiality for the system.
- Reporting all security-related incidents to the ISSM.
- Initiating protective and corrective measures when a security incident or vulnerability is discovered, with the approval of the ISSM.
- Developing and maintaining an accreditation/certification support documentation package for system(s) for which they are responsible.
- Conducting periodic reviews to ensure compliance with the accreditation/certification support documentation package.
- Ensuring Configuration Management (CM) for IS software and hardware, to include IS warning banners, is maintained and documented.
- Serving as member of the Configuration Management Board if so designated by the ISSM.
- Ensuring warning banners are placed on all monitors and appear when a user accesses a system.
- Ensuring system recovery processes are monitored and that security features and procedures are properly restored.
- Ensuring all IS security-related documentation is current and accessible to properly authorized individuals.
- Formally notifying the ISSM and the DAA Rep/SCO when a system no longer processes classified information.
- Formally notifying the ISSM and the DAA Rep/SCO when changes occur that might affect accreditation/certification.
- Ensuring system security requirements are addressed during all phases of the system life cycle.

- **Following procedures developed by the ISSM, in accordance with configuration management (CM) policies and practices, for authorizing software use prior to its implementation on a system. Any changes or modifications to hardware, software, or firmware of a system must be coordinated with the ISSM and appropriate approving authority prior to the change.**
- **Establishing audit trails and ensuring their review.**
- **Administering user identification (USERID) and authentication mechanisms of the IS or network.**
- **Ensuring the most feasible security safeguards and features are implemented for the IS or network.**
- **Ensuring no attempt is made to strain or test security mechanisms, or perform network line monitoring, or keystroke monitoring without appropriate authorization.**
- **Performing network monitoring for the purpose of identifying deficiencies, but only with approved software, and after notifying the ISSM and other appropriate authority.**
- **Accessing only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.**