

DOC IT Security Evaluation Checklist: Information System Security Officer (ISSO) Responsibilities

An Information System Security Officer (ISSO) is a DOC federal employee or contractor who ensure all aspects of information systems security are in place and operational. ISSOs implement the system-level controls and maintain system documentation. The ISSO acts to ensure compliance with automated information system (AIS) security procedures. This checklist provides ISSOs with a self-assessment tool, and their supervisors or Contracting Officer's Technical Representatives with a performance evaluation tool, to evaluate the level of compliance with ISSO duties as established by the

- *DOC IT Security Program Policy and Minimum Implementation Standards (ITSPP)*,
- *DOC Remote Access Policy and Minimum Implementation Standards (RASP)*, and
- *DOC Policy on Password Management (PPM)*.

This is an assessment of (name/operating unit/office):	
Self Assessment	Assessment Date:
Third Party Evaluation	Assessor (name/title/org.):

Status Codes: 1 = Not Started 2 = In Process 3 = In Place

Performance Levels:

- 1 ISSO is aware of comprehensive IT security policies in place
- 2 ISSO is aware of comprehensive IT security policies as well as detailed procedures in place
- 3 ISSO is familiar with comprehensive IT security policies and detailed procedures in place and fully implements them for the system
- 4 ISSO is familiar with comprehensive IT security policies and detailed procedures in place, fully implements them for the system, and tests them for effectiveness
- 5 ISSO is familiar with, and fully implements and tests, comprehensive IT security policies and detailed procedures in place as part of a fully integrated IT security program

	Information System Security Officer (ISSO) Responsibilities	Cross Reference	Status	Performance Levels
1	Advise the system owner regarding security considerations in applications systems procurement or development, implementation, operation and maintenance, and disposal activities (i.e. life cycle management)	ITSPP 2.1.10		
2	Assist in the determination of an appropriate level of security commensurate with the level of sensitivity	ITSPP 2.1.10, 3.8.2.1		
3	Assist in the development and maintenance of system documents, including system security plans, contingency plans, and other system documentation (hardware, software, and user manuals)	ITSPP 2.1.10, RASP		
4	Participate in risk assessments to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies.	ITSPP 2.1.10		
5	Participate in self-assessment of system safeguards and program elements and in certification and accreditation of the system;	ITSPP 2.1.10, 3.4.1.2		
6	Report all incidents to the appropriate Computer Incident Response Capability (CIRC) or Computer Incident Response Team (CIRT) in a timely manner.	ITSPP 3.14.3, RASP		
7	Maintain cooperative relationship with business partners or other interconnected systems.	ITSPP 2.1.10		
8	Handle and investigate incidents in cooperation with and under the direction of the IT Security Officer.	ITSPP 3.14.6		