

DOC IT Security Evaluation Checklist: System/Network Administrator Responsibilities

System/network administrators are responsible for certain aspects of system security, such as adding and deleting user accounts as authorized by the system owner, as well as normal operations of the system in keeping with job requirements. The role of a system administrator may include security of LAN or application administration.

This checklist provides system/network administrators 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 system/network administrator's duties as established by the *DOC IT Security Program Policy and Minimum Implementation Standards* (ITSP), Section 2.1.11, as well as the additional sections of the ITSP cited in the second column of the checklist.

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** System/network administrator is aware of comprehensive IT security policies in place
- 2** System/network administrator is aware of comprehensive IT security policies as well as detailed procedures in place
- 3** System/network administrator is familiar with comprehensive IT security policies and detailed procedures in place and fully implements them for the system
- 4** System/network administrator is familiar with comprehensive IT security policies and detailed procedures in place, fully implements them for the system, and tests them for effectiveness
- 5** System/network administrator 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

	System/Network Administrator Responsibilities	ITSPP References*	Status	Performance Level
1	Assist system owners in the development and maintenance of security plans for all general support systems and major applications under their responsibility.	4.3		
2	Assist system owners in the development and maintenance of contingency plans for all general support systems and major applications under their responsibility.	9		
3	Participate in risk assessments to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies.	3		
4	Participate in self-assessments of system safeguards and program elements.	6.3.1		
5	Participate in certification and accreditation of the system.	6		
6	Assist the system owner in the identification of resources needed to effectively implement technical security controls.			

* In addition to Section 2.1.11

System/Network Administrator Responsibilities		ITSPP References*	Status	Performance Level
7	Ensure the integrity in implementation and operation of technical security controls by conducting control security test and evaluation.	6.3.3		
8	Develop system administration and operational procedures and manuals as directed by the system owner.			
9	Evaluate and develop procedures that assure proper integration of service continuity with other system operations.			
10	Notify the responsible Information System Security Officer, or if none, the responsible IT Security Officer of any suspected incidents in a timely manner, and assist in the investigation of incidents if necessary;	14.7.1		
	On a routine basis and as warranted by the system's impact level:	14.6.1		
	(a) Review audit logs from the perimeter security intrusion detection systems;			
	(b) Review audit logs for servers and hosts on the internal, protected network;			
	(c) Review all trouble reports received by system administration personnel for symptoms that might indicate intrusive activity; suspicious symptoms should be reported to Network or IT security personnel;			
(d) Check host-based intrusion-detection tools.				
11	Read and understand all applicable training and awareness materials;	15		
12	Read and understand all applicable use policies or other rules of behavior regarding use or abuse of operating unit IT resources;	4.5		
13	Know and abide by all applicable DOC and operating unit policies and procedures.			
14	System administrators must be familiar with the restrictions established by the Electronic Communications Privacy Act of 1986 (Public Law 99-508), with respect to legal issues surrounding the interception of certain communications and other forms of surveillance, and implement appropriate system policies regarding keystroke monitoring.	18.2.2		