SANS Institute
Security Consensus Operational Readiness Evaluation

SCORE Security Checklist

NISPOM Chapter 8 – Check List

Based on NISPOM Chapter 8 Requirements.
Check List Compiled By: Darren Bennett (dbennett@cyberintel.com) and Joe Keegan (joe_jjk3@hotmail.com)

Assessor Name:				Assessment Date:	

Reference			Objective and Security Test	Results	
Checklist	**Standard**	**Sub-Section**	**Confirmation Question**	**Findings**	**Compliance Y/N**
Section 1. Responsibilities and Duties					
1.100.	8.100.	General			
1.101a	8.101a	Responsibilities For CSA	Establishment of a line of authority for training, oversight, program review, certification, and accreditation of IS used by contractors for the processing of classified information		
1.101a2	8.101a-2	Responsibilities For CSA	The CSA conducted a risk management evaluation based on the contractors facility, the classification, and sensitivity of the information processed		
1.101b	8.101b	Responsibilities For CSA	An IS Security Policy addressing the classified processing environment has been published and promulgated		
1.101b2	8.101b2	Responsibilities For CSA	An IS Security Manager (ISSM) has been appointed with oversight responsibility for the development, implementation, and evaluation of the facility's IS security program		
1.101b3	8.101b3		Contractor management is certain that the ISSM is trained to a level commensurate with the complexity of the facility's IS		
1.102.	8.102.	Designated Accrediting/ Approval Authority	The CSA has been Designated Accrediting/Approving authority (DAA)		
1.103.	8.103.	IS Security Manager (ISSM) Responsibilities	The ISSM has read and understands the responsibilities as per Section 8.103 of the NISPOM chapter 8		
1.104.	8.104.	Information System Security Officer(s) (ISSO)	The ISSO(s) has/have read and understand the responsibilities as per Section 8.104 of the NISPOM chapter 8		
1.105.	8.105.	Users of IS	Privileged and general users of the IS have read and understand the responsibilities as per Section 8.105 of the NISPOM chapter 8		
Section 2. Certification and Accreditation					
2.100.	8.200.	Overview			
2.101.	8.201.	Certification Process			
2.102.	8.202.	Accreditation			
Section 3. Common Requirements					
3.100.	8.300.	Introduction			
3.101.	8.301.	Clearing and Sanitization			
3.101a.	8.301a.	Clearing	Prior to re-use of media in an area that has an acceptable level of protection for the data, has all data on the media been eradicated? Including Memory, Buffers and reusable memory To prevent access to previously stored information.		
3.101b.	8.301b.	Sanitization	Prior to release of media to an area that does not have an acceptable level of protection for the data, has all data on the media been removed? (i.e. Release from classified information controls or release to a lower classification level)		
3.102.	8.302.	Examination of Hardware and Software			
3.102a.	8.302a.	IS Software	Has all commercially procured software been tested to ensure the software contains no obvious features that might be detrimental to the security of the IS? Has Security-related software been tested to verify that the security features function as specified?		
3.102b.	8.302b.	IS Hardware	Has the hardware been examined to determine that it is in good working order and has no elements that might be detrimental to the secure operation of the IS when under facility control and cognizance? (Changes and developments that affect security may require re-examination)		
3.103.	8.303.	Identification and Authentication			

		Management			
3.103a.	8.303a.	Unique Identification	Is each user uniquely identified and is that identity associated with all auditable actions taken by that individual?		
3.103b.	8.303b.	Authentication at Login	Is each user required to authenticate their identity at login by using an authenticator (i.e. password) as well as their user id before executing any application or utility on the system?		
3.103c.	8.303c.	Applicability of Logon Authentication	Is it possible to waive the requirement for Logon Authentication (are **all** of the following statements true?) *The workstation does not have a permanent internal hard drive, and the removable hard drive and other associated storage media are stored in an approved security container when not in use *All of the users with access to the workstation and the security container/ removable media have the required clearance level and need-to-know for all of the data processed on the workstation *The workstation is located within an approved security area, and all uncleared/lower-cleared personnel are escorted within the area.		
3.103d.	8.303d.	Access to Authentication Data	Has access to authentication data been restricted to authorized personnel through the use of encryption or file access controls, or both?		
3.103e.	8.303e.	User ID Reuse	Have all previous access authorizations (including file accesses for that user ID) been removed prior to reuse of any user ID's? (If applicable)		
3.103f.	8.303f.	User ID Removal	Have users that have terminated employment, lost access to the system for cause, or no longer have reason to access the IS had their user ID and its authentication disabled or removed from the system?		
3.103g.	8.303g.	User ID Revalidation	User IDs are revalidated annually (or more frequently)		
3.103h.	8.303h.	Protection of Individual Authenticator	Authenticators in the form of knowledge (password) or possession (smart card, keys) are not shared with anyone.		
3.103i.	8.303i.	Protection of Individual Passwords	Are **all** of the following requirements met when using passwords as authenticators? (1) Passwords shall be protected at a level commensurate with the sensitivity level or classification level and classification category of the information to which they allow access. (2) Passwords shall contain a minimum of eight non-blank characters, shall be valid for no longer than 12 months and changed when compromised. (3) Passwords shall be generated by a method approved by the CSA. Password acceptability shall be based on the method of generation, the length of the password, password structure, and the size of the password space. The password generation method, the length of the password, and the size of the password space shall be described in an attachment to the SSP. (4) When an IS cannot prevent a password from being echoed (e.g., in a half-duplex connection), an overprint mask shall be printed before the password is entered to conceal the typed password. (5) User software, including operating system and other security-relevant software, comes with a few standard authenticators (e.g., SYSTEM, TEST, and MASTER) and passwords already enrolled in the system. The ISSO shall ensure that the passwords for all standard authenticators are changed before allowing the general user population access to the IS. The ISSO shall also ensure that these passwords are changed after a new system version is installed or after other action is taken that might result in the restoration of these standard passwords.		
3.104.	8.304.	Maintenance			
3.104a.	8.304a.	Cleared Maintenance Personnel	Have all maintenance personal been cleared to the highest classification level on the system and been indoctrinated for all information processed on the system? When possible, will an appropriately cleared and technically knowledgeable, facility employee be present within the area where the maintenance is being performed to ensure that security procedures are being followed?		
3.104b.	8.304b.	Uncleared (or Lower-Cleared) Maintenance Personnel	Are the following procedures followed when allowing access to the system by uncleared or lower-cleared maintenance personnel? (1) an appropriately cleared and technically qualified escort monitors and records the maintenance person's activities in a maintenance log. Uncleared maintenance personnel must be U.S. citizens. (2) System initiation and termination shall be performed		

			by the escort. In addition, keystroke monitoring shall be performed during access to the system (3) Prior to maintenance, the IS shall be completely cleared and all non-volatile data storage media shall be removed or physically disconnected and secured. When a system cannot be cleared procedures, which are identified in the SSP, shall be enforced to deny the maintenance personnel visual and electronic access to any classified data contained on the system.		
3.105.	8.305.	Malicious Code			
			Have policies and procedures to detect and deter incidents caused by malicious code, such as viruses or unauthorized modification to software, been implemented? Are all files checked for viruses before being introduced on the IS and checked for other malicious code as feasible? Is the use of personal or public domain software strongly discouraged? Each installation of such software must be approved by the ISSM.		
3.106.	8.306.	Marking Hardware, Output, and Media			
3.106a.	8.306a.	Hardware Components	Do all components of the IS, including input/output devices that have the potential for retaining information, terminals, stand-alone microprocessors, or word processors used as terminals, bear a conspicuous, external label that states the highest classification level and most restrictive classification category of the information accessible to the component in the IS? (If the CSA requires that labels be color coded to indicate classification level they shall be orange for Top Secret, red for Secret, blue for Confidential, and green for unclassified.)		
3.106b.	8.306b.	Hard Copy Output and Removable Media	Have methods been established for hard copy output (paper, fiche, film, and other printed media) and removable media to be marked with visible, human-readable, external markings to the accreditation level of the IS unless an appropriate classification review has been conducted or in the case of media, the information has been generated by a tested program verified to produce consistent results and approved by the CSA. Such programs will be tested on a statistical basis to ensure continuing performance.		
3.106c.	8.306c.	Unclassified Media	Is all unclassified media in the CSA-approved areas marked as unclassified?		
3.107.	8.307.	Personnel Security			
			For all personnel with system access, are system security policies; and maintaining and monitoring the confidentiality, integrity, and availability attributes that are inherent within their IS. Duties, responsibilities, privileges, and specific limitations of IS users, both general and privileged, been specified in writing? Are security duties distributed to preclude any one individual from adversely affecting operations or the integrity of the system?		
3.108.	8.308.	Physical Security			
3.108a.	8.308a.	Safeguards	Have safeguards been established that prevent or detect unauthorized access to the IS and unauthorized modification of the IS hardware and software? Hardware integrity of the IS, including remote equipment, shall be maintained at all times, even when all classified information has been removed from the IS.		
3.108b.	8.308b.	Classified Processing	All classified processing takes place in a CSA-Approved area.		
3.108c.	8.308c.	Visual Access	Are all devices that display or output information in human-readable form positioned to prevent unauthorized individuals from reading the information?		
3.108d.	8.308d.	Unescorted Access	Do all personnel granted unescorted access to the area containing the IS have an appropriate security clearance?		
3.109.	8.309.	Protection of Media			
			Has/Will media be protected to the level of accreditation until an appropriate classification review has been conducted.		
3.110.	8.310.	Review of Output and Media			
3.110a.	8.310a.	Human readable output review	An appropriate sensitivity and classification review shall be performed on human-readable output before the output is released outside the security boundary to determine whether it is accurately marked with the appropriate classification and applicable associated security markings.		
3.110b.	8.310b.	Media Review	Electronic output, such as files, to be released outside		

			the security boundary shall be verified by a comprehensive review (in human-readable form) of all data on the media including embedded text (e.g., headers and footer) before being released. Information on media that is not in human-readable form (e.g., embedded graphs, sound, video, etc.) will be examined for content using the appropriate software application. CSA-approved random or representative sampling techniques may be used to verify the proper marking of large volumes of output.		
3.111.	8.311.	Configuration Management			
3.111a.	8.311a.	Configuration Documentation	Have processes been implemented to identify and document the type, model and brand of system or network component (e.g., workstation, personal computer, or router), security-relevant software product names and version or release numbers, and physical location?		
3.111b.	8.311b.	System Connectivity	Have procedures been implemented to identify and document system connectivity, including any software used for wireless communication, and any communications media?		
3.111c.	8.311c.	Connection Sensitivity	Is the sensitivity level of each connection or port controlled by the Security Support Structure (SSS) documented?		
3.111d.	8.311d.	CM Plan	Has the facility CM program been documented in a CM plan that includes the following? (1) Formal change control procedures to ensure the review and approval of security-relevant hardware and software. (2) Procedures for management of all documentation, such as the SSP and security test plans, used to ensure system security. (3) Workable processes to implement, periodically test, and verify the CM plan. (4) A verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted.		

Section 4. Protection Measures

4.100.	8.400.	Protection Profiles (intro)			
4.101.	8.401.	Level of Concern			
4.101a.	8.401a.	Information Sensitivity Matrices	Have the information sensitivity matrices (tables 1, 2, and 3 in Section 4 of the NISPOM Chapter 8) been used to establish the appropriate protection levels for confidentiality, and the level of concern for integrity, and availability? (if contractually mandated) (1) Has a determination of high, medium, or basic been made for each of the three attributes: confidentiality, integrity, and availability? It is not necessary for the level of concern to be the same for all attributes of the system. (2) Has the highest level of concern for each category been used when multiple applications on a system result in different levels of concern for the categories of confidentiality, integrity, and availability?		
4.101b.	8.401b.	Confidentiality Level of Concern	**What is the established Confidentiality Level of Concern?** In considering confidentiality, the principal question is the necessity for supporting the classification levels and the categories of information (e.g., Secret National Security Information) on the system in question. The Protection Level Table for Confidentiality (Table 4) combines the processing environment with the level of concern for confidentiality to provide a Protection Level. The Protection Level is then applied to Table 5 to provide a set of graded requirements to protect the confidentiality of the information on the system.	_____	
4.101c.	8.401c.	Integrity Level of Concern	**What is the established Integrity Level of Concern?** In considering integrity, the principal question is the necessity for maintaining the integrity of the information on the system in question.	_____	
4.101d.	8.401d.	Availability Level of Concern	**What is the established Availability Level of Concern?** In considering availability, the principal consideration is the need for the information on the system in question to be available in a fixed time frame to accomplish a mission.	_____	

4.102.	8.402.	Protection Level			
			(Determined by the relationship between two parameters: first, the clearance levels, formal access approvals, and need-to-know of users; and second, the level of concern based on the classification of the data on a particular system.)		
4.102a.	8.402a.	Protection Level 1	Do all users have all required approvals for access to **all** information on the system? (all users must have all required clearances, formal access approvals, and the need-to-know for all information on the IS, i.e. dedicated mode.)		
4.102b.	8.402b.	Protection Level 2	Do all users have all required clearances, and all required formal access approvals,**but at least one user lacks the need-to-know** for some of the information on the system? (i.e. a system high mode.)		
4.102c.	8.402c.	Protection Level 3	Do all users have all required clearances, but at least one user lacks formal access approval for some of the information on the system?(i.e. compartmented mode.)		
4.102.	8.402.	Appropriate Protection Level	What is the established Protection Level for the system? (based on the criteria above)	_____	
4.103.	8.403.	Protection Profiles			
			The tables listed in section 8-403 of the NISPOM chapter 8 represent Protection Profiles. Use these tables to assist in determining the Level of Concern and Protection Level of each system.		

Section 5. Special Categories

5.100.	8.500.	Overview			
5.101.	8.501.	Single-User, Stand-alone			
			Is the system a single-user, stand-alone system? Has the CSA approved administrative and environmental protection measures for the system in lieu of technical ones? What are the specific administrative/environmental measures that have been specified? (or where are they defined) (Systems that have one user at a time, are sanitized between users and periods of different classification/sensitivity, are periods processing systems as covered below)		
5.102.	8.502.	Periods Processing			
5.102a.	8.502a.	Periods Processing	Will the system be used for Periods Processing? (Periods processing provides the capability to either have more than one user or group of users (sequentially) on a single-user IS who do not have the same need-to-know or who are authorized to access different levels of information; or use an IS at more than one protection level (sequentially).)		
5.102b.	8.502b.	Sanitization after use.	What specific sanitization procedures will be employed **by each user** before and after each use of the system?		
5.102c.	8.502c.	Sanitization Between Periods	What procedures for sanitization of all information **before transitioning from one period to the next** (e.g., whenever there will be a new user(s) who does not have an access authorization or need-to-know for data processed during the previous period, changing from one protection level to another) have been established?		
5.102d	8.502d.	Media For Each Period	Is there **separate** media for each period of processing? Including copies of operating systems, utilities, and applications software?		
5.102e.	8.502e.	Audit	If there are multiple users of the system and the system is not capable of automated logging, has the CSA required manual logging? (Audit trails are not required for single-user stand-alone systems)		
5.103.	8.503.	Pure Servers			
5.103a.	8.503a.	Specialized Systems	Specialized systems acting as pure servers in a network that do not fit the protection level criteria may need fewer technical security countermeasures. Are the following statements true of the system? (**ALL** must be true) (1) No user code is present on the system. (2) Only system administrators and maintainers can access the system. (3) The system provides non-interactive services to clients (e.g., packet routing or messaging services). (4) The hardware and/or application providing network		

			services otherwise meet the security requirements of the network. (5) The risk of attack against the Security Support Structure (SSS) using network communication paths is sufficiently low. (6) The risk of attack against the SSS using physical access to the system itself is sufficiently low.		
5.103b.	8.503b.	The Platform	Does the system meet PL-3 security requirements? (minimum) Are all users who use the guard/server application limited to specific capabilities? Does the guard application/server provide more stringent technical protections appropriate for the systems protection level and operational environment? Are assurances appropriate to the level of concern for the system implemented?		
5.103c.	8.503c.	Understanding what is NOT a "Pure Server"	Is it understood that a system with general users or that executes general user code are NOT "pure servers"? (and must therefore meet all security requirements specified for their protection level and operational environment)		
5.103d.	8.503d.	The Term "Pure Server"	Is it understood that a system may be considered a "pure server" even though it may not resemble what has been traditionally refered to as a server? (i.e. a messaging system on a general purpose computer platform could be accredited under this section if it meets the requirements in 8.503b (above))		
5.103e.	8.503e.	Understanding that these exceptions do not imply relaxation of other security requirements	Is it understood that the above mentioned technical security requirements that have been eased do not imply any relaxation in other security requirements? (i.e. physical and communications requirements) Is it also understood that this easing of technical requirements is predicated upon adequate application of physical security and other appropriate security disciplines?		
5.104.	8.504.	Tactical, Embedded, Data-Acquisition, and Special-Purpose Systems	Has the CSA determined that this system is sufficiently incapable of alteration, and that the application(s) running on the system provide an adequate level of security? (If so, the system does not have to meet additional security requirements specified for more-general-purpose systems in this section)		
5.105.	8.505.	Systems with Group Authenticators	Provided that the systems includes an acceptable level of individual accountability, shall group authenticators be used for broader access after the use of a unique authenticator for initial authentication and will this be documented in the SSP? (Group authenticators may not be shared with anyone outside the group)		

Section 6. Protection Requirements

6.100.	8.600.	Introduction			
6.101.	8.601.	Alternate Power Source (Power)	Have the power requirements for each of the systems been determined? (None, Power 1 or Power 2)		
6.101a.	8.601a.	Power 1 Requirements	Have procedures to gracefully shutdown systems without the loss of data been developed and tested?		
			Have all the systems been attached to an alternate power source, such as an un-interruptible power supply (UPS)? If not has this decision been documented?		
6.101b.	8.601b.	Power 2 Requirements	Have the time requirements to transfer the system to another power source for the hosted applications been documented?		
			Have procedures to transfer systems to another power source within the required time been developed and tested?		
6.102.	8.602.	Audit Capability	Have the audit requirements for each of the systems been determined? (Audit 1, Audit2, Audit3 or Audit 4)		
6.102a.	8.602a.	Audit 1 Requirements			
6.102a1.	8.602a1.	Automated Audit Trail Creation	Has the system been configured to create and maintain an audit trail or log that includes the information located in Section 8.602.1a-1f of NIPSOM Chapter 8?		
			If the system is PL-1 and is unable to create an maintain an audit trail, have procedures been developed and documented to provide an alternate method of accountability for user activities?		
6.102a2.	8.602a2.	Audit Trail Protection	Have the contents of the audit trails been protected against unauthorized access, modification, or deletion?		
6.102a3.	8.602a3.	Audit Trail Analysis	Is analysis of the audit trail performed at least weekly? Are relevant events from that analysis documented and reported?		
			Is the frequency of audit trail analysis documented in the System Security Plan (SSP)?		
6.102a4.	8.602a4.	Audit Record Retention	Are audit records retained for at least on review cycle or as required by the CSA?		
6.102b.	8.602b.	Audit 2 Requirements	Is the system in compliance with the audit 1 requirements?		
6.102b1.	8.602b1.	Individual Accountability	Is periodic testing of individual accountability mechanisms conducted by the ISSO or ISSM?		
6.102c.	8.602c.	Audit 3 Requirements	Is the system in compliance with the audit 2 requirements?		
6.102c1.	8.602c1.	Automated Audit Analysis	Is audit analysis and reporting scheduled and performed by automated tools?		
6.102d.	8.602d.	Audit 4 Requirements	Is the system in compliance with the audit 3 requirements?		

6.102d1.	8.602d1.		Does the audit trail record changes to the mechanism's list of user formal access permission?		
6.103.	8.603.	Backup and Restoration of Data (Backup)	Have the backup and recovery requirements for each of the systems been determined? (backup 1, backup 2, backup 3)		
6.103a.	8.603a.	Backup 1 Requirements			
6.103a1.	8.603a1.	Backup Procedures	Have procedures for the regular backup of all essential and security-relevant information, including software tables and settings, such as router tables, software, and documentation, been documented?		
6.103a2.	8.603a2.	Backup Frequency	Has the frequency of backups been defined by the ISSM, with the assistance of the GCA, and documented in the backup procedures?		
6.103b.	8.603b.	Backup 2 Requirements	Is the system compliant with backup 1 requirements?		
6.103b1.	8.603b1.	Backup Media Storage	Is media containing backup files and backup documentation stored at another location?		
6.103b2.	8.603b2.	Verification of Backup Procedures	Is periodic verification of backup procedures preformed?		
6.103c.	8.603c.	Backup 3 Requirements	Is the system compliant with backup 2 requirements?		
6.103c1.	8.603c1.	Information Restoration Testing	Is incremental and complete restoration of information from backup media tested on an annual basis?		
6.104.	8.604.	Changes to Data (Integrity)	Have the integrity requirements for each of the systems been determined? (none, integrity 1 and integrity 2)		
6.104a.	8.604a.	Integrity 1 Requirements			
6.104a1.	8.604a1.	Change Procedures	Have procedures and technical system features been implemented to ensure that changes to the data and IS software are executed only by authorized personnel or processes?		
6.104b.	8.604b.	Integrity 2 Requirements	Is the system compliant with integrity 1 requirements?		
6.104b1.	8.604b1.	Transaction Log	Is the transaction log, protected from unauthorized changes, available to allow the immediate correction of unauthorized data and IS software changes and the off-line verification of all changes at all times?		
6.105.	8.605.	Data Transmission (Trans)			
6.105a.	8.605a.	Trans 1 Requirements	Are one or more protections, defined in section 8.605a1, used whenever classified information is to be transmitted through areas or components where individuals not authorized to have access to the information may have un-escorted physical or uncontrolled electronic access to the information or communications media (e.g., outside the system perimeter)?		
6.106.	8.606.	Access Controls (Access)	Have the access requirements for each of the systems been determined? (access 1, access 2, access 3)		
6.106a.	8.606a.	Access 1 Requirements			
6.106a1.	8.606a1.	Physical Access	Is physical access by unauthorized individuals only allowed under the constant supervision of technically qualified, authorized personnel?		
6.106b.	8.606b.	Access 2 Requirements	Is the system compliant with the access 1 requirements?		
6.106b1.	8.606b1.	Discretionary Access Controls	Have discretionary access controls been implemented on the system?		
			Does the discretionary access control policy include administrative procedures to support the policy and its mechanisms?		
6.106c.	8.606c.	Access 3 Requirements	Is the system compliant with the access 2 requirements?		
6.106c1.	8.606c1.		Is there a process or mechanism that allows users (or processes acting on their behalf) to determine the formal access approvals granted to another user?		
6.106c2.	8.606c2.		Is there a process or mechanism that allows users (or processes acting on their behalf) to determine the sensitivity level of data?		
6.107.	8.607.	Identification and Authentication (I&A)	Have the I&A requirements for each of the systems been determined? (I&A 1, I&A 2, I&A3, I&A 4 and I&A5)		
6.107a.	8.607a.	I&A 1 Requirements	Are there procedures that include provisions for uniquely identifying and authenticating the users?		
6.107b.	8.607b.	I&A 2 Requirements	Is the system compliant with the I&A 1 requirements?		
6.107b1.	8.607b1.	Unique Identifiers	Is there a management mechanism that ensures a unique identifier for each user and that associates that identifier with all auditable actions taken by the user?		
		Authenticators	Are the requirements for authenticators defined in section 8.607.b1 documented in the SSP?		
6.107c.	8.607c.	I&A 3 Requirements	Is the system compliant with the I&A 2 requirements?		
6.107c1.	8.607c1.		Is access to the IS by privileged users who either reside outside of the IS's perimeter or whose communications traverse data links that are outside the IS's perimeter required to use strong authentication (i.e., an I&A technique that is resistant to replay attack)?		

6.107d.	8.607d.	I&A 4 Requirements	If the means of authentication is user-specified passwords, does the ISSM employ (with the approval of the CSA) automated tools to validate that the passwords are sufficiently strong to resist cracking and other attacks intended to discover the user's password?		
6.107e.	8.607e.	I&A 5 Requirements	If users are remotely accessing the IS, Is a strong authentication mechanism required.		
6.108.	8.608.	Resource Control (ResrcCtrl)	Have the ResrcCtrl requirements for each system been determined? (None or ResrcCtrl 1)		
6.108.	8.608.	ResrcCtrl 1	Has a process been developed and tested to ensure the system contains no residual data before being assigned, allocated, or reallocated.		
6.109.	8.609.	Session Controls (SessCtrl)	Have the SessCtrl requirements for each system been determined? (SessCtrl 1 or SessCtrl 2)		
6.109a.	8.609a.	SessCtrl 1 Requirements			
6.109a1.	8.609a1.	User Notification	Are all users notified prior to gaining access to a system that system usage is monitored, recorded, and subject to audit, and that by using the system, he/she has granted consent to such monitoring and recording, and that unauthorized use is prohibited and subject to criminal and civil penalties?		
			Does each initial screen (displayed before the user log on) contain a warning text, provided and approved by the CSA, to the user and that requires positive action by the user to remove the notice from the screen. If it is not possible to provide an "initial screen" warning notice, is an other method of notification developed and approved by the CSA used?		
6.109a2.	8.609a2.	Successive Logon Attempts	Are successive logon attempts controlled as specified in section 8.609a2 ?		
6.109a3.	8.609a3.	System Entry	Does the system grant entry only in accordance with the conditions associated with the authenticated user's profile?		
			If no explicit entry conditions are defined, is the default to prohibit all remote activities, such as remote logons and anonymous file access?		
6.109b.	8.609b.	SessCtrl 2 Requirements	Is the system compliant with the SessCtrl 1 requirements?		
6.109b1.	8.609b1.	Multiple Login Control	If the IS supports multiple logon sessions for each user ID or account, does the IS provide a protected capability to control the number of logon sessions for each user ID, account, or specific port of entry?		
			Does the IS default to a single logon session?		
6.109b2.	8.609b2.	User Inactivity	Does the IS detect an interval of user inactivity, such as no keyboard entries, and disable any future user activity until the user re-establishes the correct identity with a valid authenticator?		
			Is the inactivity time period and restart requirements documented in the SSP?		
6.109b3.	8.609b3.	Logon Notification	Is the user notified upon successful logon of: the date and time of the user's last logon; the location of the user at last logon; and the number of unsuccessful logon attempts using this user ID since the last successful logon?		
			Does this notice require positive action by the user to remove it from the screen?		
6.110.	8.610.	Security Documentation (Doc)			
6.110a.	8.610a.	Doc 1 Requirements			
6.110a1.	8.610a1.	SSP	Does the SSP contain the name, location, and phone number of the responsible system owner, CSA, ISSM, and ISSO?		
			Does the SSP contain a brief narrative description of the system or network mission or purpose and architecture, including subnetworks, communications devices, and protocols?		
			Does the SSP contain the sensitivity or classification levels, and categories of all information on the system and clearance, formal access approval and need-to-know of IS users?		
			Does the SSP contain The confidentiality level of concern and protection level, the integrity level of concern, and the availability level of concern?		
			Does the SSP Identify protection measures and how they are being met?		
			Does the SSP contain a description of any approved variances from protection measures? Is a copy of the approval documentation shall be attached to the SSP?		
			Does the SSP contain a description of the risk assessment of any threats or vulnerabilities unique to the system. If there are no threats or vulnerabilities unique to the facility or system, Is there a statement to that effect included in the SSP? If any vulnerabilities are identified by the assessment of unique threats, are the countermeasures implemented to mitigate the vulnerabilities described?		
			Does the SSP contain a brief description of the system architecture, including a block diagram of the components that show the interconnections between the components and any connections to other systems, and an information flow diagram.		

			If connections to other systems exist, a memorandum of understanding is necessary if the systems are approved by a person other than the CSA responsible for this system. Does the SSP contain a copy of any memorandum of understanding with other agencies?		
			Does the SSP contain a brief description of the security support structure including all controlled interfaces, their interconnection criteria, and security requirements?		
			Does the SSP contain Test plans, procedures, and test reports including risk assessment?		
			Does the SSP contain The test plan for ongoing testing and the frequency of such testing?		
			Does the SSP contain a certification statement that the system complies with the requirements of the protection level and levels of concern for this system? Is the statement signed by the ISSM?		
			Does the SSP contain the documentation for accreditation including the certification package? Did the CSA approve the package and provide accreditation documentation?		
6.111.	8.611.	Separation of Function Requirements (Separation)	If the system is Protection Level 3, are the functions of ISSO and system manager performed by separate people?		
6.112.	8.612.	System Recovery (SR)			
6.112a.	8.612a.	SR 1 Requirements	Are Procedures and IS features implemented to ensure that IS recovery is done in a controlled manner.		
6.113.	8.613.	System Assurance (SysAssur)	Have the SysAssur requirements for each system been determined? (SysAssur1, SysAssur 2 or SysAssur 3)		
6.113a.	8.613a.	SysAssur 1 Requirements			
6.113a1.	8.613a1.	Access to Protection Functions	Is Access to hardware/software/firmware that perform systems or security functions limited to authorized personnel?		
6.113b.	8.613b.	SysAssur 2 Requirements	Is the system compliant with the SysAssur 2 requirements?		
6.113b1.	8.613b1.	Protection Documentation	Are the protections and provisions of the SysAssur documented?		
6.113b2.	8.613b2.	Periodic Validation of SysAssur	Do features and procedures exist to periodically validate the correct operation of the hardware, firmware, and software elements of the SSS and are documented in the SSP?		
6.113c.	8.613c.	SysAssur 3 Requirements	Is the system compliant with the SysAssur 3 requirements?		
6.113c1.	8.613c1.	SSS Isolation	Does the SSS maintain a domain for its own execution that protects it from external interference and tampering (e.g., by reading or modifying its code and data structures)?		
6.114.	8.614.	Security Testing (Test)	Have the test requirements for each system been determined? (Test 1, Test 2 or Test3)		
6.114a.	8.614a.	Test 1 Requirements	Is assurance provided to the CSA that the system operates in accordance with the approved SSP and that the security features, including access controls and configuration management, are implemented and operational?		
6.114b.	8.614b.	Test 2 Requirements	Is the system compliant with the Test 1 requirements?		
6.114b1.	8.614b1.		Is written assurance provided to the CSA that the IS operates in accordance with the approved SSP, and that the security features, including access controls, configuration management and discretionary access controls, are implemented and operational?		
6.114c.	8.614c.	Test 3 Requirements	Is the system compliant with the Test 2 requirements?		
6.114c1.	8.614c1.		Has Certification testing been conducted, using a test plan including the requirements defined in section 8.614c1, including verification that the features and assurances required for the Protection Level are functional?		
6.115.	8.615.	Disaster Recovery Planning	If disaster recovery planning is contractually mandated, Did the ISSM develop a plan that identifies the facility's mission essential applications and information, procedures for the backup of all essential information and software on a regular basis, and testing procedures?		
Section 7. Interconnected Systems					
7.100.	8.700.	Interconnected Systems Management			
7.100a.	8.700a.		For two or more connected networks, has the CSA reviewed the security attributes of each network to determine whether the combination of data and/or the combination of users on the connected network requires a higher protection level?		
7.100c.	8.700c.		Have all interconnected networks been accredited as a single unit?		
7.100d.	8.700d.		If systems that process information at differing classification levels or with different compartmentalization are interconnected, have they been interconnected in a manner that meets the requirements defined in section 8.700d1 – 8.700d3?		
7.100e.	8.700e.		If an IS is connected to another system that does not meet either 8.700d2 or 8.700d3, does the system utilize a Controlled Interface (CI) that meets the requirements defined in section 8.700e1 – 8.700e3?		

7.101.	8.701.	Controlled Interface Functions			
7.102.	8.702.	Controlled Interface Requirements			
7.102a.	8.702a.	Adjudicated Differences	Does the CI monitor and enforce the protection requirements of the network and adjudicate the differences in security policies?		
7.102b.	8.702b.	Routing Decisions	Does the CI base its routing decisions on information that is supplied or alterable only by the SSS?		
7.102c.	8.702c.	Restrictive Protection Requirements	Does the CI support the protection requirements of the most restrictive of the attached networks or IS?		
7.102d.	8.702d.	User Code	Is user code prohibited from running on the CI?		
7.102e.	8.702e.	Fail-Secure	Has The CI been implemented such that all possible failures shall result in no loss of confidentiality or unacceptable exposure to loss of integrity or availability?		
7.102f.	8.702f.	Communication Limits	Does the CI ensure that communication policies and connections that are not explicitly permitted are prohibited?		
7.102g.	8.702g.	Only Privileged Users	Do only privileged users, such as systems admins, have access to the CI?		
7.103.	8.703.	Assurances for CI's	Has each CI been tested and evaluated to ensure that the CI, as implemented, can provide the separation required for the system's protection level?		

Upcoming SANS Training
Click Here for a full list of all Upcoming SANS Events by Location

SANS Secure Caribbean 2026	**Kingston, JM**	**Feb 16, 2026 - Feb 21, 2026**	**Live Event**
SANS Surge 2026	**La Jolla, CAUS**	**Feb 23, 2026 - Feb 28, 2026**	**Live Event**
SANS Dublin February 2026	**Dublin, IE**	**Feb 23, 2026 - Feb 28, 2026**	**Live Event**
SANS Secure Japan 2026	**Tokyo, JP**	**Mar 02, 2026 - Mar 14, 2026**	**Live Event**
SANS London March 2026	**London, GB**	**Mar 02, 2026 - Mar 07, 2026**	**Live Event**
SANS DC Metro March 2026	**Arlington, VAUS**	**Mar 02, 2026 - Mar 07, 2026**	**Live Event**
SANS Secure Singapore 2026	**Singapore, SG**	**Mar 02, 2026 - Mar 14, 2026**	**Live Event**
SANS Paris March 2026	**Paris, FR**	**Mar 09, 2026 - Mar 14, 2026**	**Live Event**
SANS Open-Source Intelligence Summit 2026	**Arlington, VAUS**	**Mar 16, 2026 - Mar 22, 2026**	**Live Event**
SANS Thailand March 2026	**Bangkok, TH**	**Mar 16, 2026 - Mar 21, 2026**	**Live Event**
SANS Amsterdam March 2026	**Amsterdam, NL**	**Mar 16, 2026 - Mar 21, 2026**	**Live Event**
SANS Melbourne March 2026	**Melbourne, VIC, AU**	**Mar 16, 2026 - Mar 21, 2026**	**Live Event**
SANS Cybersecurity Leadership Summit & Training 2026	**Arlington, VAUS**	**Mar 17, 2026 - Mar 22, 2026**	**Live Event**
SANS 2026	**Orlando, FLUS**	**Mar 29, 2026 - Apr 03, 2026**	**Live Event**
SANS London April 2026	**London, GB**	**Apr 13, 2026 - Apr 18, 2026**	**Live Event**
SANS Rome April 2026	**Rome, IT**	**Apr 13, 2026 - Apr 18, 2026**	**Live Event**
SANS Secure Australia 2026	**Canberra, ACT, AU**	**Apr 13, 2026 - Apr 18, 2026**	**Live Event**
SANS Rocky Mountain 2026	**Denver, COUS**	**Apr 20, 2026 - Apr 25, 2026**	**Live Event**
SANS SEC535 at AI Cybersecurity Summit & Training 2026	**Arlington, VAUS**	**Apr 20, 2026 - Apr 27, 2026**	**Live Event**
SANS AI Cybersecurity Summit & Training 2026	**Arlington, VAUS**	**Apr 20, 2026 - Apr 27, 2026**	**Live Event**
SANS Amsterdam April 2026	**Amsterdam, NL**	**Apr 20, 2026 - Apr 25, 2026**	**Live Event**
SANS ICS Munich 2026	**Munich, DE**	**Apr 20, 2026 - Apr 25, 2026**	**Live Event**
SANS Doha April 2026	**Doha, QA**	**Apr 26, 2026 - Apr 30, 2026**	**Live Event**
SANS Cyber Incident Management 2026	**OnlineAU**	**Feb 09, 2026 - Feb 13, 2026**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**