BASELINE SECURITY REQUIREMEMTS (U) {tc "B ASSUMPTIONS MADE DURING THIS RISK ASSESSMENT (U) "}

	Administrative Security (AS) Requirements				
Requirement	Reference	Met	Partially Met	Not Met	N/A
1. All federal government departments and agencies shall establish and implement programs that mandate the certification and accreditation (C&A) of national security systems under their operational control. These C&A programs shall ensure that information processed, stored, or transmitted by national security systems is adequately protected with respect to requirements for confidentiality, integrity, and availability.	NSTISSP No. 6, I.1				
2. When AISs managed by different DAAs are interfaced or networked, a memorandum of agreement (MOA) is required that addresses the accreditation requirements for each AIS involved.	DoDD 5200.28, par D.8; CJCSI 6731.01, 18 Nov 96, Encl. B.1.e				
3. A DAA shall be designated as responsible for the overall security of the AIS.	DoDD 5200.28, par D.9;				
4. The accreditation of an AIS shall be supported by a certification plan, a risk analysis, of the AIS in its operational environment, an evaluation of the security safeguards, and a certification report.	DoDD 5200.28, par D.9.d;				
5. A program for conducting periodic reviews of the adequacy of the safeguards for operational, accredited AISs shall be established.	DoDD 5200.28, par D.9.e				
6. The Computer Security Manager (CSM) will ensure that a System Security Plan (SSP) is prepared for each AIS and network under their purview.	NSA/CSS Manual 130-1, Chap. I.6.c				
7. The SSP will be used by the accrediting authority as the basis for an accreditation decision.	NSA/CSS Manual 130-1, Chap. II.15				
8. The SSP is to be reviewed periodically (annually, at a minimum) and revised whenever hardware, software, configuration, or usage changes that have an impact on security are made.	NSA/CSS Manual 130-1, Chap. III.15.e				
9. A program for developing and testing contingency plans shall be established.	DoDD 5200.28, par D.9.f				

	Administrative Security (AS) Requirements				
Requirement	Reference	Met	Partially Met	Not Met	N/A
10. Each file or data collection in the AIS shall have an identifiable source throughout its life cycle. Its accessibility, maintenance, movement, and disposition shall be governed by security clearance, formal access approval, and need-to-know.	DoDD 5200.28, Encl. 3, A.7				
11. Contingency plans shall be developed and tested in accordance with OMB A-130 to ensure that AIS security controls function reliably and, if not, that adequate backup functions are in place to ensure that security functions are maintained continuously during interrupted service. If data is modified or destroyed, procedures must be in place to recover.	DoDD 5200.28, Encl. 3, A.9;				
12. Each AIS shall be accredited to operate in accordance with a DAA-approved set of security safeguards.	DoDD 5200.28, Encl. 3, A.10;				
13. There should be in place a risk management program to determine how much protection is required, how much exists, and the most economical way of providing the needed protection.	DoDD 5200.28, Encl. 3, A.11				
14. A risk management program will be implemented to determine how much protection is required, how much exists, and the most economical way of providing the needed protection.					
15. Federal departments and agencies are required to develop and implement information systems security (INFOSEC) education, training and awareness programs for national security systems.	NSTISSD No. 500, I.1				
16. Every INFOSEC education, training and awareness program will contain three types of activities: initial orientation, more advanced education and training commensurate with duties and responsibilities, and reinforcement activities.	NSTISSD No. 500, VI.8				
17. Federal departments and agencies are required to implement training programs for information systems security (INFOSEC) professionals as defined in NSTISSI 4011. An INFOSEC professional is an individual who is responsible for the security oversight or management of national security systems during each phase of the life cycle.	NSTISSD No. 501, I.1				
18. There shall be in place a security training and awareness program with training for the security needs of all persons accessing the AIS.	DoDD 5200.28, Encl. 3, A.3				

	Administrative Security (AS) Requirements				
Requirement	Reference	Met	Partially Met	Not Met	N/A
19. Heads of DoD Components shall establish security education programs for their personnel which stresses the objectives of improving the protection of information.	DoDR 5200.1, Chap. X, 10-100				
20. The security education program shall include all personnel authorized or expected to be authorized access to classified information.	DoDR 5200.1, Chap. X, 10-101				
21. Security Education Programs shall be established to provide, at a minimum, annual security training for personnel having continued access to classified information.	DoDR 5200.1, Chap. X, 10-102				
22. Upon termination of employment or contemplated absence from duty or employment for 60 days or more, DoD personnel shall be given a termination briefing, return all classified material, and execute a Security Termination Statement.	DoDR 5200.1, Chap. X, 10-104.a				
23. Plans shall be developed for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action. These plans shall establish detailed procedures and responsibilities for the protection of classified material to ensure that the material does not come into the possession of unauthorized persons.	DoDR 5200.1, Chap. V, Sec. 2, 5-203.a				
24. The Emergency Plan shall require that classified material holdings be assigned a priority for emergency evacuation or destruction.	DoDR 5200.1, Chap. V, Sec. 2, 5-203.e				
25. No person may have access to classified information unless that person has been determined to be trustworthy and unless access is necessary for the performance of official duties.	DoDR 5200.1, Chap. VII, Sec. 1, 7-100				
26. Commanding officer and ADP security staff are responsible for implementing service ADP security policies					
27. Each unit will follow the Service Department ADP Security Program.					
28. Establish a program to assess local compliance to DOD and service standards, policies, & regulations					
29. ADP security countermeasure implementation will be based on service security policies and procedures or higher authority, and a comprehensive risk assessment.					
30. Local security directives established and disseminated					

	Administrative Security (AS) Requirements				
Requirement	Reference	Met	Partially Met	Not Met	N/A
31. Each activity must develop a contingency plan.					
32. Contingency plans contain necessary security reinforcements					
33. An activity ADP Security Plan is developed, with a copy submitted to headquarters					
34. A single activity Information System Security Officer (ISSO) is appointed, in writing.					
35. All networks under activity cognizance have a DAA, a sponsor, and a Network Security Officer (NSO).					
36. The sponsor and NSO are appointed in writing.					
37. The ISSO insures that an effective Risk Management program is implemented.					
38. Terminal Area Security Officer (TASO) is appointed for each remote terminal or terminal cluster.					
39. Security Education Program is developed and established at each activity					
40. All personnel receive security indoctrination training within 90 days of reporting for duty or employment					
41. All personnel receive annual security refresher training					
42. Each employee is indoctrinated in local protection procedures during initial and annual security education. LAN users must be trained in data protection and password selection procedures.					

	Communications Security (CO) Requirements				
Requirement	Reference	Met	Partially Met	Not Met	N/A
1. Only NSA endorsed products, techniques, and protected services shall be used.					
2. [T]he end-user system is responsible for detecting and recovering information that may have been damaged or altered by the communications process through the transport service.					
3. Classified or sensitive information in clear text is not allowed to pass through the multiplexers layer or over individual circuits					
4. All IP routers, X.25 packet switches, multiplexers and related components shall be protected at the SECRET level.					
5. SIPRNET and local network users must protect all exposed trunks between IP routers and X.25 packet switches, and exposed subscriber access links to routers or switches with KG-type devices.					
6. ADP communication links and lines will be secured in a manner appropriate for the level of data transmitted.					

	Computer Security (CS) Requirements				
Requirement	Reference	Met	Partially Met	Not Met	N/A
1. All AISs that process or handle classified or sensitive-but-unclassified information and that require at least controlled access protection (i.e., class C2 security) shal implement required security features by 1992.	DoDD 5200.28, par D.6.a				
2. Operate at least at a C2 level of trust.					
3. There shall be safeguards in place to ensure each person having access will be held accountable for their actions. There shall be an audit trail providing a documented history of system use.					
4. Any changes to the system or associated environments that affect the accredited safeguards or result in changes to the prescribed security requirements shall require recertification and reaccreditation					
5. Each ISSO shall ensure that audit trails are reviewed periodically.	DoDD 5200.28, par E.10.d				
6. There shall be an audit trail providing a documented history of AIS use of sufficient detail to reconstruct events in determining the cause of magnitude of compromise should a security violation or malfunction occur. The audit trail shall document: a. the identity of each person and device having access to the AIS. b. the time of the access. c. user activity sufficient to ensure user actions are controlled and open to scrutiny. d. activities that might modify, bypass, or negate safeguards controlled by the AIS. e. security relevant actions associated with periods processing or the changing of security levels or categories of information.	DoDD 5200.28, Encl. 3.A.1;				
5. There shall be an access control policy for each AIS.	DoDD 5200.28, Encl. 3.A.2;				
6. The identify of each user authorized access to the AIS shall be established positively before authorizing access.	DoDD 5200.28, Encl. 3.A.2;				
7. The AIS shall function so that each user has access to all of the information to which the user is entitled (by virtue of clearance, formal access approval), but no more.	DoDD 5200.28, Encl. 3.A.6;				

Requirement	Computer Security (CS) Requirements				
	Reference	Met	Partially Met	Not Met	N/A
8. There shall be safeguards to detect and minimize inadvertent modification or destruction of data, and detect and prevent malicious destruction or modification of data.	DoDD 5200.28, Encl. 3.A.8;				
9. SIRNET and the local network will effect means necessary to prevent unauthorized information disclosure/ dissemination					
10. Users' identities shall be authenticated before the users are granted further access to data, services, and other controlled resources. Users shall be uniquely identified in the system.					
11. ADP activity or network is externally protected against unauthorized access					
12. All ADP system or network elements function in a cohesive, identifiable, predictable, and reliable manner					
13. Each file or collection of data in the ADP system or network will have an identifiable origin and use.					
14. Each user will have access to all of the data entitled, but no more. (Concept of Least Privilege).					
15. The NSO will ensure security countermeasures and requirements for networks are met.					
16. A risk assessment will be conducted when developing a new ADP system or network and for each existing ADP activity or network.					
17. Risk assessments will be conducted at least every five years or whenever, in the judgment of the commanding officer, a system configuration or facility change impacts the current ADP security posture.					
18. The security of peripheral or remote devices is prescribed by the activity responsible of the security of the host ADP system or network.					
19. Security measures for peripherals and remotes used by differing activities will be agreed to, formally documented, and implemented before the equipment is connected to the host.					
20. Navy ADP activities and systems will only operate if properly accredited.					
21. All activities will insure that any software development or modification will take into account all ADP safeguards, including access control and auditing.					

	Computer Security (CS) Requirements				
Requirement	Reference	Met	Partially Met	Not Met	N/A
22. Service activities are protected by a cost-effective computer security program for environmental and physical security; and an adequate contingency plan.					
23. Activities must perform an appropriate Security Test and Evaluation for the level of information processed.					

	Information Security (IS) Requirements				
Requirement	Reference	Met	Partially Met	Not Met	N/A
1. Classified and sensitive unclassified information shall be safeguarded at all times while in AISs. Safeguards shall be applied so that such information is accessed only by authorized persons, is used only for its intended purpose, retains its content integrity, and is marked properly as required.	DoDD 5200.28, D.1				
2. The safeguarding of information and AIS resources (against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or release to unauthorized persons) shall be accomplished through the continuous employment of safeguards consisting of administrative, procedural, physical and /or environmental, personnel, communications security, emanations security and computer security (i.e., hardware, firmware, and software), as required. The mix of safeguards selected shall achieve the requisite level of security or protection.	DoDD 5200.28, D.3;				
3. The mix of safeguards selected for an AIS that processes classified or sensitive unclassified information shall ensure the AIS meets the minimum requirements... through automated and manual means in a cost-effective and integrated manner.	DoDD 5200.28, D.4;				
4. Classified and sensitive unclassified output shall be marked to accurately reflect the sensitivity of the information.	DoDD 5200.28, Encl. 3, 5				
5. Assure that information that warrants protection against unauthorized disclosure is properly classified and safeguarded.	DoDD 5200.1, C				
6. Ensure that Information requiring protection in the interest of national security is properly classified and safeguarded.	DoDD 5200.1, D.1				
7. Ensure that overclassification and unnecessary classification are avoided.	DoDD 5200.1, D.2				
8. Ensure that information is classified as long as required by national security considerations.	DoDD 5200.1, D.3				
9. Output shall be marked to accurately reflect the sensitivity of the information.					
10. Classified documents removed from storage shall be kept under constant surveillance and face down or covered when not in use.	DoDR 5200.1, Chap. V, Sec. 2, 5-201.a				

	Information Security (IS) Requirements				
Requirement	Reference	Met	Partially Met	Not Met	N/A
11. Preliminary drafts, carbon sheets, plates, stencils, stenographic notes, worksheets, typewriter ribbons, and other items containing classified information shall be either destroyed immediately after they have served their purpose; or shall be given the same classification and secure handling as the classified information they contain.	DoDR 5200.1, Chap. V, Sec. 2, 5-201.b				
12. Heads of activities shall establish a system of security checks at the close of each working day to ensure that: all classified material is stored in the proper manner; burn bags are properly stored or destroyed; and, wastebaskets do not contain classified material.	DoDR 5200.1, Chap. V, Sec. 2, 5-202.a., b., c				
13. All media (and containers) shall be marked and protected at the SECRET..., system high level until the media are declassified (e.g., degaussed or overwritten) using a DoD-approved methodology.	NCSC-TG-025				
14. ADP storage media or output will be safeguarded as appropriate for the level of data assigned and will bear eye-readable security markings					
15. File or data backup, use, accessibility, maintenance, movement, and disposition is governed on level and type of data, need-to-know, and other sensitive measures.					

	Personnel Security (PE) Requirements				
Requirement	Reference	Met	Partially Met	Not Met	N/A
1. Only authorized personnel shall have access to information systems.	OMB A-130, 7, 8.b.12				
2. Personnel security policies and procedures shall be established and managed to assure an adequate level of security for Federal automated information systems. Policies shall include requirements for screening all individuals participating in the design, development, operation, or maintenance of sensitive applications as well as those having access to sensitive data.	OMB A-130, III-4, 3.b				
3. ADP users will be identified by appropriate administrative or hardware and software measures.					
4. A Personnel Security Investigation shall be conducted in connection with: the entry of a person in the Armed Forces of the United States; the granting of clearance for access to classified information; or, the assignment of an individual to such other duties designated in accordance with DOD 5200.2-R which require a determination of trustworthiness.	DoDD 5200.2, C., 2., (b)(c)(d)				
5. Each ISSO shall ensure that users have the required personnel security clearances, authorization and need-to-know, have been indoctrinated, and are familiar with internal security practices before access to the AIS.	DoDD 5200.28, E., 10., c				
6. All users will possess a final US SECRET clearance. Contractor personnel must possess the appropriate clearance levels…[and]…must be controlled and monitored by US government employees.					
7. Subjects shall have access to only those objects and/or services for which they have clearance, authorization, need-to-know, and need to use.					

	Physical Security (PH) Requirements				
Requirement	Reference	Met	Partially Met	Not Met	N/A
1. Hardware, software, and documentation, and all it's data shall be protected to prevent unauthorized disclosure, destruction, or modification.					
2. Due to the critical nature of servers, strongly recommend that all servers be inaccessible except through controlled means.					
3. Physical security survey conducted annually or upon change of security officer.					
4. Risk and threat analysis must be completed to determine degree of physical requirements prior to employing security measures					
5. Determine restricted area level for computer facility					
6. Access to the AIS facility shall be controlled by physical security measures and/or administrative procedures.					
7. Establish a strict key and lock control program supervised by the security officer					
8. Local security force established and composed of proper elements					
9. Identification and control procedures are documented and followed					
10. Badges issued followed established standards.					
11. Physical barriers established around restricted areas					
12. Exterior doors, windows, skylights, and other access points in the restricted area offer proper asset protection					
13. Intrusion Detection System used is the proscribed system for all Navy activities and installations					