

Chapter 8 Information System Security

Industrial Security Letter

This is a special section of the Industrial Security Letter (ISL) dedicated to interpreting and clarifying the May 1, 2000 Chapter 8. The document compliments the Director of Central Intelligence Directive (DCID 6/3) "Protecting Sensitive Compartmented Information within Information Systems." The ISL provides industry with the DoD perspective on protecting classified information while maintaining uniformity and consistency with established Department of Defense (DoD) policies. There are references to additional technical data or information being present on the DSS website (www.dss.mil) in the responses to a number of questions in this ISL. That additional information will be posted on March 9, 2001.

1. Question: What is the implementation date of the May 1, 2000 Chapter 8?

Answer: The implementation date is currently scheduled for May 1, 2001. All Information Systems (IS) submitted for accreditation or reaccreditation after this date shall implement the requirements of the new chapter.

2. Question: Will Automated Information Systems (AIS) accredited under Chapter 8 of the 1995 NISPOM retain their accreditation?

Answer: Yes. Currently accredited AISs retain their accreditation for three years from the date of this ISL. Within the three-year period, contractors shall implement the requirements of the new chapter and request reaccreditation for all IS accredited against the 1995 Chapter 8 requirements.

3. Question: When will training become available for the new Chapter 8?

Answer: The DSS Academy has prepared a presentation describing the changes between the January 1995 and May 2000 version of the NISPOM chapter 8. This presentation is annotated so that contractor personnel can provide training within their own organizations. The presentation can be viewed at, or downloaded from, www.dss.mil/infoas/index.htm. For a more in-depth class of Information Security that includes the new Chapter 8, the DSS Academy has updated the IS Security Procedures for Industry Course. The course will be available beginning February 2001. The Central Intelligence Agency has also developed training for DCID 6/3. DSS will post information on that and any additional available training.

Section 1. Responsibilities and Duties

8-100. General.

a. Information systems (IS) that are used to capture, create, store, process or distribute classified information must be properly managed to protect against unauthorized disclosure of classified information, loss of data integrity, and to ensure the availability of the data and system.

4. Question: Paragraph 8-100a states that the IS must be properly managed to protect against loss of data integrity and to ensure the availability of the data and system. Paragraph 8-400 states that integrity and availability are not covered by the National Industrial Security Program (NISP) and will be determined in additional guidance or requirements issued by the GCA. Is paragraph 8-100a addressing “general security concerns” and not National Industrial Security Program Operating Manual (NISPOM) requirements?

Answer: Yes. While important, data integrity and system availability are not covered by the NISP (paragraph 8-400) and will be determined in additional guidance or requirements issued by the GCA.

b. Protection requires a balanced approach including IS security features to include but not limited to, administrative, operational, physical, computer, communications, and personnel controls. Protective measures commensurate with the classification of the information, the threat, and the operational requirements associated with the environment of the IS are required.

c. The requirements outlined in the following sections apply to all information systems processing classified information. Additional requirements for high-risk systems and data are covered in the NISPOM Supplement

5. Question: Paragraph 8-100c states that “additional requirements for high-risk systems and data are covered in the NISPOM supplement. What is the definition of “high-risk systems and data?”

Answer: “High-risk” refers to the vulnerability and the nature of the technology, process, or data relative to other classified systems and data. For the purpose of this ISL, a high-risk system is one that requires protection above the baseline of chapter 8 (i.e., multilevel) where high-risk data would be non-collateral data. NOTE: Director of Central Intelligence

Directive (DCID) 6/3 is being coordinated as Chapter 8 of the NISPOM Supplement (Automated Information System Security) the requirements of Protection Level 4 of the should be used for “high risk” systems and data. These requirements can be found at <http://www.dss.mil/infoas/index.htm>.

8-101. Responsibilities.

a. The CSA shall establish a line of authority for training, oversight, program review, certification, and accreditation of IS used by contractors for the processing of classified information. The CSA will conduct a risk management evaluation based on the contractor's facility, the classification, and sensitivity of the information processed. The evaluation must ensure that a balanced, cost-effective application of security disciplines and technologies is developed and maintained.

6. Question: Paragraph 8-101a. Will a copy of the risk management evaluation be given to the contractor?

Answer: In many facilities the level of complexity of the contractor's IS program or the sensitivity of their classified projects does not warrant a “formal” risk management evaluation and report. When one is required, the Facility Security Officer (FSO) and Information System Security Manager (ISSM) will be provided a copy.

b. Contractor management will publish and promulgate an IS Security Policy addressing the classified processing environment. Additionally, an IS Security Manager (ISSM) will be appointed with oversight responsibility for the development, implementation, and evaluation of the facility's IS security program. Contractor management will assure that the ISSM is trained to a level commensurate with the complexity of the facility's IS.

7. Question: Paragraph 8-101b. Must the ISSM be an employee of the contractor and can an ISSM manage the IS security program for more than one contractor?

Answer: The ISSM must be an employee. However, in a multiple facility organization, contractor management can appoint an employee as the ISSM with oversight responsibility for multiple facilities. The travel distance between these facilities can not be greater than one hour, the complexity of any one, or all,

facilities is such that only one ISSM is required, the ISSM is trained to a level commensurate with the overall complexity of all facilities, and that each facility has an appointed Information System Security Officer(s) (ISSO) that has been assigned all responsibilities identified in paragraph 8-104.

8. Question: Paragraph 8-101b. What training should the ISSM receive and how will management assure the requirement is met?

Answer: Contractor management should take maximum advantage of the DSS IS for Industry Course to train the ISSM. The course is offered in various locations around the country approximately 12 times a year. The ISSM can arrange to take any nationally known or government agency information system security training which includes testing or certification.

8-102. Designated Accrediting/Approving Authority.

The CSA is the Designated Accrediting/Approving Authority (DAA) responsible for accrediting information systems used to process classified information in industry

9. Question: Paragraph 8-102 states the CSA is the Designated Accrediting/Approving Authority (DAA) responsible for accrediting IS used to process classified information. Since this is the first time the NISPOM has identified this position and responsibility, would you elaborate?

Answer: Within the NISP, the Designated Approving Authority (DAA) is the government official with the authority to formally accredit operation of the contractor's IS. Officially the DAA declares the environment the contractor has identified in their System Security Plan (SSP) will effectively protect classified information from unauthorized disclosure. The DAA provides a level of assurance that the IS will provide the protection required. As a general rule, the DSS Industrial Security Representative (IS Rep) assigned responsibility for the contractor's facility is the DAA for standalone IS. The DAA for all other IS will be the DSS regional IS manager.

8-103. IS Security Manager (ISSM). The ISSM:

a. Ensures the development, documentation, and presentation of IS security education, awareness, and training activities for facility management, IS personnel, users, and others, as appropriate.

b. Establishes, documents, implements, and monitors the IS Security Program and related

procedures for the facility and ensures facility compliance with requirements for IS.

c. Identifies and documents unique local threats/vulnerabilities to IS.

d. Coordinates the facility IS Security Program with other facility security programs.

e. Ensures that periodic self-inspections of the facility's IS Program are conducted as part of the overall facility self-inspection program and that corrective action is taken for all identified findings and vulnerabilities. Self-inspections are to ensure that the IS is operating as accredited and that accreditation conditions have not changed.

f. Ensures the development of facility procedures to:

(1) Govern marking, handling, controlling, removing, transporting, sanitizing, reusing, and destroying media and equipment containing classified information.

(2) Properly implement vendor supplied authentication (password, account names) features or security-relevant features.

(3) Report IS security incidents to the CSA. Ensure proper protection or corrective measures have been taken when an incident/vulnerability has been discovered.

(4) Require that each IS user sign an acknowledgment of responsibility for the security of the IS.

(5) Implement security features for the detection of malicious code, viruses, and intruders (hackers), as appropriate.

10. Question: Paragraph 8-103f(5). When is it "appropriate" to implement security features for the detection of malicious code and viruses?

Answer: As a general rule, malicious code and viruses are a concern to all IS and must be addressed by the ISSM and identified in the SSP. However, there are special categories of IS (Section 5) that are immune to these threats and do not require detection procedures.

g. Certifies to the CSA, in writing, that each System Security Plan (SSP) has been implemented; that

the specified security controls are in place and properly tested; and that the IS is functioning as described in the SSP.

h. Ensures notification of the CSA when an IS no longer processes classified information, or when changes occur that might affect accreditation.

i. Ensures that personnel are trained on the IS's prescribed security restrictions and safeguards before they are initially allowed to access a system.

j. Develops and implements general and remote maintenance procedures based on requirements provided by the CSA.

8-104. Information System Security Officer(s) (ISSO). ISSOs may be appointed by the ISSM in facilities with multiple accredited IS. The ISSM will determine the responsibilities to be assigned to the ISSO that may include the following:

a. Ensure the implementation of security measures, in accordance with facility procedures.

b. Identify and document any unique threats.

c. If so directed by the GCA and/or if an identified unique local threat exists, perform a risk assessment to determine if additional countermeasures beyond those identified in this chapter are required.

d. Develop and implement a certification test as required by the ISSM/CSA.

11. Question: Paragraph 8-104d requires an IS certification test be developed and implemented. What is a certification test and when would it be required?

Answer: A certification test outlines the inspection and test procedures used to demonstrate compliance with the security requirements associated with the Protection Level assigned to the IS. The certification test is administered during the certification process and is discussed later (paragraph 8-614) in this ISL.

e. Prepare, maintain, and implement an SSP that accurately reflects the installation and security provisions.

f. Notify the CSA (through the ISSM) when an IS no longer processes classified information, or when changes occur that might affect accreditation.

g. Ensure:

(1) That each IS is covered by the facility Configuration Management Program, as applicable.

12. Question: Paragraph 8-104g(1). When is it "applicable" for each IS to be covered by the facility Configuration Management (CM) program?

Answer: The CM program varies with the complexity and size of the IS. Some IS require a formal configuration management board that makes change control decisions where others might require only the coordination and approval of the ISSO. Every SSP must have a CM section describing how the accredited IS protection features are implemented and maintained.

(2) That the sensitivity level of the information is determined prior to use on the IS and that the proper security measures are implemented to protect this information.

(3) That unauthorized personnel are not granted use of, or access to, an IS.

(4) That system recovery processes are monitored to ensure that security features and procedures are properly restored.

h. Document any special security requirement identified by the GCA and the protection measures implemented to fulfill these requirements for the information contained in the IS.

i. Implement facility procedures:

(1) To govern marking, handling, controlling, removing, transporting, sanitizing, reusing, and destroying media and equipment containing classified information.

(2) To ensure that vendor-supplied authentication (password, account names) features or security-relevant features are properly implemented.

(3) For the reporting of IS security incidents and initiating, with the approval of the ISSM, protective or corrective measures when a security incident or vulnerability is discovered.

(4) Requiring that each IS user sign an acknowledgment of responsibility for the security of IS and classified information.

(5) For implementing and maintaining security-related software for the detection of malicious

code, viruses, and intruders (hackers), as appropriate.

j. Conduct ongoing security reviews and tests of the IS to periodically verify that security features and operating controls are functional and effective.

k. Evaluate proposed changes or additions to the IS, and advise the ISSM of their security relevance.

l. Ensure that all active user IDs are revalidated at least annually.

13. Question: Paragraphs 8-104l and 8-303g require that active user IDs be revalidated at least annually. Is there a requirement to revalidate users of standalone workstations or small local area networks (paragraph 8-303c) since user IDs are not required?

Answer: Yes. The intent of this paragraph is to verify that all users have a continued need to access the accredited IS. Since user IDs are not always required (paragraph 8-303c), access lists can be used. If used for revalidation, access lists shall be retained as an audit 1 requirement.

8-105. Users of IS. Users of IS are either privileged or general users.

a. Privileged users have access to IS control, monitoring or administration functions. Examples include:

(1) Users having "superuser," "root," or equivalent access to a system (e.g., system administrators, computer operators, ISSOs); users with near or complete control of an IS or who set up and administer user accounts and authenticators.

(2) Users having access to change control parameters (routing tables, path priorities, addresses, etc.) on routers, multiplexers, and other key IS equipment.

(3) Users who have been given the authority to control and change other users' access to data or program files (e.g., applications software administrators, administrators of specialty file systems, database managers).

(4) Users who have been given special access for troubleshooting or monitoring an IS' security functions (e.g., those using analyzers, management tools).

b. General users are individuals who can input

information to or modify information on an IS or who can receive information from an IS without a reliable human review.

c. All users shall:

(1) Comply with the IS Security Program requirements.

(2) Be aware of and knowledgeable about their responsibilities in regard to IS security.

(3) Be accountable for their actions on an IS.

(4) Ensure that any authentication mechanisms (including passwords) issued for the control of their access to an IS are not shared and are protected at the highest classification level and most restrictive classification category of information to which they permit access.

(5) Acknowledge, in writing, their responsibilities for the protection of the IS and classified information.

Section 2. Certification and Accreditation

14. Issue: Section 2 identifies the requirements associated with the certification and accreditation process. Certification is the comprehensive analysis to validate both technical and nontechnical security features and safeguards of the IS and is conducted in support of the accreditation process. In December 1997, the Office of the Secretary of Defense signed a directive that implements a standard infrastructure-centric approach to the certification and accreditation process. The DoD Information Technology Security Certification and Accreditation Process (DITSCAP) implements policy, assigns responsibility and prescribes procedures to all DoD Agencies, their contractors and agents. The DITSCAP can only be imposed via a requirements clause in the contract. Since the DITSCAP is a process that focuses mainly on government certifiers and accreditors, the DITSCAP has little impact on the contractor other than requiring a System Security Authorization Agreement (SSAA) that is prepared and updated during the lifecycle of the IS. Where the DITSCAP is imposed by contract or otherwise adopted by a contractor under the terms of its GCAs security requirements, the contractor has the option of maintaining the SSAA and the System Security Plan (SSP) separately or of using the DSS modified SSAA that combines both into one document (<http://www.dss.mil/infoas/index.htm>).

8-200. Overview. The certification and accreditation (C&A) process is an integral part of the life cycle of an IS. The identification of protection measures occurs during system design or development. The formal C&A occurs after the protection measures have been implemented and any required IS protection documentation has been approved. Certification validates that the protection measures described in the SSP have been implemented on the system and that the protection measures are functioning properly. Accreditation is the approval by the CSA for the system to process classified information.

8-201. Certification Process. Certification is the comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made as part of and in support of the accreditation process, to establish the extent to which a particular design and implementation meet a specified set of security requirements. The certification process subjects the system to appropriate verification that protection measures have been correctly implemented. The ISSM shall review and certify to the CSA that all systems have the appropriate protection measures in place and validate that they provide the protection intended. The CSA may conduct an on site assessment to validate the ISSM's review and certification of the IS.

15. Question: Paragraph 8-201 introduces a new requirement of the ISSM certifying that their ISs have undergone a comprehensive evaluation of all technical and non-technical security features and safeguards. Is this all that is required for certification?

Answer: No. DSS is assigned the responsibility of certification (paragraph 8-101). DSS has implemented an internal process of certifying contractor's IS that their IS Reqs and ISSPs follow. Part of this process includes the ISSM certifying that their ISs have undergone a comprehensive evaluation.

8-202. Accreditation. The accreditation of an IS is the official management decision to permit operation of an IS in a specified environment at an acceptable level of risk, based on the implementation of a CSA approved set of technical, managerial and procedural safeguards. All IS certifications shall be reviewed and IS accredited to operate by the CSA.

a. Interim Approval to Operate. The CSA may grant interim approval (temporary authority) to operate an IS. Interim approval to operate may be granted for up to 180 days with an option for the CSA to extend the interim approval for an additional 180 days. CSA-approved protection measures shall be in place and functioning during the period of interim approval.

16. Question: Paragraph 8-202a permits a contractor's IS to be granted interim approval to operate for 180 days with an optional extension of a second 180 days. Under what conditions would an IS require an interim approval of up to 360 days?

Answer: Interim approvals that last up to 360 days should be rare. Normally, interim approvals are granted by the DAA so the contractor can begin processing classified information while the DAA is reviewing the contractor's IS during the accreditation process. Interim approvals must be in writing and must identify what protection measures are required.

b. Reaccreditation. IS shall be reaccredited whenever security relevant changes are made to the accredited IS. Proposed modifications to an IS shall be reviewed by the ISSM to determine if the proposed modifications will impact the protections on the system. If the protection aspects of the system's environment change, if the applicable IS protection requirements change, or if the protection mechanisms implemented for the system change, the system shall be reaccredited.

During the reaccreditation cycle, the CSA may grant an interim approval to operate the system.

c. Review of Security-Relevant Changes. All modifications to security-relevant resources (including software, firmware, hardware, or interfaces and interconnections to networks) shall be reviewed and approved in accordance with procedures prior to implementation. All security-relevant changes shall be subject to the provisions of the system configuration management program. The ISSM shall notify the CSA of requests for changes to the resources that deviate from the requirements of the approved SSP. The CSA shall determine if system reaccreditation is required.

17. Question: Paragraph 8-202c. Which procedures should the contractor follow when reviewing changes to security-relevant resources?

Answer: The contractor's configuration management (CM) program will address the review and approval process of security-relevant resources and changes. Additionally, the CM program will identify that DSS must be notified prior to the changes being implemented so a reaccreditation decision can be made.

d. Re-evaluation of an Accreditation. Each IS shall be re-evaluated for reaccreditation every 3 years. Such review involves a determination by the CSA, with input from the ISSM that the conditions under which the original accreditation was granted still apply. If the accreditation remains valid, the accreditation originally furnished by the CSA need only be annotated that the re-evaluation was conducted and the date of the re-evaluation.

18. Question: Paragraph 8-202d. Who is responsible for re-evaluating the IS, tracking the 3 year suspense, and what notification to DSS is required?

Answer: It is the ISSM's responsibility to re-evaluate each IS for changes that would require reaccreditation (paragraph 8-202b). If no changes were made, the ISSM would notify DSS by phone, postal or electronic mail. After verifying the original accreditation was valid, DSS would annotate the original accreditation letter with the date of the re-evaluation and provide a copy to the ISSM.

e. Withdrawal of Accreditation. The CSA shall evaluate the risks and consider withdrawal of accreditation if the protection measures approved for the system do not remain effective or whenever any of the following items change: levels of concern,

protection level, technical or nontechnical protection measures, vulnerabilities, operational environment, operational concept, or interconnections. The CSA shall withdraw accreditation and ensure proper sanitization when the system is no longer required to process classified information, or if the operational need for the system no longer outweighs the risk of operating the system.

f. Invalidation of an Accreditation. The CSA will be notified and an accreditation will become invalid immediately whenever detrimental, security-significant changes occur to any of the following: the required protection level; the operational environment; or the interconnections.

19. Issue: Paragraph 8-202f introduces a new concept of "invalidation" without identifying how, or if, this is different from withdrawal of accreditation (8-202e).

Answer: The end result for either withdrawal or invalidation is the same, the IS is not authorized to process classified information. The difference is in the process and the extent that classified information might be compromised. Invalidation by the DAA requires immediate termination of classified processing. Invalidation is caused when "detrimental" security-significant changes occur that could cause a compromise of classified information. Withdrawal requires the DAA to evaluate new or different risks. During the evaluation, the DAA may decide to permit classified processing to continue.

g. Certification and Accreditation of Similar Systems. If two or more similar IS are to be operated in equivalent operational environments (e.g., the levels of concern and protection level are the same, the users have at least the required clearances and access approvals for all information on the IS, the IS configurations are essentially the same, and the physical security requirements are similar), a Master SSP may be written by the ISSO, certified by the ISSM, and then approved by the CSA to cover all such IS. The IS covered by a Master SSP may range from stand alone workstations up to and including multi-user IS and local networks that meet the criteria for a Master SSP approach. This type of approval applies only to systems operating at Protection Levels 1 and 2 (see 8-402).

20. Question: Paragraph 8-202g. Can a multiple facility organization develop just one master SSP covering all locations?

Answer: No. Each facility is responsible for developing and maintaining their own master SSP.

21. Question: Paragraph 8-202g. Can "one" master SSP be written that covers all IS within the contractor's facility that operates at Protection Levels 1 and 2?

Answer: No. A master SSP can be prepared for "similar" IS that operate in equivalent operational environments (i.e., a master SSP for stand alone workstations, another for multi-user IS or local networks).

(1) Master Information Systems Security Plan. The Master SSP shall specify the information required for each certification for an IS to be accredited under the plan.

(2) An IS Certification Report shall contain the information system identification and location and a statement signed by the ISSM certifying that the IS implements the requirements in the Master SSP.

(3) The CSA shall accredit the first IS under the Master SSP. All other IS to be operated under the Master SSP shall be certified by the ISSM as meeting the conditions of the approved Master SSP. This certification, in effect, accredits the individual IS to operate under the Master SSP. A copy of each certification report shall be retained with the approved copy of the Master SSP.

22. Question: Paragraph 8-202g(3) requires the ISSM to certify additional ISs under a master SSP but does not require notification to DSS. Should DSS be notified?

Answer: Yes. The number of accredited ISs and SSPs are used in determining the size and complexity of the contractor's security program.

(4) Recertification. IS certified under a Master SSP remain certified until the Master SSP is changed or 3 years have elapsed since the IS was certified. If either the levels of concern or protection level described in the Master SSP change, the Master SSP shall be re-accredited by the CSA and all IS certified under the Master SSP shall be re-certified by the ISSM in coordination with the CSA.

h. Systems under Multiple CSAs. For a system that involves multiple CSAs, the CSAs shall designate a primary CSA. Each facility involved in the system shall identify, in writing, the security officials who are responsible for implementing IS protection on the system components at their respective facility.

Section 3. Common Requirements

8-300. Introduction. This section describes the protection requirements that are common to all IS.

8-301. Clearing and Sanitization. Instructions on clearing, sanitization and release of IS media shall be issued by the accrediting CSA.

23. *Question: Paragraph 8-301. Where can instructions on clearing and sanitizing IS memory and media be found?*

Answer: DSS posted the clearing and sanitization matrix at <http://www.dss.mil/infoas/index.htm> along with instructions/procedures on their use.

a. Clearing. Clearing is the process of eradicating the data on media before reusing the media in an environment that provides an acceptable level of protection for the data that was on the media before clearing. All internal memory, buffer, or other reusable memory shall be cleared to effectively deny access to previously stored information.

24. *Question: Paragraph - 8-301a provides the requirements for clearing data from memory and media. When is "clearing" required?*

Answer: Clearing of memory and media is required (sanitized for TOP SECRET) before and after periods processing (paragraph 8-502a) and as a method of ensuring need-to-know protection, and prior to maintenance (paragraph 8-304b(3)).

b. Sanitization. Sanitization is the process of removing the data from media before reusing the media in an environment that does not provide an acceptable level of protection for the data that was in the media before sanitizing. IS resources shall be sanitized before they are released from classified information controls or released for use at a lower classification level.

8-302. Examination of Hardware and Software. IS hardware and software shall be examined when received from the vendor and before being placed into use.

a. IS Software. Commercially procured software shall be tested to ensure that the software contains no obvious features that might be detrimental to the security of the IS. Security-related software shall be tested to verify that the security features function as specified.

25. *Question: Paragraph 8-302a. What are the review requirements of contractors that develop unclassified software that will be used during classified processing periods?*

Answer: Unclassified software, that will eventually be used during classified processing periods, is either developed by cleared, knowledgeable personnel or reviewed and/or tested by cleared, knowledgeable personnel. The review and/or testing is to provide reasonable assurance that security vulnerabilities do not exist.

26. *Question: Paragraph 8-302a. Are contractor employees that test commercially procured or security-related software required to have a clearance?*

Answer: Yes. By definition, they are "privileged users" as per paragraph 8-105a and require a security clearance to the level the IS is accredited.

27. *Question: Paragraph 8-302a. Can commercially procured or security related software be used to configure (e.g. disconnect hardware components not used for classified processing) the IS for a classified processing session?*

Answer: Yes. Provided the IS is not accredited TOP SECRET.

b. IS Hardware. Hardware shall be examined to determine that it appears to be in good working order and has no elements that might be detrimental to the secure operation of the IS when placed under facility control and cognizance. Subsequent changes and developments that affect security may require additional examination.

8-303. Identification and Authentication Management. As the complexity of a specific IS and the associated residual risk for this system increase, the need for identification and authentication of users and process becomes more significant. Identification and authentication controls are required to ensure that users have the appropriate clearances and need-to-know for the information on a particular system and shall be managed in accordance with procedures identified in the SSP.

a. Unique Identification. Each user shall be uniquely identified and that identity shall be associated

with all auditable actions taken by that individual.

b. Authentication at Logon. Users shall be required to authenticate their identities at “logon” time by supplying their authenticator, such as a password, smart card, or biometrics, in conjunction with their user identification (ID) prior to the execution of any application or utility on the system.

c. Applicability of Logon Authentication. In some cases, it may not be necessary to use IS security controls as logon authenticators. In the case of stand alone workstations, or small local area networks, physical security controls and personnel security controls may suffice. For example, if the following conditions are met, it may not be necessary for the IS to have a logon and password:

28. Question: Paragraph 8-303c permits physical security controls and personnel security controls to augment the logon authentication requirement for standalone workstations or local area networks. What types of personnel security controls are acceptable?

Answer: The ISSM/ISSO are responsible for verifying all users’ clearance and need-to-know requirements. Once briefed, the users’ names will be added to the area access list or the equipment authorization lists which authenticates that the user is authorized and briefed. The access lists shall be retained as an audit 1 requirement.

29. Question: Paragraph 8-303c permits physical security and personnel security controls in place of logon authenticators for small local area networks. Does “small” refer to the number of workstations or the area in which the workstations reside?

Answer: The area, to include size, in which the workstations are located. Paragraph 8-303 is addressing an alternative authentication procedure where the ISSO will be able to quickly and easily authenticate the users.

(1) 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.

(2) 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.

(3) The workstation is located within an

approved security area, and all uncleared/lower-cleared personnel are escorted within the area.

d. Access to Authentication Data. Access to authentication data shall be restricted to authorized personnel through the use of encryption or file access controls, or both.

e. User ID Reuse. Prior to reuse of a user ID, all previous access authorizations (including file accesses for that user ID) shall be removed from the system.

f. User ID Removal. When an employee terminates, loses access to the system for cause, or no longer has a reason to access the IS, that individual’s user ID and its authentication shall be disabled or removed from the system.

g. User ID Revalidation. Active user IDs are revalidated at least annually.

13. Question: Paragraphs 8-1041 and 8-303g require that active user IDs be revalidated at least annually. Is there a requirement to revalidate users of standalone workstations or small local area networks (paragraph 8-303c) since user IDs are not required?

Answer: Yes. The intent of this paragraph is to verify that all users have a continued need to access the accredited IS. Since user IDs are not always required (paragraph 8-303c), access lists can be used. If used for revalidation, access lists shall be retained as an audit 1 requirement.

h. Protection of Individual Authenticator. An authenticator that is in the form of knowledge (password) or possession (smart card, keys) shall not be shared with anyone.

i. Protection of Individual Passwords. When passwords are used as authenticators, the following shall apply:

(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.

30. Question: Paragraph 8-303i(3). What method(s) of password generation will DSS approve?

Answer: The preferred method of password generation is for the IS to generate unique, random passwords. However, users are permitted to generate their own passwords. User generated passwords must be a minimum of eight alpha/numeric upper/lower case characters. Users shall be briefed not to use dictionary definable passwords to include sport names, pets or family members. The SSP must address the password generation method (i.e., IS or user generated), length and whether the password is unique and random.

(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.

8-304. Maintenance. IS are particularly vulnerable to security threats during maintenance activities. The level of risk is a factor of the nature of the maintenance person's duties, the security awareness of the employees, and the maintenance person's access to classified information and facilities.

a. Cleared Maintenance Personnel. Maintenance personnel who are cleared to the highest classification level of information on the system and indoctrinated for all information processed on that system do not require an escort, if need-to-know controls can be implemented. When possible, an appropriately cleared and technically knowledgeable, facility employee shall be present within the area where the maintenance is being performed to ensure that security procedures are being followed.

b. Uncleared (or Lower-Cleared) Maintenance

Personnel.

(1) If appropriately cleared personnel are unavailable to perform maintenance, an unclassified or lower-classified person may be used, provided an appropriately cleared and technically qualified escort monitors and records the maintenance person's activities in a maintenance log. Unclassified maintenance personnel must be U.S. citizens.

31. Question: Paragraph 8-304b(1). Is the contractor required to verify the citizenship of the unclassified maintenance personnel?

Answer: The contract must specify that the unclassified maintenance personnel are U.S. citizens. The ISSM may spot check the citizenship of the maintenance personnel by contacting the company if there is doubt as to the citizenship of a specific maintenance person.

(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.

32. Question: Paragraph 8-304b(3). What maintenance procedures must be identified, enforced, and documented when the IS cannot be cleared (paragraph 8-301a) either before or after maintenance?

Answer: Every effort should be made to use cleared maintenance personnel. If a cleared person is not performing maintenance, a technically knowledgeable escort is required to oversee all maintenance operations. Any, and all, vendor-supplied software used for maintenance must reside on write-protected media or be read only.

24. Question: Paragraph - 8-301a provides the requirements for clearing data from memory and media. When is "clearing" required?

Answer: Clearing of memory and media is required (sanitized for TOP SECRET) before and after periods processing (paragraph 8-502a) and as a method of ensuring need-to-know protection, and prior to maintenance (paragraph 8-304b(3)).

(4) A separate, unclassified copy of the operating system, including any micro-coded floppy disks, CD-ROM, or cassettes that are integral to the operating system, shall be used for all maintenance operations. The copy shall be labeled "UNCLASSIFIED -- FOR MAINTENANCE ONLY" and protected in accordance with procedures established in the SSP. Maintenance procedures for an IS using a non-removable storage device on which the operating system is resident shall be considered by the ISSM on a case-by-case basis.

33. Question: Paragraph 8-304b(4) states that a separate copy of the operating system is used during maintenance operations. If the contractor has arranged for remote maintenance, can the original operating system that is used for classified processing stay resident on-line during the maintenance operation?

Answer: No. The contractor must use a separate copy of the operating system and any maintenance software.

34. Question: Paragraph 8-304b(4). What procedures should the ISSM implement for an IS using non-removable storage?

Answer: Same procedures identified above for paragraph 8-304b(3).

8-305. Malicious Code. Policies and procedures to detect and deter incidents caused by malicious code, such as viruses or unauthorized modification to software, shall be implemented. All files must be checked for viruses before being introduced on an IS and checked for other malicious code as feasible. The use of personal or public domain software is strongly discouraged. Each installation of such software must be approved by the ISSM.

8-306. Marking Hardware, Output, and Media. Markings on hardware, output, and media shall conform to Chapter 4 of this Manual. If the required marking is impractical or interferes with the operation of the media, the CSA may approve alternate marking procedures.

a. Hardware Components. All components of an IS, including input/output devices that have the

potential for retaining information, terminals, stand-alone microprocessors, or word processors used as terminals, shall 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. This labeling may be accomplished using permanent markings on the component, a sign placed on the terminal, or labels generated by the IS and displayed on the screen. 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.

35. Question: Does DSS require external color-coded labels as per paragraph 8-306a?

Answer: No.

b. Hard Copy Output and Removable Media.

Hard copy output (paper, fiche, film, and other printed media) and removable media shall 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.

36. Issue: Paragraphs 8-306b and 8-310b discuss the "trusted download" process where electronic files and/or media can be created at a classification level lower than the accreditation level of the IS without going into sufficient detail of the review process or program. Because of the many different vendor platforms and applications (e.g., word processing, database, electronic mail, spreadsheets) additional guidance is needed.

Answer: Every vendor's platform and application are unique and each requires a thorough review by the ISSM and DSS before they can be used to create classified or unclassified files and/or media. DSS has developed a "standard" for the trusted download process that can be found at <http://www.dss.mil/infoas/index.htm>. If the ISSM is unable to implement the DSS "standard," the SSP must include a description of how and why the contractor has deviated from the standard under the vulnerability-reporting requirement of paragraph 8-610a(1)(c). If the ISSM is unable to provide any acceptable countermeasure to mitigate this vulnerability, the ISSM must notify and get acceptance from the GCA/data owner of the additional risk.

c. Unclassified Media. In the CSA-approved areas where classified and unclassified information are processed on collocated IS, unclassified media shall be so marked.

37. Issue: Paragraph 8-306c requires marking of unclassified media when classified and unclassified IS are collocated. Since the DSS approved area can range in size and structure (e.g., small office cubicle to a multi-story building) additional guidance is needed.

Answer: The purpose of externally marking media when classified and unclassified IS are collocated is to clearly convey/distinguish the classification level of the media. The ISSM/ISSO must establish well-defined perimeters for the classified IS. These perimeters not only distinguish the classified area, but assist in distinguishing classified media from unclassified media within the area. Writeable media within the classified IS area perimeter that is unmarked and not in factory sealed-packages must be considered classified and marked accordingly. Writeable media not in the classified IS area that is unmarked is considered unclassified.

8-307. Personnel Security. Personnel with system access play an integral role in protecting information; defining their 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, shall be specified in writing. So far as feasible, security duties shall be distributed to preclude any one individual from adversely affecting operations or the integrity of the system. Protection levels for particular IS shall be determined by the clearance level, formal access approvals, and need-to-know held by users of the IS, and the classification level of data processed or stored.

8-308. Physical Security.

a. Safeguards shall be 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.

38. Question: Paragraph 8-308a. How is hardware integrity maintained?

Answer: Hardware integrity of the accredited IS not

processing classified information or powered off can be maintained by one or more of the following methods:

a. Continuous supervision by authorized personnel.

b. Use of approved cabinets, enclosures, seals, locks or Closed Areas.

c. Use of area controls that prevent or detect tampering or theft of the IS hardware and/or software. These controls will vary depending on the security in-depth at the contractor's facility and in the immediate area of the IS.

b. Classified processing shall take place in a CSA-approved area.

39. Issue/Question: Paragraph 8-308b. What is the boundary of the DSS approved area.

Answer: Attended classified processing shall take place in an area where authorized contractor personnel can exercise constant surveillance and maintain control of the IS. The area shall have an identifiable boundary (e.g., walls, signs, tape on floor, rope or chains) where it is obvious that the area is restricted to only authorized personnel. Unattended classified processing requires a closed area and supplemental controls depending upon the accreditation level of the IS.

c. Visual Access. Devices that display or output information in human-readable form shall be positioned to prevent unauthorized individuals from reading the information.

d. Unescorted Access. All personnel granted unescorted access to the area containing the IS shall have an appropriate security clearance.

40. Question: Paragraph 8-308d. If the IS is not located in a DSS closed area, but in an office environment, does everyone in the area require a clearance or escorted?

Answer: No, provided the contractor has security-in-depth and has area controls or devices on the IS that prevent or detect tampering or theft of the IS hardware and/or software.

8-309. Protection of Media. Media must be protected to the level of accreditation until an appropriate classification review has been conducted.

8-310. Review of Output and Media.

a. 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.

41. Question: Paragraph 8-310a. What software applications can be used to examine information not in human-readable form (e.g., embedded graphs, sound, video, etc)?

Answer: DSS has developed a "standard" for the trusted download process that can be found at <http://www.dss.mil/infoas/index.htm>. Many of the standard applications are identified and can be used with reasonable assurance that only the requested information will be transferred. However, for some applications (i.e., sound, video) there is little to no assurance in the "trusted download" process, requiring acknowledgement of the additional risk from the GCA.

b. 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.

36. Issue: Paragraphs 8-306b and 8-310b discuss the "trusted download" process where electronic files and/or media can be created at a classification level lower than the accreditation level of the IS without going into sufficient detail of the review process or program. Because of the many different vendor platforms and applications (e.g., word processing, database, electronic mail, spreadsheets) additional guidance is needed.

Answer: Every vendor's platform and application are unique and each requires a thorough review by the ISSM and DSS before they can be used to create classified or unclassified files and/or media. DSS has developed a "standard" for the trusted download process that can be found at <http://www.dss.mil/infoas/index.htm>. If the ISSM is unable to implement the DSS "standard," the SSP must include a description of how and why the contractor has deviated from the standard under the vulnerability-reporting requirement of paragraph 8-610a(1)(c). If

the ISSM is unable to provide any acceptable countermeasure to mitigate this vulnerability, the ISSM must notify and get acceptance from the GCA/data owner of the additional risk.

42. Issue: Paragraph 8-310b indicates that DSS will approve random or representative sampling techniques when verifying large volumes of output for proper markings.

Answer: When the output is in printed form, a random sampling of no less than 20% is required. When the output is in electronic form, "text" searches or scans looking for classified information can produce the desired results.

8-311. Configuration Management Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.

43. Question: Paragraph 8-311. Should the CM program include peripherals as well as platforms?

Answer: Yes. Configuration Management shall be implemented on any IS component that has the capability of retaining information.

a. Configuration Documentation. Procedures shall be implemented to identify and document the type, model, and brand of system or network component (e.g., a workstation, personal computer, or router), security-relevant software product names and version or release numbers, and physical location.

b. System Connectivity. Procedures shall be implemented to identify and document system connectivity, including any software used for wireless communication, and any communications media.

c. Connection Sensitivity. The sensitivity level of each connection or port controlled by the Security Support Structure (SSS) shall be documented.

44. Question: Paragraph 8-311c. What is the Security Support Structure (SSS)?

Answer: The Security Support Structure is the hardware, software and firmware required to adjudicate security policy and implementation differences among IS components and networks. A reference guide to networks that discusses the SSS in

more detail can be found at <http://www.dss.mil/infoas/index.htm>.

d. CM Plan. The facility CM program shall be documented in a CM plan and shall include:

(1) Formal change control procedures to ensure the review and approval of security-relevant hardware and software.

45. Question: Paragraph 8-311d(1). What is “security-relevant” hardware and software?

Answer: For hardware, any IS component that contains, or has the potential of containing, classified information. For software, and all virus detection and sanitization software. Additionally, all operating system software used on an IS where Identification & Authentication is technically implemented.

(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

8-400. Protection Profiles. Protection profiles required for a particular IS are determined by the Level of Concern for Confidentiality and by the operating environment of the system as reflected by the clearances, access approvals and need-to-know embodied in the user environment. Operational data integrity and system availability, while important security concerns, are not covered by the NISP and will be determined in additional guidance or requirements issued by the GCA. However, provisions for integrity and availability concerns are included in this Chapter to provide guidance when the GCA contractually imposes them.

4. Question: Paragraph 8-100a states that the IS must be properly managed to protect against loss of data integrity and to ensure the availability of the data and system. Paragraph 8-400 states that integrity and availability are not covered by the National Industrial Security Program (NISP) and will be determined in additional guidance or requirements issued by the GCA. Is paragraph 8-100a addressing “general security concerns” and not National Industrial Security Program Operating Manual (NISPOM) requirements?

Answer: Yes. While important, data integrity and system availability are not covered by the NISP (paragraph 8-400) and will be determined in additional guidance or requirements issued by the GCA.

8-401. Level of Concern. The level of concern reflects the sensitivity of the information and the consequences of the loss of confidentiality, integrity or availability.

a. Information Sensitivity Matrices. The matrices presented in Tables 1, 2, and 3 are designed to assist the CSA, with input from the ISSM in determining the appropriate protection level for confidentiality, and the level of concern for integrity, and availability, if contractually mandated, for a given IS processing a given set of information. The Information Sensitivity Matrices should be used as follows:

(1) A determination of high, medium, or basic shall be 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) When multiple applications on a system result in different levels of concern for the categories of

confidentiality, integrity and availability the highest level of concern for each category shall be used.

b. 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.

c. 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.

d. 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.

8-402. Protection Level. The protection level of an IS is 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. The protection level translates into a set of requirements (tables 5, 6, and 7) that must be implemented in the resulting system. Table 4 presents the criteria for determining the following three protection levels for confidentiality.

46. Question: Section 4, Paragraph 8-402 does not have a protection level that corresponds to the Multilevel Security Mode. What are the security requirements for contractors who need to develop systems in the Multilevel Security Mode?

Answer: DoD has determined that the multilevel security mode is “high-risk” and should be addressed by the NISPOM Supplement. For the purposes of this ISL, systems are operating at Protection Level 4 when at least one user lacks sufficient clearance for access to all the information on the IS, but all users have at least a Confidential clearance when the IS is accredited at the Secret level or a Secret clearance when the IS is accredited at the Top Secret level.

a. Systems are operating at Protection Level 1 when all users have all required approvals for access to all information on the system. This means that all users have all required clearances, formal access approvals, and the need-to-know for all information on the IS, i.e. dedicated mode.

b. Systems are operating at Protection Level 2 when 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.

c. Systems are operating at Protection Level 3 when 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.

8-403. Protection Profiles. Protection requirements graded by levels of concern and confidentiality protection level are detailed in Section 6. Tables 5, 6, and 7 present the requirements detailed in Section 6. To use these tables, find the column representing the protection level for confidentiality, or, if contractually mandated, find the column representing the level of concern for integrity or availability.

a. Confidentiality Components. Confidentiality components describe the confidentiality protection requirements that must be implemented in an IS using the profile. The confidentiality protection requirements are graded according to the confidentiality protection levels.

b. Integrity Components. Integrity components, if applicable, describe the integrity protection requirements that must be implemented in an IS using the profile. The integrity protection requirements are graded according to the integrity level of concern.

c. Availability Components. Availability components, if applicable, describe the availability protection requirements that must be implemented in an IS using the profile. The availability protection requirements are graded according to the availability level of concern.

Table 1. Information Sensitivity Matrix for Confidentiality.

Level of Concern	Qualifiers
High	TOP SECRET and SECRET Restricted Data (SIGMAs 1,2,14,15)
Medium	SECRET SECRET Restricted Data
Basic	CONFIDENTIAL

Table 2. Information Sensitivity Matrix for Integrity.

Level of Concern	Qualifiers
High	Absolute accuracy required for mission accomplishment; or loss of life might result from loss of integrity; or loss of integrity will have an adverse effect on national-level interests; or loss of integrity will have an adverse effect on confidentiality.
Medium	High degree of accuracy required for mission accomplishment, but not absolute; or bodily injury might result from loss of integrity; or loss of integrity will have an adverse effect on organizational-level interests.
Basic	Reasonable degree of accuracy required for mission accomplishment.

Table 3. Information Sensitivity Matrix for Availability.

Level of Concern	Qualifiers
High	Information must always be available upon request, with no tolerance for delay; or loss of life might result from loss of availability; or loss of availability will have an adverse effect on national-level interests; or loss of availability will have an adverse effect on confidentiality.
Medium	Information must be readily available with minimum tolerance for delay; or bodily injury might result from loss of availability; or loss of availability will have an adverse effect on organizational-level interests.
Basic	Information must be available with flexible tolerance for delay.

NOTE: In this context, “High - no tolerance for delay” means no delay; “Medium - minimum tolerance for delay” means a delay of seconds to hours; and “Basic - flexible tolerance for delay” means a delay of days to weeks. In the context of the NISPOM, integrity and availability shall only apply when they have a direct impact on protection measures for confidentiality, i.e., integrity of the password file, integrity of audit logs or when contractually imposed.

Table 4. Protection Level Table for Confidentiality.

Lowest Clearance	Formal Access Approval	Need-To-Know	Protection Level
<i>Confidential, information classification no more than one level higher</i>	<i>NOT ALL Users Have ALL</i>	<i>Not contributing to the decision</i>	<i>4</i>
At Least Equal to Highest Data	NOT ALL Users Have ALL	Not contributing to the decision	3
At Least Equal to Highest Data	ALL Users Have ALL	NOT ALL Users Have ALL	2
At Least Equal to Highest Data	ALL Users Have ALL	ALL Users Have ALL	1

Table 5. Protection Profile Table for Confidentiality.

Requirements (Paragraph)	Confidentiality Protection Level			
	P L 1	PL 2	PL 3	<i>PL 4</i>
Audit Capability (8-602)	Audit 1	Audit 2	Audit 3 Audit 4	<i>Audit 5,6,7</i>
Data Transmission (8-605)	Trans 1	Trans 1	Trans 1	<i>Trans 1</i>
Access Controls (8-606)	Access 1	Access 2	Access 3	<i>Access 4,5</i>
Identification & Authentication (8-607)	I&A 1	I&A 2,3,4	I&A2,4,5	<i>I&A 6</i>
Resource Control (8-608)		ResrcCtrl 1,	ResrcCtrl 1	<i>ResrcCtrl 1</i>
Session Controls (8-609)	SessCtrl 1	SessCtrl 2	SessCtrl 2	<i>SessCtrl 2</i>
Security Documentation (8-610)	Doc 1	Doc 1	Doc 1	<i>Doc 2,4</i>
Separation of Functions (8-611)			Separation	<i>Separation</i>
System Recovery (8-612)	SR 1	SR 1	SR 1	<i>SR 1</i>
System Assurance (8-613)	SysAssur 1	SysAssur 1	SysAssur 2	<i>SysAssur 3,4</i>
Security Testing (8-614)	Test 1	Test 2	Test 3	<i>Test 4</i>

Table 6. Protection Profile Table for Integrity.

Requirements (Paragraph)	Integrity Level of Concern		
	Basic	Medium	High
Audit Capability (8-602)	Audit 1	Audit 2	Audit 3
Backup and Restoration of Data (8-603)	Backup 1	Backup 2	Backup 3
Changes to Data (8-604)		Integrity 1	Integrity 2
System Assurance (8-613)		SysAssur 1	SysAssur 2
Security Testing (8-614)	Test 1	Test 2	Test 3

Table 7. Protection Profile Table for Availability.

Requirements (Paragraph)	Availability Level of Concern		
	Basic	Medium	High
Alternate Power Source (8-601)		Power 1	Power 2
Backup and Restoration of Data (8-603)	Backup 1	Backup 2	Backup 3

Section 5. Special Categories

47. Issue/Question: Section 5, Special Categories. Identifies several categories of “systems” that can be adequately secured without implementation of all the technical features and safeguards identified in Sections 3, 4 and 6. Would you clarify?

Answer: The DSS ISSP and the ISSM/ISSO develop protection measures for special categories of systems on a case-by-case basis. Once determined, the facility’s SSP will reflect the “special system” and all agreed upon protection measures.

8-500. Special Categories. Several categories of systems can be adequately secured without implementation of all the technical features specified this Chapter. These systems are not “exceptions” or “special cases” but applying the technical security requirements to these systems by rote results in unnecessary costs and operational impacts. In general, the technical questions are where, when, and how to apply a given set of protection measures, rather than whether to apply the measures. For many of these “special” systems (such as guards or pure servers; and tactical, embedded, data-acquisition, and special-purpose systems), the physical security protections for the system provide the required access control, while the application running on the platform provides the required user separation.

8-501. Single-user, Stand-alone Systems. Extensive technical protection measures are normally inappropriate and inordinately expensive for single-user, stand-alone systems. The CSA can approve administrative and environmental protection measures for such systems, in lieu of technical ones. Systems that have one user at a time, but have a total of more than one user with no sanitization between users, are multi-user systems, and the CSA shall consider the systems as such in determining the protection level and the resulting security requirements. Systems that have one user at a time, are sanitized between users and periods of different classification/sensitivity, are periods processing systems as described below.

48. Question: Paragraph 8-501. When is sanitization of memory and media required?

Answer: Sanitization of memory and media is required if the standalone system is being “released” to users with a PCL lower than the accreditation level or the standalone system is accredited at the TOP SECRET level. Clearing (paragraph 8-301a) is all that is required when changing classification levels or information sensitivity.

8-502. Periods Processing. Periods processing is a method of sequential operation of an IS that provides

the capability to process information at various levels of sensitivity at distinctly different times.

a. 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).

24. Question: Paragraph - 8-301a provides the requirements for clearing data from memory and media. When is “clearing” required?

Answer: Clearing of memory and media is required (sanitized for TOP SECRET) before and after periods processing (paragraph 8-502a) and as a method of ensuring need-to-know protection, and prior to maintenance (paragraph 8-304b(3)).

b. Sanitization After Use. If an IS is used for periods processing either by more than one user or for segregating information by classification level onto separate media, the SSP shall specify the sanitization procedures to be employed by each user before and after each use of the system.

c. Sanitization Between Periods. The IS shall be sanitized 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). These procedures shall be documented in the SSP. Such procedures could include, among others, sanitizing non-volatile storage, exchanging disks, and powering down the IS and its peripherals.

d. Media For Each Period. An IS employed in periods processing shall have separate media for each period of processing, including copies of operating systems, utilities, and applications software.

e. Audit. If there are multiple users of the system and the system is not capable of automated logging, the

CSA shall consider requiring manual logging. Audit trails are not required for single-user stand-alone systems.

49. Question: Paragraph 8-502e states that the CSA shall consider manual logging for multiple user systems that are not capable of automated logging. Does DSS require manual logging, and if so, can access lists be used for validation purposes as addressed in an earlier question?

Answer: Yes. Manual logging is required, and like the answer for 8-104l, access lists can be used for validation purposes and shall be retained as an Audit 1 requirement.

8-503. Pure Servers.

a. Certain specialized systems, when acting as pure servers in a network, do not fit the protection level criteria and may need fewer technical security countermeasures. These systems have the following characteristics:

- (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.

b. The platform (i.e., hardware and operating system) on which the guard or pure server runs usually needs to meet no more than Protection Level 3 security requirements. The guard or pure server may have a large number of clients (i.e., individuals who use the guard or server functional capabilities in a severely constrained way). The guard application or server application itself will have to provide the more stringent technical protections appropriate for the system's protection level and operational environment. Assurances appropriate to the levels of concern for the

system shall be implemented.

50. Question: Paragraph 8-503b states that the platform on which the guard or server runs usually needs to meet no more than Protection Level 3 security requirements. Is this correct since the May Chapter 8 only has 3 Protection Levels?

Answer: Yes. The protection profile table for confidentiality (Chapter 8, Table 5) is made up of eleven requirements identifying graded requirements for the three protection levels. The wording in paragraph 8-503b does not restrict the platform on which a guard or pure server resides to a single protection level for all eleven requirements (e.g., a guard or pure server might have an access requirement of PL3 but an auditing requirement of PL1).

51. Question: Paragraph 8-500 indicates that special categories of systems do not require all the technical features and safeguards of chapter 8 to be adequately secured. This philosophy of less applies to all systems identified in Section 5 except to guard or server applications (8-503b) where they will be provided with more stringent technical protections than the system's protection level. Please explain?

Answer: The application running on a guard or server is viewed separately from the hardware platform. It is not uncommon for the guard or pure server platform to be at a protection level less than the protection level associated with the application.

c. Systems that have general users or execute general user code are not "pure servers" within the meaning of this section, and so must meet all security requirements specified for their protection level and operational environment.

d. The term "pure server" is not intended to limit the applicability of this section to systems that have traditionally been referred to as servers. For example, a messaging system that happened to be implemented on a general-purpose computer platform could be accredited under this section and, if such a system meets the specifications in a, above, the system's technical requirements could be categorized by this section.

52. Question: Paragraph 8-503d. Do "pure servers" (i.e., guard, proxy server, application server) require accreditation separate from the "general-purpose computer" they support or are connected to?

Answer: Normally the only "pure server" that would

require separate accreditation is a guard. The guard requires more stringent technical protection and assurance than the ISs it protects by the very nature of its function. The other types of "pure servers" can be described and included in the "general-purpose computers SSP."

authenticators may not be shared with anyone outside of the group.

e. The above easing of technical security requirements does not imply any relaxation in other security requirements (e.g., physical and communications security requirements) which are determined by the information handled or protected by the system. As stated above, this easing of technical requirements is predicated upon adequate application of physical security and other appropriate security disciplines.

8-504. Tactical, Embedded, Data-Acquisition, and Special-Purpose Systems. Some systems are incapable of alteration by users and are designed and implemented to provide a very limited set of predetermined functions. Certain tactical or so-called "embedded" systems fall into this category, as do some data-acquisition systems and some other special-purpose systems. These systems also have the characteristics that: first and most importantly, there are no general users on the system; and, second, there is no user code running on the system. If the CSA determines that such a system is sufficiently incapable of alteration, and that the application(s) running on the system provide an adequate level of security, then the system does not have to meet additional security requirements specified for more-general-purpose systems in this section. The CSA and implementers are cautioned to be sure that such systems do, in all operational situations, provide the separation appropriate to the system's protection level.

8-505. Systems with Group Authenticators. Many security measures specified in this section implicitly assume that the system includes an acceptable level of individual accountability. This is normally ensured by the use of unique user identifiers and authenticators. Operationally, the design of some systems necessitates more than one individual using the same identifier/authenticator combination. Such situations are often referred to as requiring the use of group authenticators. In general, the use of group authenticators precludes the association of a particular act with the individual who initiated that act. In turn, this can preclude assignment of responsibility and can exacerbate the difficulties involved in incident investigation. Group authenticators shall be used only for broader access after the use of a unique authenticator for initial identification and authentication, and documented in SSP. Group

Section 6. Protection Requirements

8-600. Introduction. This section describes the implementation requirements for different protection measure.

8-601. Alternate Power Source (Power). An alternate power source ensures that the system availability is maintained in the event of a loss of primary power. An APS can also provide a time period for orderly system shutdown or the transfer of system operations to another system or power source.

a. Power 1 Requirements. Procedures for the graceful shutdown of the system shall ensure no loss of data. The decision not to use an alternate source of power, such as an uninterruptible power supply (UPS) for the system, shall be documented.

b. Power 2 Requirements. Instead of Power 1, procedures for transfer of the system to another power source shall ensure that the transfer is completed within the time requirements of the application(s) on the system.

8-602. Audit Capability. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.

53. Question: Paragraph 8-602. What security-relevant activities should be recorded for all protection levels and all special category IS?

Answer: Audit requirements 1-4 identify IS functions that are normally captured by an automated audit capability. Additionally, manual logs are required for:

a. Maintenance, repair, installation, or removal of hardware components. Log must include the component involved, the action taken and the name of the escort if the maintenance was performed by an uncleared individual.

b. Installation, testing, and modification of operating system and security-related software (if applicable). Logs must identify the software involved.

c. Periods processing times.

d. Sanitization and declassifying memory, media and devices.

e. Application and reapplication of security seals (if applicable).

a. Audit 1 Requirements.

(1) Automated Audit Trail Creation: The system shall automatically create and maintain an audit trail or log (On a PL-1 system only: In the event that the Operating System cannot provide an automated audit capability, an alternative method of accountability for user activities on the system shall be developed and documented.) Audit records shall be created to record the following:

54. Question: Paragraph 8-602a(1) permits an alternative method of auditing a PL-1 system when the Operating System cannot provide an automated capability. What alternative method should be used?

Answer: When the IS cannot provide an automated capability (paragraph 8-502e), or the IS meets the requirements of paragraph 8-501, manual logs are required.

(a) Enough information to determine the date and time of action (e.g., common network time), the system locale of the action, the system entity that initiated or completed the action, the resources involved, and the action involved.

(b) Successful and unsuccessful logons and logoffs.

(c) Successful and unsuccessful accesses to security-relevant objects and directories, including creation, open, close, modification, and deletion.

55. Question: Paragraph 8-602a(1)(c) can generate upwards to 100 audit entries for each successful access to security-relevant objects and/or directories. From a security standpoint, is this information of enough importance to generate voluminous amounts of auditing data?

Answer: No. Only unsuccessful accesses need to be audited.

(d) Changes in user authenticators.

(e) The blocking or blacklisting of a user ID, terminal, or access port and the reason for the action.

(f) Denial of access resulting from an excessive number of unsuccessful logon attempts.

(2) Audit Trail Protection. The contents of audit trails shall be protected against unauthorized access, modification, or deletion.

(3) Audit Trail Analysis. Audit analysis and reporting shall be scheduled, and performed. Security relevant events shall be documented and reported. The frequency of the review shall be at least weekly and shall be documented in the SSP.

(4) Audit Record Retention. Audit records shall be retained for at least one review cycle or as required by the CSA.

56. Question: How long are the audit records retained (paragraph 8-602a(4))?

Answer: Audit records covering the previous 12 months, or since the IS was accredited (which ever is less), must always be retained.

b. Audit 2 Requirements. In addition to Audit 1:

(1) Individual accountability (i.e., unique identification of each user and association of that identity with all auditable actions taken by that individual). Periodic testing by the ISSO or ISSM of the security posture of the IS.

c. Audit 3 Requirements. In addition to Audit 2:

(1) Automated Audit Analysis. Audit analysis and reporting using automated tools shall be scheduled and performed.

d. Audit 4 Requirements. In addition to Audit 3:

(1) An audit trail, created and maintained by the IS, that is capable of recording changes to mechanism's list of user formal access permissions.

e. Audit 5 Requirements. In addition to Audit 4:

(1) Periodic testing by the ISSO or ISSM of the security posture of the IS by employing various intrusion/attack detection and monitoring tools. The ISSO/M shall not invoke such attack software without approval from the appropriate authorities and

concurrence of legal counsel. The output of such tools shall be protected against unauthorized access, modification, or deletion. These tools shall build upon audit reduction and analysis tools to aid the ISSO or ISSM in the monitoring and detection of suspicious, intrusive, or attack-like behavior patterns.

f. Audit 6 Requirements. In addition to Audit 5:

(1) Enforcement of the capability to audit changes in security labels.

(2) Enforcement of the capability to audit accesses or attempted accesses to objects or data whose labels are inconsistent with user privileges.

(3) Enforcement of the capability to audit all program initiations, information downgrades and overrides, and all other security-relevant events (specifically including identified events that may be used in the exploitation of covert channels).

(4) In the event of an audit failure, system shutdown unless an alternative audit capacity exists.

g. Audit 7 Requirements. In addition to Audit 6:

(1) The capability of the system to monitor occurrences of, or accumulation of, auditable events that may indicate an imminent violation of security policies.

(2) The capability of the system to notify the ISSO of suspicious events and taking the least-disruptive action to terminate the suspicious events.

8-603. Backup and Restoration of Data (Backup).

The regular backup of information is necessary to ensure that users have continuing access to the information. The periodic checking of backup inventory and testing of the ability to restore information validates that the overall backup process is working.

a. Backup 1 Requirements.

(1) Backup Procedures. Procedures for the regular backup of all essential and security-relevant information, including software tables and settings, such as router tables, software, and documentation,

shall be documented.

(2) Backup Frequency. The frequency of backups shall be defined by the ISSM, with the assistance of the GCA, and documented in the backup procedures.

b. Backup 2 Requirements. In addition to Backup 1:

(1) Backup Media Storage. Media containing backup files and backup documentation shall be stored at another location, such as another part of the same building, a nearby building, or off facility, so as to reduce the possibility that a common occurrence could eliminate the on-facility backup data and the off-facility backup data.

(2) Verification of Backup Procedures. Backup procedures shall be periodically verified.

c. Backup 3 Requirements. In addition to Backup 2:

(1) Information Restoration Testing. Incremental and complete restoration of information from backup media shall be tested on an annual basis.

8-604. Changes to Data (Integrity). The control of changes to data includes deterring, detecting, and reporting of successful and unsuccessful attempts to change data. Control of changes to data may range from simply detecting a change attempt to the ability to ensure that only authorized changes are allowed.

a. Integrity 1 Requirements.

(1) Change Procedures. Procedures and technical system features shall be implemented to ensure that changes to the data and IS software are executed only by authorized personnel or processes.

b. Integrity 2 Requirements. In addition to Integrity 1:

(1) Transaction Log. A transaction log, protected from unauthorized changes, shall be available to allow the immediate correction of unauthorized data and IS software changes and the off-line verification of all changes at all times.

8-605. Data Transmission (Trans). Information protection is required whenever classified information is to be transmitted through areas or components where individuals not authorized to have access to the

information may have unescorted physical or uncontrolled electronic access to the information or communications media (e.g., outside the system perimeter).

a. Trans 1 Requirements.

(1) Protections. One or more of the following protections shall be used.

(a) Information distributed only within an area approved for open storage of the information.

(b) National Security Agency (NSA)-approved encryption mechanisms appropriate for the encryption of classified information.

(c) Protected Distribution System.

8-606. Access Controls (Access). The IS shall store and preserve the integrity of the sensitivity of all information internal to the IS.

a. Access 1 Requirements.

(1) Denial of physical access by unauthorized individuals unless under constant supervision of technically qualified, authorized personnel.

b. Access 2 Requirements. In addition to Access 1:

(1) Discretionary access controls shall be provided. A system has implemented discretionary access controls when the security support structure defines and controls access between named users and named objects (e.g., files and programs) in the system. The discretionary access control policy includes administrative procedures to support the policy and its mechanisms.

c. Access 3 Requirements. In addition to Access 2:

(1) Some process or mechanism that allows users (or processes acting on their behalf) to determine the formal access approvals granted to another user.

(2) Some process or mechanism that allows users (or processes acting on their behalf) to determine the sensitivity level of data.

d. Access 4 Requirements. *In addition to Access 3: Access Control, including assurance that*

each user shall receive from the system only that information to which the user is authorized access.

***e. Access 5 Requirements.** In addition to Access 4: Access Control, including a Mandatory Access Control (MAC) Policy that shall require:*

(1) The Security Support Structure to enforce a mandatory access control policy over all subjects and storage objects under its control (e.g., processes, files, segments, devices).

(2) These subjects and objects to be assigned sensitivity labels that combine hierarchical classification levels and non-hierarchical categories; the labels shall be used as the basis for mandatory access control decisions.

(3) The Security Support Structure to be able to support two or more such security levels.

Identification and authentication data to be used by the Security Support Structure to authenticate the user's identity and to assure that the security level and authorization of subjects external to the Security Support Structure that may be created to act on behalf of the individual user are dominated by the clearance and authorization of that user.

(4) Application of the following restrictions to all accesses between subjects and objects controlled by the Security Support Structure:

(a) A subject can read an object only if the security level of the subject dominates the security level of the object (i.e., a subject can "read down").*

*[*Security level S1 is said to dominate security level S2 if the hierarchical classification of S1 is greater than or equal to that of S2 and the non-hierarchical categories of S1 include all those of S2.]*

(b) A subject can write to an object only if two conditions are met: the security level of the object must dominate the security level of the subject, and the security level of the user's clearance must dominate the security level of the object (i.e., a subject can "write up," but no*

higher than the user's clearance).

*[*In those instances where a subject is an electronic entity (e.g., a process), then the subject is generally acting on the behalf of a user.]*

8-607. Identification and Authentication (I&A).

a. I&A 1 Requirements. Procedures that include provisions for uniquely identifying and authenticating the users. Procedures can be external to the IS (e.g., procedural or physical controls) or internal to the IS (i.e., technical). Electronic means shall be employed where technically feasible.

b. I&A 2 Requirements. In addition to I&A 1:

(1) An I&A management mechanism that ensures a unique identifier for each user and that associates that identifier with all auditable actions taken by the user. The following must be specified in the SSP:

(a) Initial authenticator content and administrative procedures for initial authenticator distribution.

(b) Individual and Group Authenticators. Group authenticators may only be used in conjunction with an individual/unique authenticator, that is, individuals must be authenticated with an individual authenticator prior to use of a group authenticator.

(c) Length, composition and generation of authenticators.

(d) Change processes (periodic and in case of compromise.

(e) Aging of static authenticators (i.e., not one-time passwords or biometric patterns).

(f) History of authenticator changes, with assurance of non-replication of individual authenticators.

57. Question: Paragraphs 8-607b(f) requires that the IS be able to maintain a history of authenticator changes (e.g., password) with assurance of non-replication under the audit 2 requirement. What does the contractor do if the IS is unable to meet this requirement?

Answer: The ISSM will document this as a unique

vulnerability in their SSP as per paragraph 8-610a(1)(c).

(g) Protection of authenticators.

c. I&A 3 Requirements. In addition to I&A 2:

(1) 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 shall require the use of strong authentication (i.e., an I&A technique that is resistant to replay attacks.)

58. Question: Paragraphs 8-607c requires "strong authentication" for privileged users that are either located or communicate outside the IS's perimeter. What will DSS accept for strong authentication?

Answer: Strong authentication is synonymous with cryptographic or biometric devices (e.g., one-time passwords, and retina identification).

d. I&A 4 Requirements. In those instances where the means of authentication is user-specified passwords, the ISSM may 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.

e. I&A 5 Requirements. In those instances where the users are remotely accessing the IS, the users shall employ a strong authentication mechanism.

f. I&A6 Identification and Authentication management mechanisms that include:

(1) Implementation and support of a trusted communications path between the user and the Security Support Structure of the desktop for login and authentication. Communication via this path shall be initiated exclusively by the user and shall be unmistakably distinguishable from other paths.

(2) In the case of communication between two or more systems (e.g. client server architecture), bi-directional authentication between the two systems.

8-608. Resource Control (ResrcCtrl) The system shall ensure that resources contain no residual data before being assigned, allocated, or reallocated.

8-609. Session Controls (SessCtrl). Session controls are requirements, over and above identification and

authentication, for controlling the establishment of a user's session.

a. SessCtrl 1 Requirements.

(1) User Notification. All users shall be notified prior to gaining access to a system that system usage is monitored, recorded, and subject to audit. The user shall also be advised that, by using the system, he/she has granted consent to such monitoring and recording. The user shall also be advised that unauthorized use is prohibited and subject to criminal and civil penalties. If the operating system permits, each initial screen (displayed before user logon) shall contain a warning text to the user and the user shall be required to take positive action to remove the notice from the screen (monitoring and recording, such as collection and analysis of audit trail information, shall be performed). The CSA will provide an approved banner. If it is not possible to provide an "initial screen" warning notice, other methods of notification shall be developed and approved by the CSA.

(2) Successive Logon Attempts. If the operating system provides the capability, successive logon attempts shall be controlled as follows:

(a) By denying access after multiple (maximum of five) consecutive unsuccessful attempts on the same user ID.

(b) By limiting the number of access attempts in a specified time period.

(c) By the use of a time delay control system.

(d) By other such methods, subject to approval by the CSA.

(3) System Entry. The system shall grant system entry only in accordance with the conditions associated with the authenticated user's profile. If no explicit entry conditions are defined, the default shall prohibit all remote activities, such as remote logons and anonymous file access.

b. SessCtrl 2 Requirements. In addition to SessCtrl 1:

(1). Multiple Logon Control. If the IS supports multiple logon sessions for each user ID or account, the IS shall provide a protected capability to control the number of logon sessions for each user ID, account, or specific port of entry. The IS default shall

be a single logon session.

(2). User Inactivity. The IS shall detect an interval of user inactivity, such as no keyboard entries, and shall disable any future user activity until the user re-establishes the correct identity with a valid authenticator. The inactivity time period and restart requirements shall be documented in the SSP.

59. Question: Paragraph 8-609b(2). What is the baseline time period of user inactivity and what procedures are required?

Answer: After 15 minutes of user inactivity, the user will be required to reauthenticate themselves (e.g., reenter password) to the IS. If it is technically not feasible for the IS to implement this requirement, or the ISSM has implemented a time period longer than 15 minutes, the ISSM will document this as a unique vulnerability in their SSP as per paragraph 8-610a(1)(c).

(3). Logon Notification. If the operating system provides the capability, the user shall be notified upon successful logon of: the date and time of the user's last logon; the location of the user (as can best be determined) at last logon; and the number of unsuccessful logon attempts using this user ID since the last successful logon. This notice shall require positive action by the user to remove the notice from the screen.

8-610. Security Documentation (Doc). Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.

a. Doc 1 Requirements.

(1) SSP. The SSP shall contain the following:

(a) System Identification.

1. Security Personnel. The name, location, and phone number of the responsible system

owner, CSA, ISSM, and ISSO.

2. Description. A brief narrative description of the system or network mission or purpose and architecture, including subnetworks, communications devices, and protocols.

(b) System Requirements Specification.

1. Sensitivity and Classification Levels. 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.

2. Levels of Concern for Confidentiality, Integrity, and Availability. The confidentiality level of concern and protection level, the integrity level of concern, and the availability level of concern.

3. Protection Measures. Identify protection measures and how they are being met.

4. Variances from Protection Measure Requirements. A description of any approved variances from protection measures. A copy of the approval documentation shall be attached to the SSP.

(c) System-Specific Risks and Vulnerabilities. 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, a statement to that effect shall be entered. If any vulnerabilities are identified by the assessment of unique threats, the countermeasures implemented to mitigate the vulnerabilities shall be described.

(d) System Configuration. 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.

(e) Connections to Separately Accredited Networks and Systems. 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. A copy of any memoranda of understanding with other agencies shall be attached to the SSP.

(f) Security Support Structure. A brief

description of the security support structure including all controlled interfaces, their interconnection criteria, and security requirements.

(2) Certification and Accreditation Documentation.

(a) Security Testing. Test plans, procedures, and test reports including risk assessment.

(b) Documentation. The test plan for ongoing testing and the frequency of such testing shall be documented in the SSP.

(c) Certification. A certification statement that the system complies with the requirements of the protection level and levels of concern for this system. The statement shall be signed by the ISSM.

(d) Accreditation. Documentation for accreditation includes the certification package. The CSA approves the package and provides accreditation documentation.

b. Doc 2 Requirements. *Documentation shall include guide(s) or manual(s) for the system's privileged users. The manual(s) shall at a minimum provide information on (1) configuring, installing, and operating the system; (2) making optimum use of the system's security features; and (3) identifying known security vulnerabilities regarding the configuration and use of administrative functions. The documentation shall be updated as new vulnerabilities are identified.*

c. Doc 4 Requirements. *Documentation shall include:*

(1) Certification test plans and procedures detailing the implementation of the features and assurances for the required Protection Level.

(2) Reports of test results.

(3) A general user's guide that describes the protection mechanisms provided, and that supplies guidelines on how the mechanisms are to be used, and how they interact.

(4) Documentation, including System Design Documentation, if applicable.

8-611. Separation of Function Requirements (Separation). At Protection Level 3 the functions of the ISSO and the system manager shall not be performed by

the same person.

8-612. System Recovery (SR). System recovery addresses the functions that respond to failures in the SSS or interruptions in operation. Recovery actions ensure that the SSS is returned to a condition where all security-relevant functions are operational or system operation is suspended.

a. SR 1 Requirements. Procedures and IS features shall be implemented to ensure that IS recovery is done in a controlled manner. If any off-normal conditions arise during recovery, the IS shall be accessible only via terminals monitored by the ISSO or his /her designee, or via the IS console.

8-613. System Assurance (SysAssur). System assurance includes those components of a system (hardware, software, firmware, and communications) that are essential to maintaining the security policy(ies) of the system, (e.g. Security Support Structure).

a. SysAssur 1 Requirements.

(1) Access to Protection Functions. Access to hardware/software/firmware that perform systems or security functions shall be limited to authorized personnel.

b. SysAssur 2 Requirements. In addition to SysAssur1:

(1) Protection Documentation. The protections and provisions of the SysAssur shall be documented.

(2) Periodic Validation of SysAssur. Features and procedures shall exist to periodically validate the correct operation of the hardware, firmware, and software elements of the SSS and shall be documented in the SSP.

c. SysAssur 3 Requirements. In addition to SysAssur2:

(1) SSS Isolation. The SSS shall 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).

(2) Using up-to-date vulnerability assessment tools to validate the continued integrity of the Security Support Structure by ensuring that the system configuration does not

contain any well-known security vulnerabilities.

***d. SysAssur 4 Requirements.** The Security Support Structure shall maintain separate execution domains (e.g., address spaces) for each executing process.*

8-614. Security Testing (Test). Certification and ongoing security testing are the verification of correct operation of the protection measures in a system. The ISSM will perform and document the required tests.

a. Test 1 Requirements. Assurance shall be 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.

60. Question: Paragraph 8-614a requires the ISSM provide "assurance" where as paragraph 8-614b requires the ISSM provide "written assurance." Is there a difference and if so please explain?

Answer: The assurance the ISSM provides under Test 1 is a statement in the SSP that the security features, including access controls and configuration management, are implemented and operational. The written assurance the ISSM provides under Test 2, since technical security features and safeguards are required, is individual verification that each of the requirements of Table 5 are implemented and operational. Additionally, the statement must verify that access controls and configuration management is implemented.

b. Test 2 Requirements. In addition to Test1:

(1) Written assurance shall be 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.

c. Test 3 Requirements. In addition to Test2:

(1) Certification testing shall be conducted including verification that the features and assurances required for the Protection Level are functional.

(a) A test plan and procedures shall be developed and shall include:

1. A detailed description of the manner in which the system's Security Support Structure meets the technical requirements for the Protection

Levels and Levels-of-Concern for integrity and availability.

2. A detailed description of the assurances that have been implemented, and how this implementation will be verified.

3. An outline of the inspection and test procedures used to verify this compliance.

d. Test4 Requirements. Testing, including:

(1) Security Penetration Testing shall be conducted to determine the level of difficulty in penetrating the security countermeasures of the system.

(2) An Independent Validation and Verification team shall be formed to assist in the security testing and to perform validation and verification testing of the system.

8-615. Disaster Recovery Planning. If disaster recovery planning is contractually mandated, the ISSM will 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

8-700. Interconnected Systems Management. The characteristics and capabilities of an IS implemented as networks require special security considerations. This section states additional requirements on a network or expands on the security requirements stated in Section 6 as they apply to a network.

a. When connecting two or more networks, the CSA shall review the security attributes of each network (even if the networks are accredited at the same protection level) to determine whether the combination of data and/or the combination of users on the connected network requires a higher protection level.

b. A unified network is a connected collection of systems or networks that are accredited (1) under a single SSP, (2) as a single entity, and (3) by a single CSA. Such a network can be as simple as a small stand-alone LAN operating at Protection Level 1, following a single security policy, accredited as a single entity, and administered by a single ISSO. Conversely, it can be as complex as a collection of hundreds of LANs separated over a wide area but still following a single security policy, accredited as a single entity by a single CSA. The perimeter of each network encompasses all its hardware, software, and attached devices. Its boundary extends to all of its users.

62. Question: Paragraph 8-700b states that a unified network must be accredited by a single entity by a single CSA. Since DSS has more than one accrediting entity, can a unified network exist which spans more than one DSS geographical region?

Answer: Yes. The DSS structure, and not its individual accreditors, is viewed as a single entity for the purpose of this requirement.

c. An interconnected network is comprised of two or more separately accredited systems and/or networks. Each separately accredited system or network maintains its own intra-system services and controls, protects its own resources, and retains its individual accreditation. Each participating system or network has its own ISSO. The interconnected network shall have a controlled interface capable of adjudicating the different security policy implementations of the participating systems or unified networks. An interconnected network also requires accreditation as a unit.

61. Question: Section 7, Paragraphs 8-700 and 8-701 refer to the use of a Controlled Interface (CI) when connecting networks of the same or different classification levels. DoD uses the term "high assurance guard." Are the terms "high assurance guard" and "controlled interface" interchangeable?

Answer: They have the same meaning but not the same depth in scope. The description of CI, as it appears in Section 7, goes beyond the definition/capability of a "high assurance guard" as it encompasses communication equipment like routers and bridges. Within DoD, the common practice is to refer to specialized equipment by the function they serve.

63. Question: Paragraph 8-700c indicates that an interconnected network requires accreditation as a unit. Is a network SSP required and who is responsible for its preparation?

Answer: Yes. Normally the prime contractor or one of its sub-contractors prepares the network SSP. Additionally, a network ISSO must be assigned whose job is to oversee the security of the network.

d. Systems that process information at differing classification levels or with differing compartmentation (i.e., at least two kinds of information that require different formal access approvals) can be interconnected if:

64. Issue/Question: Paragraph 8-700d states that interconnected systems (i.e., networks) can process information at different classification levels or different compartments. What are the required technical security features, safeguards and assurances?

Answer: Since the purpose of the CI is to provide protection to IS at different classification levels or compartments, the CI will have to have been evaluated and found to meet the B3 level of trust under the Department of Defense Trusted

Computer System Evaluation Criteria (TCSEC) program, or the EAL6 level under the Common Criteria.

65. Question: As a follow on to the above question, when a contractor has a connection to a government network and has a CI that is used to transfer information of a different classification level, what security features, safeguards and assurances are required?

Answer: DoD requires that the contractor use a CI evaluated and certified under DoD's Secret and Below Interoperability (SABI) program. A list of evaluated SABI products is posted at <http://www.dss.mil/infoas/index.htm> along with requirements for certification and accreditation.

66. Question: Must the contractor use a CI from the SABI program when networks belonging only to contractors are interconnected at different classification levels or different compartments?

Answer: No. However, the CI must be of an equivalent evaluation as the CI from the SABI program.

(1) They are interconnected through a Controlled Interface (as defined below) that provides the separation appropriate to the combination of the level(s) and compartment(s) being processed on both systems; or

(2) Both systems are operating at the same protection level (both systems must be accredited to protect the information being transferred); or

(3) Both systems are accredited to process the level(s) and compartment(s) of information that they will receive, and at least one system is accredited to provide appropriate separation for the information being transferred.

e. Any IS connected to another system that does not meet either d (2) or d (3) above shall utilize a Controlled Interface(s) (CI) that performs the following:

(1) A communication of lower classification level from within the system perimeter shall be reviewed for classification before being released.

(2) A classified communication from within the system perimeter shall have the body and attachments of the communication encrypted with the appropriate level of encryption for the information, transmission medium, and target system.

(3) Communications from outside the system perimeter shall have an authorized user as the addressee (i.e., the CI shall notify the user of the communication and forward the communication only on request from the user). If classified information exists in the communication, it shall be encrypted with the appropriate level of encryption for the information, transmission medium, and target system.

8-701. Controlled Interface Functions.

a. The functions of the CI include:

(1) Providing a secure point of interconnection between networks, connected peripheral devices, remote terminals, or remote hosts.

(2) Providing a reliable exchange of security-related information.

(3) Filtering information in a data stream based on associated security labels for data content.

b. CIs have several characteristics including the following:

(1) There are no general users on the CI.

(2) There is no user code running on the CI.

(3) The CI provides a protected conduit for the transfer of user data.

(4) Communications from outside the perimeter of the system shall be reviewed for viruses and other malicious code.

8-702. Controlled Interface Requirements. The CI shall have the following properties:

a. Adjudicated Differences. The CI shall be implemented to monitor and enforce the protection requirements of the network and to adjudicate the differences in security policies.

b. Routing Decisions. The CI shall base its routing decisions on information that is supplied or alterable only by the SSS.

c. Restrictive Protection Requirements. The CI shall support the protection requirements of the most restrictive of the attached networks or IS.

d. User Code. The CI shall not run any user code.

e. Fail-secure. The CI shall be implemented so that all possible failures shall result in no loss of confidentiality or unacceptable exposure to loss of integrity or availability.

f. Communication Limits. The CI shall ensure that communication policies and connections that are not explicitly permitted are prohibited.

g. In general, such systems have only privileged users; i.e., system administrators and maintainers. The CI may have a large number of clients (i.e., individuals who use the CI's functional capabilities in a severely constrained way). The CI application itself will have to provide the more stringent technical protections appropriate for the system's protection level. Multiple applications do not affect the overall protection provided by the CI if each application (and the resources associated with it) is protected from unauthorized access or circumvention from other applications or users.

8-703. Assurances for CIs. Each CI shall be tested and evaluated to ensure that the CI, as implemented, can provide the separation required for the system's protection level. Specifically, the platform on which the CI runs does not necessarily have to provide the needed separation alone.

67. *Question: What requirements of the new chapter 8 apply to both Restricted FGI and NATO information?*

Answer: Generally, the requirements of the new Chapter 8 apply but to a lesser standard as they would for U.S. Confidential, Secret or Top Secret information:

- a. Accredited to the Restricted level (Section 2, NISPOM).*
- b. Users do not require a clearance except when Spanish Restricted information is resident (ISL 95L-2).*
- c. Sanitization of memory and media can be accomplished by following the “clearing” procedures identified in the clearing and sanitization matrix at <http://www.dss.mil/infoas/index.htm>.*
- d. Physical security to the IS to include all components will be one or a combination of the follow:*
 - 1. Secured in areas protected by key operated locks (5 pin tumbler locks) constructed in a manner which precludes surreptitious access.*
 - 2. Equipment protected with seals in an area that has been identified as having security in-depth. If the restricted information remains resident on the IS during periods of non-use, the IS must be accredited to meet the PL2 Confidentiality requirements.*
- e. Data transmission (paragraph 8-605a(1)(b)) within the contractor’s facility (i.e., local area network) must be encrypted using an encryption key of at least 128 bits (i.e., Data Encryption Standard (DES) or Public key/Private key products of a good commercial grade).*
- f. Data transmission (Section 7) that leaves the contractor’s facility (i.e., interconnected or unified network) must use the encryption device specified by the foreign government.*
- g. IS that process Restricted information can be connected to unclassified IS or networks provided they are connected through a Controlled Interface (paragraphs 8-701 and 8-702).*
- h. All other requirements of the May 1st Chapter 8 apply.*