DEPARTMENT OF DEFENSE • DEFENSE SECURITY SERVICE, INDUSTRIAL SECURITY PROGRAM OFFICE
1340 Braddock Place, Alexandria, VA 22314-1651

INDUSTRIAL SECURITY

LETTER

Industrial Security letters will be issued periodically to inform cleared contractors, User Agencies and DoD Activities of developments relating to industrial security. The contents of these letters are for information and clarification of existing policy and requirements. Local reproduction of these letters in their original form is authorized. Suggestions for articles to be included in future Industrial Security Letters are welcome. Articles and ideas contributed will become the property of DSS. Contractor requests for copies of the Industrial Security Letter and inquiries concerning specific information should be addressed to the cognizant DSS industrial security office.

ISL 2007-01 **October 11, 2007**

The articles in this Industrial Security Letter (ISL) all pertain to NISPOM Chapter 8, "Information System Security". This ISL: 1) reissues verbatim some articles from previous ISLs that are still current and applicable; 2) includes some previously published articles that have been modified to reflect changes in practices or procedures since their original publication; and 3) includes new articles to answer more recent questions or to provide clarification on issues pertaining to information system security policy. Articles are written in a question and answer format, and are annotated with the associated NISPOM paragraph in parentheses. Unless otherwise noted, all paragraph references refer to the NISPOM. Additional requirements for high-risk systems and data are covered in the NISPOM Supplement (NISPOMSUP). It is important to note that any security requirements imposed on contractors that are above the NISPOM baseline must be included in the contract document. This includes any DoD Information Assurance Certification and Accreditation Program (DIACAP) requirements imposed on contractors. (Note: DIACAP has superseded the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) in the Department of Defense.)

1. **Closed Areas and Open Storage Requirements incidental to IS Operations (5-306, 8-100b)**
2. **General Security versus NISPOM Requirements (8-100a, 8-400)**
3. **ISSM Appointment (8-101b)**
4. **ISSM Certification Authority (8-101b, 8-103)**
5. **ISSM Training (8-101b)**
6. **DAA Responsibilities (8-102)**
7. **IS Certification Process (8-104d, 8-614)**
8. **User ID Revalidation Requirement (8-104l, 8-303g)**

9. **IS Certification Requirements (8-201, 8-610a)**
10. **IS Relocation MOU Requirement (8-202, 8-610)**
11. **IS Accreditation Tracking Requirement (8-202c, 8-202d, 8-202e, 8-202f))**
12. **MFO MSSP (8-202g)**
13. **MSSP for Multiple PLs (8-202g)**
14. **Parameters for ISSM Self Certification (8-202g)**
15. **DSS Notification of ISSM Certified IS (8-201, 8-202, 8-202g(3))**
16. **Memory and Media Sanitization and Clearing Requirement (8-301a, 8-501)**
17. **Unclassified Software Review Process (8-302a)**
18. **Periods Processing Software Review Requirements (8-302a)**
19. **Contractor PCL Requirements for COTs or SR Software Testing on IS (8-105a, 8-302a)**
20. **Use of COTS or SR Software for Hardware Disconnect or IS Configuration (8-302a)**
21. **CSA Trusted Download Process – Media Review (8-302a, 8-305, 8-306b, 8-309, 8-310a, 8-401, 8-610a (1) (c))**
22. **BIOS Passwords Requirements (8-303i)**
23. **Security Controls for LAN, Standalone IS (8-303c)**
24. **Area Requirements for LAN, Standalone Security Requirements (8-303c)**
25. **Password Generation Requirements (8-303i(3))**
26. **Maintenance Procedures Requirements for Operating Systems (8-304b(4))**
27. **Malicious Code (8-305)**
28. **NISPOM Labeling Requirements (8-306a)**
29. **Marking Requirements for Media in Co-Located (Mixed) Environment (8-306c)**
30. **Hardware Integrity Requirements (8-308a)**
31. **Boundary of DSS Classified Processing Area (8-308b)**
32. **OS/Application Software Requirements for Configuration Management (8-311)**
33. **Security Requirements for High Risk IS and Data (8-400, 8-100c)**
34. **Technical Security Requirements for Special Category System's Platforms and Applications (8-500, 8-503b)**
35. **Definition of Single User Standalone IS (8-501)**
36. **Booting IS from Floppy Drive or CD ROM (8-502)**
37. **CSA Audit Log Requirements – Manual Logging (8-502e)**

38. Special Category Systems Platform Protection Level (PL) Requirements (8-503b)

39. Pure Server Security (8-503b)

40. Security Requirements for Tactical and Embedded Systems (8-504)

41. NISPOM Auditing Requirements (8-602, 8-500)

42. Audit Requirements for Security Relevant Activities (8-602)

43. Audit Record Retention (8-602)

44. SRO Auditing Requirements by Protection Level (PL) (8-602a)

45. SRO Examples (8-602a(1)(c))

46. Authenticator Change History Requirements (8-607b(f))

47. Authentication Requirements for Privileged Users (8-607c)

48. User In-activity Procedures (8-609b(2))

49. ISSM IS Assurance Requirements (8-614a)

50. Security Requirements – Interconnected WANs Multiple Programs (8-700)

51. Controlled Interface – High Assurance Guard (8-700, 8-701)

52. Technical Security Requirements for Interconnected Systems (8-700d)

53. Controlled Interface Security Requirements (8-700d)

54. DSS Clearing and Sanitization Matrix (5-704, 5-705, 8-103f, 8-301)

1. (5-306, 8-100b) Must classified materials incidental to the operation of Information Systems (IS) maintained in the Closed Area be stored in GSA approved containers?

Answer: Classified material, which includes magnetic and electronic media as well as printed materials, are normally to be stored in approved security containers within the Closed Area during non-working hours or when the area is unattended unless the area has been approved for open shelf or bin storage in accordance with NISPOM paragraph 5-306b. Large items essential to the operation of an IS do not need to be secured in approved security containers in the Closed Area, provided all personnel with access to the Closed Area have the clearance and need-to-know for all classified information within the Closed Area. Examples of items that do not need to be stored in security containers inside the Closed Area include large removable hard drives that are not easily disconnected from the IS or physically moved, or can be damaged by constant removal, or other media and technical manuals that need to be readily accessible for ongoing classified processing.

2. (8-100a, 8-400) NISPOM 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. Is paragraph 8-100a a statement of general security concerns or is it a National Industrial Security Program Operating Manual (NISPOM) requirement?

Answer: Paragraph 8-100a states a baseline standard. As stated in paragraph 8-400, the Government Contracting Activity (GCA)) will issue additional guidance or requirements if there is a need for data integrity and system availability controls.

3. (8-101b) Must the Information Systems Security Manager (ISSM) be an employee of the contractor?

Answer: Yes, the ISSM must be an employee of the contractor. Under certain circumstances (e.g., the corporate family operates in the same fashion as a multiple facility organization) and subject to DSS approval, the ISSM may be an employee of another cleared entity within the contractor's corporate family.

4. (8-101b, 8-103) In a multiple facility organization (MFO), can an ISSM who has been granted self-certification authority self-certify systems across the MFO structure?

Answer: The ISSM who has been granted self-certification authority for like systems under approved Master System Security Plans (MSSP) may self-certify systems for those facilities where he or she has been designated as the ISSM. Within an MFO, contractor management can appoint an employee to serve as the ISSM for multiple facilities if the following conditions are met:

- Facilities are in close proximity to, or within a reasonable commuting distance from, the ISSM's duty station (Note: DSS will consider exceptions to this reasonable distance criteria on a case by case basis. Such requests must specify how the ISSM will carry out oversight and other responsibilities from afar).
- The aggregate complexity of the collective facilities is such that only one ISSM is required.
- The ISSM is trained to a level commensurate with the overall complexity of all facilities.
- Each facility has at least one appointed Information System Security Officer (ISSO) who has been assigned the duties identified in paragraph 8-104.

There are no restrictions on an experienced ISSM assisting another ISSM in a different geographical location but the local ISSM is responsible for the local system and must meet the requirements for self-certification. Emergency situations will be reviewed by DSS on a case-by-case basis.

5. (8-101b) What training should the ISSM receive and how will management ensure the requirement is met?

Answer: Contractor management is required to ensure that the ISSM is trained commensurate with the complexity of the systems managed. Contractors should take advantage of available courses such as the Defense Security Service (DSS) Academy NISPOM Chapter 8 Implementation Course to train the ISSM. The ISSM can also arrange to take any recognized or government agency IS security courses.

6. (8-102) NISPOM paragraph 8-102 states the Cognizant Security Agency (CSA) is the Designated Approving Authority (DAA) responsible for accrediting IS used to process classified information. Can you elaborate on the responsibilities of the DAA position?

Answer: Within the National Industrial Security Program (NISP), the DAA is the government official with the authority to formally accredit operation of the contractor's IS for processing classified information. The DAA determines that the protection measures the contractor has identified in their System Security Plan (SSP) will effectively protect classified information. The DSS ODAA is the DAA for IS used to process classified information in cleared contractor facilities under DSS cognizance.

7. (8-104d, 8-614) Paragraph 8-104d requires that an IS certification test be developed and implemented. What is a certification test and when would it be required?

Answer: A certification test or process outlines the inspection and test procedures used to demonstrate compliance with the security requirements associated with the Protection Level (PL) assigned to the IS. The certification test is administered during the certification process and verifies correct operation of the protection measures in the IS. When the ISSM signs the Certification Test, he/she is affirming in writing that the system is currently installed and configured as described in the SSP. The DSS accreditation decision relies heavily on the accuracy of the ISSM's certification.

8. (8-104l, 8-303g) These paragraphs 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 (LAN) since user IDs are not required?

Answer: Yes, users of standalone workstations and LANs must be validated at least annually to verify that all users have a continued need to access the accredited IS. Access control lists (i.e., physical access) may be used if the IS does not require User IDs under 8-303c. If access control lists are used for revalidation, then the access control lists must be retained as an Audit 1 requirement as well as clearly identified in the system security plans. An on-going account management program is one of the basic tenets of IS security.

9. (8-201, 8-610a) These paragraphs requires the ISSM to certify that their IS have undergone a comprehensive evaluation of all technical and non-technical security features and safeguards. Is this all that is required for certification?

Answer: For the ISSM's certification, yes. However, to make such a certification, the ISSM must ensure that all other NISPOM required signatures identified in 8-610a as a Doc 1 requirement have been included. In addition, DSS can require an on-site validation of the ISSM's certification prior to the final accreditation of the system.

10. (8-202, 8-610) Is a Memorandum of Understanding (MOU) required when accredited mobile systems are relocated to government activities or test sites?

Answer: The contractor must have a signed letter from the GCA acknowledging acceptance of the relocation of the IS to the Government Activity prior to shipment. An MOU is not necessary unless the mobile system is connecting to an accredited government system.

11. (8-202c, 8-202d, 8-202e, 8-202f) Who is responsible for re-evaluating the IS, tracking the IATO and requesting re-accreditation prior to the end of the three (3) year Approval to Operate (ATO)?

Answer: Expiration, withdrawal or invalidation of an accreditation are all events that mean the affected IS is not authorized to process classified information. It is the ISSM's responsibility to:

a) Track and prepare for the expiration of the IATO.

b) Track and prepare for the expiration of the three (3) year ATO.

c) Track changes to the IS for compliance with the proposed SSP for the IATO.

d) Re-evaluate each IS for changes that would require re-accreditation (paragraph 8-202b).

e) Contact the DSS ODAA prior to the ATO accreditation expiration and notify the ODAA as to whether or not changes have been made to the IS.

12. (8-202g) Can one Master SSP (MSSP) cover multiple cleared facilities?

Answer: No. While many elements of an MSSP may be the same (for similar IS), each MSSP must be tailored to the unique circumstances of each cleared facility.

13. (8-202g) Can one MSSP be written that covers all IS within the contractor's facility that operate at PL 1 and PL 2?

Answer: No. Paragraph 8-202g states that the IS covered by a single MSSP must have equivalent operational environments, and PL1 and PL2 are distinct operational environments.

14. (8-201, 8-202) What are the parameters for self-certification by a contractor?

The certification and accreditation processes are discussed in NISPOM paragraphs 8-201 and 8-202, respectively. The following discussion is an effort to make clear how DSS applies these terms.

Certification is the attestation by a contractor that comprehensive technical and non-technical system security controls are established and operating in conformity to a specified set of NISPOM security requirements. Certification of an IS is performed by the contractor in order to achieve accreditation from the Government.

Accreditation is the official governmental action performed by the DSS ODAA to permit an IS to operate at an acceptable risk level within a specified environment. Accreditation is issued after the contractor provides a certification that security controls are in place and operating as intended. All IS certifications shall be reviewed and IS accredited to operate by DSS (ODAA).

Self-Certification

Certification and accreditation of similar systems, commonly referred to as self-certification, is discussed in NISPOM paragraph 8-202g. When specifically authorized in writing by DSS, an ISSM

may extend an existing DSS accreditation to (i.e., self-certify) similar systems. ISSMs may self-certify similar systems only within specified parameters.

The general rules and parameters for self-certification are:

a) Self-certification must be based on a DSS-approved Master System Security Plan (MSSP). WANs and WAN interconnections (adding a node to a Network Security Plan) cannot be self-certified.

b) Any self certified system must be in compliance with applicable NISPOM requirements.

c) If a contractor is uncertain of the self-certification authority granted to them by DSS, the contractor should consult with DSS ODAA about the extent of their authority.

d) All required documentation for self-certified systems must be readily available for DSS review as detailed in the DSS ODAA Process Guide.

e) Self-certification authority is granted by DSS to a specific person at a particular CAGE Code in the Approval to Operate (ATO) letter. Self-certification of systems outside of the CAGE Code specified in the ATO is not permitted.

The following table provides parameters governing self-certification by industry under a DSS-approved MSSP.

Table for self-certification
(most common parameters)

	Protection Level (PL) (Note: 1)	Level of Concern (Note: 2)	Physical (Note: 3)	Operating Systems (OS) (Note: 4)	System Type (Note: 5)	Trusted Downloading Procedures (Note: 6)	Periods Processing (Note: 7)	Mobile Systems/ Alt Site (Note: 8)	Test Equipment (Note: 9)
Required to be considered "similar"	☒	☒	☒	☒	☒	☒	☒	☒	☒

Note: 1 - MSSP can consist of systems at PL-1 or PL-2, but not both.
Note: 2 – Level of Concern (NISPOM 8-401) must be the same. This refers to the classification levels of information (Top Secret, Secret, and Confidential)
Note: 3 – Physical. This pertains to the physical security environment (most notably restricted areas and closed areas). Be mindful that there are many scenarios that could describe a restricted area. Therefore, if the scenarios are not similar the IS will not be self-certified. In this case a reaccreditation of the MSSP would be required to include the additional scenario. There are hybrids (i.e. A LAN that encompasses closed and restricted areas) but are generally the exception rather than the rule.
Note: 4 - Only approved OS can be used for subsequent self-certified systems. However, a new OS can be added to an approved Protection Profile provided it's been previously approved by ODAA under another Protection Profile or Master Plan. In addition, any OS version changes may not be self-certified if the new version changes an approved existing security configuration. For clarification please check with ODAA for determination.

Note: 5 - System Type generally refers to system architecture: For example, Multi-user standalones (MUSA) or LANs. It can also refer how an IS is used. A Windows 2003 Server can be used as a Domain Controller (which controls half the (I&A) "handshake" and requires all technical security features to be enabled) or as a file server (which can be recognized as a pure server in some instances which doesn't require all technical security features to be enabled).
Note: 6 - TDP (Trusted Downloading Procedures). Only the DSS approved procedures can be considered for self-certification.
Note: 7 – Periods Processing (NISPOM 8-502). 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).
Note: 8 – Mobile Systems. Procedures for identifying, managing and protecting mobile systems must be similar for DSS to consider approving self-certification.
Note: 9 – Test equipment can only be self-certified if it is the same make and model as another device that has been previously accredited by DSS.

15. (8-202g(3)) Paragraph 8-202g(3) requires the ISSM to certify additional IS under an MSSP but does not require notification to DSS. Should DSS be notified?

Answer: Yes. It's imperative that DSS have up-to-date knowledge and awareness of all accredited IS processing classified information. At a minimum, the contractor shall provide an updated list of IS self-certified under an MSSP to the IS Rep and ISSP on a quarterly basis. If the IS Rep or ISSP determines that more frequent notification is necessary because of volume or complexity or to address specific security concerns, the IS Rep or ISSP can request more frequent notification.

16. (8-301a, 8-501) Can DSS provide more guidance on when sanitization or clearing of memory and media is required?

Answer: Sanitization of memory and media is required when the memory or media is no longer needed to store classified information. Clearing is required before and after periods of processing as a method of ensuring need-to-know protection, and prior to maintenance. Clearing is all that is required when the memory or media will be used at a higher classification level or at a more restrictive information sensitivity level. The clearing and sanitization matrix is available on the DSS web site. Users unable to access the matrix should contact their local DSS Industrial Security Representative.

17. (8-302a) What does an unclassified software review and/or testing encompass?

Answer: Paragraph 8-302a provides two options for examination of unclassified software prior to its introduction into the IS and use for classified processing. The contractor may choose either a review or testing of the unclassified software. An unclassified software review must be a line-by-line source code review. Unclassified software testing must include a verification of all functionality for security-relevant items (e.g., includes security relevant software such as all OS software on an IS where Identification and Authentication(I&A) and/or auditing have been technically implemented, virus and malicious code detection and sanitization software, all security relevant information such as software and router tables, configuration settings, IS and OS documentation, audit data, etc. Security relevant hardware includes any hardware or IS component that contains, or has the potential of containing

classified information) as well as resolution of any discrepancies. For example, if the software writes to a file, the file must then be reviewed using a hexadecimal editor to ensure that only the intended information was written.

18. (8-302a) What are the review requirements for 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 must either be developed by cleared, knowledgeable personnel or reviewed and/or tested by cleared, knowledgeable personnel. The review and/or testing is done to provide reasonable assurance that security vulnerabilities do not exist.

19. (8-105a, 8-302a) Are contractor employees who test commercially procured or security related software on an accredited classified system or a system in development that will process classified information required to have a clearance?

Answer: Yes. They are "privileged users" and require a security clearance at least equal to the level at which the IS is accredited.

20. (8-302a) Can commercially procured or security related software be used to disconnect hardware components not used for classified processing or to configure the IS for a classified processing session?

Answer: Yes. Provided the IS is not accredited at the level of TOP SECRET and the procured security related software has been tested and operates as specified.

21. (8 -302a, 8-305, 8-306b, 8-309, 8-310a, b, 8-401, 8-610a (1)c)) Can DSS provide additional guidance on the trusted download process and the requirement for output and media review?

Answer: Yes, Due to the diversity and uniqueness of the numerous vendor platforms and applications in use (e.g., word processing, database, electronic mail, and spreadsheets), a thorough review by the ISSM and DSS must be conducted before the trusted downloading procedures are used to create classified or unclassified electronic files and/or media.

All trusted downloading procedures must use new media. This mitigates the possibility of classified system contamination or corruption, as used media could contain and inadvertently introduce unauthorized software into the classified system.

The DSS Trusted Downloading Procedures can be found on the DSS web site (www.dss.mil) under the Industrial Security Program link. These procedures support many of the standard applications and can be used to examine information that is not in human readable form with the reasonable assurance that only the requested information was transferred.

If the ISSM is unable to implement the DSS procedures found on the DSS website, the System Security Plan (SSP) must (under the vulnerability reporting requirement of paragraph 8-610a(1)(c)) include a

description of how and why the contractor has deviated from the standard, and a risk acceptance statement by the GCA. .

Trusted Downloading Procedures do not need to be followed when classified information is transferred from an accredited PL 1 system storing the same level of classified information from multiple programs to media that will be handled and then remain at the same or higher level classified environment and controls (i.e., handling, marking, distribution/access controls, safeguarding, etc.). However, a review must be accomplished to ensure that only the designated files were transferred to the new media. This could include a review of hard copy output and/or a visual review of the electronic file.

22. (8-303i) Must BIOS Passwords meet the same NISPOM requirements as authenticator passwords?

Answer: Yes, BIOS passwords must meet the NISPOM length and complexity requirements. A waiver is not required if a system's BIOS passwords cannot be configured to meet the NISPOM requirement. However, a waiver must be requested if the system's BIOS cannot be password protected for operational reasons. BIOS passwords are not deemed user authenticators and need not be changed annually.

23. (8-303c) This paragraph permits physical security controls and personnel security controls to augment the logon authentication requirement for standalone workstations or local area networks (LANs). What types of personnel security controls are acceptable?

Answer: The ISSM/ISSO must ensure that all users meet clearance, formal access approval, and need-to-know requirements. GCA concurrence is required when technical logon controls (i.e., identification and authentication) are not established. These personnel controls are acceptable to meet or augment the logon authentication requirements for those systems. Once briefed, the users' names should be added to the area access list or the equipment authorization list which authenticates that the users are authorized and briefed.

24. (8-303c) This paragraph permits physical security and personnel security controls in place of logon authenticators for small local area networks (LANs). Does "small" refer to the number of workstations or the area in which the workstations reside?

Answer: "Small" refers to size of the area in which the workstations are located. The users and systems should be easily observable by the ISSO (e.g., within the same room, group of cubicles, adjoining offices in close proximity to each other).

25. (8-303i (3)) What method(s) of password generation will DSS approve?

Answer: The recommended method of password generation is for the IS to generate unique, random passwords. User-generated passwords are permitted, but must be a minimum of eight characters that are a mix of alpha/numeric and upper/lower case characters. Users shall be briefed not to use dictionary definable words for passwords that include sport names, pets or family members. The SSP must address the password generation method, and whether the password is unique and random.

26. (8-304b(4)) This paragraph states that a separate copy of the operating system must be 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 performing maintenance must use a separate copy of the operating system and any maintenance software. As an exception, the ISSM may consider using alternate maintenance procedures for remote maintenance by contractors in accordance with the SSP using an on-line operating system.

27. (8-305, 8-103f(5)) What are the NISPOM security requirements for protection against malicious code in IS?

Answer: NISPOM requires that all IS, regardless of the OS, are protected against malicious code. The ISSM must implement policies and procedures that detect and deter incidents caused by malicious code, viruses, intruders, or unauthorized modifications to software or hardware. The IS must employ the appropriate software to check all files for viruses and malicious code before being introduced on an IS.

28. (8-306a) Are external color-coded labels required per paragraph 8-306a?

Answer: No, the NISPOM does not require color-coded labels to indicate classification level.

29. (8-306c) This paragraph requires that unclassified media be marked when classified and unclassified IS are collocated. Since the DSS approved area can range in size and structure (e.g., from a small office cubicle to a multi-story building) can DSS provide additional guidance?

Answer: Externally marking media when classified and unclassified IS are collocated clearly communicates and distinguishes the classification level of the media. The ISSM/ISSO must establish well-defined perimeters for the classified IS. These perimeters not only set apart 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 must be marked and protected accordingly. Writeable media not in the classified IS area that is unmarked is considered unclassified unless circumstances dictate a conclusion that the material is in fact classified.

30. (8-308a) How is hardware integrity of an IS maintained?

Answer: Hardware integrity 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 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.

31. (8-308b) What is the boundary of the DSS approved area for classified processing?

Answer: The physical boundary of the DSS approved area for classified processing is limited to the area within which authorized contractor personnel can exercise constant surveillance and maintain control of the IS. The area must have an identifiable boundary (e.g., walls, signs, tape on floor, rope or chains, etc.) 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.

32. (8-311) Do operating system (OS) and application software need to be updated?

Answer: Yes. Patch management (e.g., installation of system software updates) is an important aspect of configuration management, which is in turn crucial in preventing malicious code from infecting an IS and its data.

33. (8-400, 8-100c) NISPOM 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? What are the security requirements for contractors who need to develop systems at PL 4?

Answer: A high-risk system is one that requires protection above the NISPOM baseline (i.e., multi-level) where high-risk data would be Special Access Program (SAP) or Special Compartment Information (SCI) information. Standards for SAP and SCI are typically established in contract documents by the responsible GCA.

34. (8-500, 8-503b) Why are the Chapter 8 technical security requirements different for the platforms of Special Category systems (such as guards and servers) than for applications of the Special Category guards or servers?

Answer: Special category systems do not require all the technical features and safeguards of Chapter 8 to be adequately secured. The application running on a guard or server is viewed separately from the hardware and OS platform. The platform of the guard or pure server may be at a PL lower than the PL associated with the application(s) due to its large number of users. The guard or pure server application itself must provide the more stringent technical protections appropriate to the systems' PL and operational environment.

35. (8-501) Can an IS that is used by more than one person be considered a single user standalone IS?

Answer: A single user standalone IS is defined as an IS physically and electronically isolated from all other systems and is intended for use by one person only, e.g., a laptop assigned to one person, a personal computer assigned to one individual. An IS with more than one user will be considered a single user standalone if each user of the IS has an individually assigned removable hard drive and the

system is sanitized between users. Information Technology support personnel are not considered users of single user standalone systems.

36. (8-502) Can an IS being upgraded to process classified information be booted from a floppy disk or CD-ROM?

Answer: Yes, provided the floppy disk or CD ROM is protected to the level of the IS and is used in a read-only configuration. However, DSS recommends that classified IS be configured to boot only from specific hard drives to minimize the possibility of security controls being circumvented by external media.

37. (8-502e) Paragraph 8-502e states that the CSA shall consider manual logging for multiple user systems that are not capable of automated logging. Does the NISPOM require manual logging, and if so, can access lists be used for validation purposes?

Answer: As provided for in 8-502e, DSS requires manual logging when automated logging cannot be accomplished. DSS can approve alternate procedures for accountability of user activities on an IS that mitigate risk to an acceptable level. Manual logs and access control lists (i.e., physical assess) can be used for validation purposes and shall be retained as an Audit 1 requirement.

38. (8-503b) Paragraph 8-503b states that the platform on which the guard or server runs usually needs to meet no more than Protection Level (PL) 3 security requirements. Is this correct since Chapter 8 only has 3 PLs?

Answer: Yes, the platform on which the guard or server runs usually must meet no more than PL 3 requirements, given that PL3 represents the most stringent protection requirements identified in Chapter 8. However, a higher PL specified in a more stringent standard (e.g., DCID 6-3) may be imposed by contract. Table 5, Protection Profile for Confidentiality (NISPOM Chapter 8, Section 4) illustrates a matrix of eleven (11) graded protection requirements for the three (3) PLs. The platform's set of graded protection requirements will depend on the confidentiality PL and the level of concern (high, medium, and basic) for the data being processed or stored. The platform is not restricted to a single PL for all 11 requirements; for example, the platform may have an access requirement of PL3 but an auditing requirement of PL1.

39. (8-503b) Do "pure servers" (e.g., guard, proxy server, application server) require accreditation separate from the general-purpose computers they support or are connected to?

Answer: Normally the only "pure server" that requires separate accreditation is a guard. The guard requires more stringent technical protection and assurance than the IS it protects by the very nature of its function. The other types of "pure servers" can be described and included in the general-purpose computer SSP.

40. (8-504) What security requirements apply to systems that are tactical and/or embedded as an integral element of a larger system?

Answer. DSS has been receiving questions as to what security requirements apply to systems that are embedded as an integral element of a larger system (NISPOM 8-504). The following guidance is provided:

While certain types and configurations of equipment or components fit the definition of an information system[1] (IS) requiring accreditation, others may not. The Information System Security Manager (ISSM) will determine and document the capabilities of such equipment to collect and process classified information. As a general rule, equipment composed of volatile memory with no other storage media (such as test equipment) does not require accreditation.

Security requirements for information systems that are embedded as an integral element of a larger system that is used to perform or control a specific function (such as control systems or weapons systems) should be established by the Government Contracting Activity (GCA) concurrently with the design and development of the system. If the GCA has not provided those requirements, the contractor shall request them from the GCA. Regardless of the existence of guidance from the GCA, these systems will not require Cognizant Security Agency (CSA) accreditation. However, if GCA security requirements are not provided, the contractor will be required to submit classified processing procedures to the CSA that describe the security requirements and procedures implemented that protect the embedded system and classified information against unauthorized disclosure or loss.

41. (8-602, 8-500) If an IS is capable of auditing, must the contractor enable this feature?

Answer. Yes. The contractors must make every effort to meet NISPOM Chapter 8 auditing requirements, to include upgrading their operating system as appropriate and/or obtaining third party software, if necessary. However, an exception to this requirement may be invoked in situations where a GCA certifies one or more of the following:

a) The contractor is required to use an OS that is not capable of meeting Chapter 8 audit requirements;

b) Enabling auditing on a legacy OS will result in unnecessary costs, operational impacts, or deviation from the secure deployed operating environment; or,

c) The IS is a Special Category System, meets NISPOM 8-500 requirements and can be adequately secured without all Chapter 8 technical requirements being implemented.

In these three instances, a NISPOM waiver is not required. Contract documentation from the GCA, such as the DD Form 254, formal classification guidance and/or a formal memorandum that clearly cites one or more of the circumstances cited above must be provided to DSS. A suggested format is a statement such as, "the contractor is required to use Windows 98," followed by the rationale for its use. The statement must be signed by the Contracting Officer, the Contracting Officer's Representative (COR) or the Contracting Officer's Technical Representative (COTR), or the Government Program Manager. A formal contract modification is not necessary.

42. (8-602) What security relevant activities should be recorded for all PLs and all Special Category IS?

Answer: Security relevant activities are those identified in Paragraph 8-602 audit requirements 1-4 that identify IS security relevant activities normally captured by an automated audit capability for all PLs and those Special Category Systems that have the capability to do so without adverse impact on operations. 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 un-cleared 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).

43. (8-602) How long should audit records be retained?

Answer: Audit records must be retained covering the previous 12 months.

44. (8-602a) Can DSS provide clarification on the NISPOM Paragraph 8-602 auditing requirements for Security Relevant Object (SRO)?

Answer. The following chart identifies auditing requirements by type of Security Relevant Object (SRO), protection level and whether the attempt to access the SRO was successful or not. For example, only unsuccessful attempts to access operating system executables are required to be audited at the PL-1 level. Auditing scripts and a list of security relevant objects for use by contractors are on the DSS web site (www.dss.mil) under "ODAA Tools".

Security Relevant Object (SRO)	PL-1	PL-2	PL-3	PL-4 NISPOMSUP
Operating system executables	U	U	S, U	S, U
Operating system configuration	U	U	S, U	S, U
System management and maintenance executables	U	U	S, U	S, U
Audit data	U	U	S, U	S, U
Security related software	U	U	S, U	S, U
User files, classified data	(no auditing)	U	S, U	S, U

S-Successful U-Unsuccessful

45. (8-602a (1) (c)) This paragraph requires the auditing of security relevant objects (SRO) and directories. Can DSS provide clarification on OS configuration and location of SRO?

Answer. All OS contain SRO and directories but the location (folder or directory) and the OS configuration may vary with the OS. The following table represents a standard configuration of SRO to be audited for Windows NT and UNIX. Please note that while the SRO and directories will remain constant, directory examples can vary by installation, by administrator and by OS.

Security Relevant Objects (SRO)	Directory Examples (can vary by installation)	
	Windows	Unix
Operating system executables	Refer to the Security Relevant Objects list located under "ODAA Tools" on the DSS web site (www.dss.mil).	/bin and /usr/bin
Operating system configuration		/etc
System management and maintenance executables		/etc, /sbin, /usr/sbin
Audit data	C:\WINNT\system32\config	/var/audit
Security related software	C:\Program files\NispUtilities	/usr/local or /opt
User files/classified data beginning at PL-2	C:\Profiles or C:\Documents and Settings	/home

46. (8-607b (f)). This paragraph 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 must document this as a unique vulnerability and describe compensating measures in the applicable SSP as required by paragraph 8- 610a (1).

47. (8-607c). This paragraph requires "strong authentication" for privileged users that are either located or communicate outside the IS perimeter. In the context of the NISPOM, what constitutes "strong authentication?"

Answer: Strong authentication techniques provide countermeasures against common authentication attacks. This includes the use of cryptographic technologies (e.g., two factor tamper resistant hardware or software token authentication, digital signatures, etc.), one-time passwords, or biometric devices (retina, fingerprint, hand geometry, retina identification, etc.).

Consideration should be given to the use of a combination of technical (anomaly detection/prevention technologies, use of secure communication channels to mitigate eavesdropping, replay and session hijacking attacks) and non-technical measures (user education, enrollment procedures, authentication key management, etc.).

48. (8-609b (2)) What is the baseline time period of user inactivity and what procedures are required?

Answer: Users will be required to re-authenticate themselves (e.g., reenter password) after 15 minutes of user inactivity. 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 because of mission requirements, the GCA may

accept this risk in a letter to the contractor. The ISSM will document this as a unique vulnerability in the applicable SSP as required by paragraph 8-610a(1)(c).

49. (8-614a) What is the difference between Paragraph 8-614a, which requires the ISSM provide "assurance" and paragraph 8- 614b where the ISSM is required to provide "written assurance"?

Answer: The assurance the ISSM provides under paragraph 8-614a Test 1 is a statement in the SSP that the security features, including access controls and configuration management, are implemented and operational. Under paragraph 8-614b Test 2 requirement, the ISSM provides written assurance to the CSA that the IS operates in accordance with the approved SSP and the individual verification that each of the requirements of Table 5 for technical security features and safeguards has been implemented and is operational to include access controls, configuration management and discretionary access controls.

50. (8-700) What are the overall PL2 network security requirements for interconnected Wide Area Networks (WAN) involving different classified programs, multiple contractor facilities, (i.e. individual nodes) under different need to know criteria?

Answer: Network security requirements for multiple nodes connected to a WAN are determined by the overall WAN DAA. The WAN DAA will determine the certification testing requirements for the WAN and individual nodes. The WAN DAA may determine that the combination of data and/or users on the interconnected network requires a higher PL than those of its nodes. Security requirements for these networks will address the following minimum requirements:

a) Each interconnected WAN node must be separately accredited and maintain its individual accreditation. All WAN nodes must be issued an Approval To Connect (ATC) by the WAN DAA before connecting to the WAN.

b) An approved overall Network Security Plan (NSP) and Network Protection Profile (NPP). The NSP and NPP are maintained and updated to reflect changes, topography, connections, new technologies and new Operating Systems as required.

c) When a connection to a government system is involved, the WAN DAA shall require the establishment of an MOU to document the need for the connection, connection requirements, all required approvals, and the certification and accreditation (C&A) roles and responsibilities of all WAN participants.

d) Each separately accredited system or network will maintain its own intra-system services and controls and protects its own resources.

e) Each participating system or network must have its own ISSO.

f) Utilization of a Controlled Interface (CI) to provide a protected conduit for the transfer of user data. The CI must be capable of adjudicating the different security policy implementations of the participating systems or unified networks, and must support the required protection requirements of the most restrictive attached WAN nodes.

51. (8-700, 8-701) 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" (HAG) and "Controlled Interface" (CI) interchangeable?

Answer: No, there is some difference between these terms. The HAG is comprised of hardware and software that enforces the established security rules during transmission of message and directory traffic between enclaves of different classification levels. The CI is a mechanism that can actually adjudicate the different interconnected security policies (controls the flow of information in and out of the interconnected systems).

52. (8-700d) This paragraph 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: The technical security features, safeguards and assurances for interconnected systems or networks require the use of a Controlled Interface (CI). The CI must have been evaluated and been found to meet the Evaluation Assurance Level 6 (EAL 6) level of trust under the National Information Assurance Partnership (NIAP) - NSA and National Institute of Standards and Technology (NIST) Common Criteria Evaluation and Validation Scheme (CCEVS).

The EAL 6 evaluations are a semiformal verification and testing of the IS eleven (11) standard categories of functional requirements and ten (10) categories of assurance requirements. The functional requirements include identification and authentication, protection of security functions, security management, privacy, user data protection (access control, information flow, etc.), communication protection (encryption, Public Key Information (PKI), non-repudiation, confidentiality, security audit, resource utilization, fault tolerance, etc.). The 10 assurance requirements are a Protection Profile (PP) evaluation, Security Target (ST) evaluation, configuration management, development, test, delivery/operation, life cycle, guidance documents, vulnerability assessment, and maintenance of assurance requirements. EAL-6 corresponds roughly to the DoD (Trusted Computer System Evaluation Criteria (TCSEC) B3 level of trust functional and assurance requirements.

More information on the CCEVS can be found at URL: http://www.niap-ccevs.org/cc-scheme/.

53. (8-700d) Must the contractor use a Controlled Interface (CI) from the SECRET and Below Interoperability (SABI) Program when networks belonging only to contractors are interconnected at different classification levels or different compartments?

Answer: No. The contractor must use a CI meeting the DISA Global Information Assurance Program (GIAP) Cross Domain Solutions (CDS) Program requirements, which replaced the SABI connections process. For more information on DISA's CDS requirements, go to http://iase.disa.mil/index2.html or directly to CDS at: http://iase.disa.mil/cds/index.html.

54. Can DSS provide guidance on the clearing and sanitization requirements for classified material no longer required? (5-704, 5-705, 8-103f, 8-301)?

Answer. Yes, DSS has published the following updated DSS Clearing and Sanitization Matrix on the DSS web site (www.dss.mil) under the Industrial Security Program tab.

DSS Clearing and Sanitization Matrix
(Updated June 28, 2007)

NISPOM paragraphs 5-704 and 5-705 set out requirements for the destruction of classified material that is no longer required, including media, memory, and equipment. The appropriate procedure to be used is based on the classification sensitivity of the information and the type (size, capacity and coercivity) of the media. There is currently no overwriting product or process that has been evaluated in accordance with the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS).

Therefore, in accordance with NISPOM paragraph 8-301, DSS will apply the guidance in the NSA CSS Policy Manual 9-12, "NSA/CSS Storage Device Declassification Manual", dated 13 Mar 2006, to sanitization, declassification, and release of IS storage devices for disposal or recycling. Effective immediately, DSS will no longer approve overwriting procedures for the sanitization or downgrading (e.g. release to lower level classified information controls) of IS storage devices (e.g., hard drives) used for classified processing.

The matrix provides guidance regarding clearance, sanitization (destruction) and disposition of the most common media, memory and equipment used for classified processing.

Clearing and Sanitization Matrix[1]

Media	Clear					Sanitize														
Magnetic Tape																				
Type I	a						b									l				
Type II	a						b									l				
Type III	a						b									l				
Magnetic Disk																				
Bernoullis	a	c					b									l				
Floppy	a	c					b									l				
Non-Removable Rigid Disk		c				a										l				
Removable Rigid Disk	a	c				a										l				
Optical Disk																				
Read Many, Write Many		c														l				

[1] In addition, NIST Special Publication 800-88, Guidelines for Media Sanitization, dated Sep 2006, can assist organizations and system owners in making practical sanitization decisions based on the level of confidentiality of their information, ensuring cost effective security management of their IT resources, and mitigate the risk of unauthorized disclosure of information.

Read Only																	l	m				
Write Once, Read Many (Worm)																	l	m				
Memory																						
Dynamic Random Access Memory (DRAM)		c	g					c					g				l					
Electronically Alterable Programmable Read Only Memory (EAPROM)				h											i		l					
Electronically Erasable PROM (EEPROM)				h							f						l					
Erasable Programmable ROM (EPROM)					j			**c**								**k**	l					k then c
Flash EPROM (FEPROM)				h				**c**						**h**			l					c then h
Programmable ROM (PROM)		c															l					
Magnetic Bubble Memory		c				a		c									l					
Magnetic Core Memory		c				a			d								l					
Magnetic Plated Wire		c						**c**			**e**						l					**c and e**
Magnetic Resistive Memory		c															l					
Non-Volatile RAM (NOVRAM)		c						c									l					
Read Only Memory (ROM)																	l					
Synchronous DRAM (SDRAM)		c	g					c					g				l					
Static Random Access Memory (SRAM)		c	g					c					g				l					
Equipment																						
Monitor			g																		p	
Impact Printer			g										**g**							**o**		**o then g**
Laser Printer			g										**g**						**n**			

INSTRUCTIONS FOR READING THE MATRIX:

A letter in black in the above table indicates the procedure is a complete, single option, e.g. EEPROM sanitization: Perform either procedure g or l (refer to indices below) and the media/memory is completely sanitized. Letters in ***red*** indicate the procedures must be combined for a complete sanitization, e.g., Laser Printer sanitization**:** **n** must be performed, then **g**. Note: when a combination of two procedures is required, the far right hand column indicates the order of the procedures. e.g., **o then g**.

MATRIX INDEX:

a. Degauss with Type I, II, or III degausser.
b. Degauss with same Type (I, II, or III) degausser.
c. Overwrite all addressable locations with a single character.
d. Overwrite all addressable locations with a character, its complement, then a random character.
e. Each overwrite must reside in memory for a period longer than the classified data resided.
f. Overwrite all locations with a random pattern, then with binary zeros, and finally with binary ones.
g. Remove all power to include battery power.
h. Perform a full chip erase as per manufacturer's data sheets.
i. Perform h above, then c above, a total of three times.

j. Perform an ultraviolet erase according to manufacturer's recommendation.
k. Perform j above, but increase time by a factor of three.
l. Destruction (see below.)
m. Destruction required only if classified information is contained.
n. Run 1 page (font test acceptable) when print cycle not completed (e.g. paper jam or power failure). Dispose of output as unclassified if visual examination does not reveal any classified information.
o. Ribbons must be destroyed. Platens must be cleaned.
p. Inspect and/or test screen surface for evidence of burn-in information. If present, screen must be destroyed.

Destruction Methods for Classified Media and Equipment:

A. NISPOM Paragraph 5-705 reflects requirements for destruction of classified material, including classified media and equipment. DSS recommends methods and procedures for destroying classified media and equipment should be reflected in the System Security Plan and reviewed/approved in connection with the information system certification and accreditation process. The following summary information is provided for contractor facilities in updating system security procedures for destruction of classified media:

- Incineration is the most common and recommended method for removing recording surfaces.

- Applying an abrasive substance to completely remove the recording surface (e.g. emery wheel, disk sander, belt sander, sand blaster) from the magnetic disk or drum. Make certain that the entire recording surface has been thoroughly destroyed before disposal. Ensure proper protection from inhaling the abraded dust.

- Degaussing or destruction using government approved devices. NSA publishes guidance on the sanitization, declassification, and release of Information Systems (IS) storage devices for disposal or recycling in the NSA CSS Policy Manual 9-12, NSA/CSS Storage Device Declassification Policy Manual, dated 13 Mar 2006. It is recommended that prior to performing any process for disposal, recycling or release of storage, media, or equipment that users review the manual and/or check for any updates to the guidance. NSA publishes on a recurring basis, updated Evaluated Products Lists (EPL) for High Security Crosscut Paper Shredders, High Security Disintegrators and Optical Media Destruction Devices. Contractors may utilize NSA evaluated destruction devices for destruction of classified media and hardware without prior authorization from DSS. For use of non-NSA approved devices or procedures, prior approval of the CSA is required.

- Smelting, disintegrating, or pulverizing hard disks or drums at an approved metal destruction facility. Prior approval of the CSA is required.

- Destroying by the use of chemicals (e.g. application of concentrated hydriodic acid (55 to 58 percent solution). Chemical destruction is hazardous and should only be done by trained

personnel in a proper environment (e.g. licensed facility, well-ventilated area, safety equipment and procedures, etc.) Prior CSA approval is required.

- Due to the proliferation, wide spread use, interoperability, low cost of USB technologies throughout the Global Information Grid (GIG), USB media and equipment no longer required to store or process classified information must be destroyed.

B. The National Security Agency (NSA) Classified Material Conversion (CMC) destruction facility may be utilized by qualified and registered contractors. NSA CMC will accept all COMSEC hardware and materials (regardless of ownership), classified Government Furnished Equipment (GFE) (including media), and Special Access Program (SAP) information from contractor facilities, with the prior endorsement of a government contracting officer (CO) or contracting officer representative (COR) in accordance with NSA CMC contractor registration procedures reflected in NSA guidance "Contractor Request for NSA CDC Services". Guidance for registration for NSA destruction services is also available on the DSS website.

INDEX

A

account management....5
accreditation....5, 6, 7, 13, 14, 18, 22
application....13, 14
assurance....10, 14, 17, 18, 19
ATO....6
audit....9, 15, 16, 17, 19
authentication....11, 17, 19
availability....3, 4

C

CCEVS....19, 20
certification....4, 5, 6, 7, 18, 22
confidentiality....14, 19, 20
configuration management....18, 19
Controlled Interface....3, 18, 19
controls....4, 11, 12, 13, 18, 19, 20
Cross Domain Solutions....19

D

DAA....5, 18
DIACAP....1
DITSCAP....1
DoD....19

E

EAL....19
evaluation....5, 19

G

GCA....4, 5, 10, 11, 13, 15, 17
GIAP....19

H

HAG....19

I

IATO....6
integrity....3, 4, 12
interconnected....7, 18, 19
ISSM....1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 17, 18

L

LAN....2, 5, 8

M

maintenance....7, 9, 11, 12, 16, 17, 19
malicious code....9, 12, 13
media....3, 9, 10, 12, 14, 16, 20, 21, 22, 23
MFO....4
MOU....2, 5, 18
MSSP....2, 4, 6, 9

N

NIAP....19, 20
NISP....5
NISPOM baseline....1, 13
NISPOMSUP....1, 16
NIST....19, 20
NSA....19, 20, 22, 23

O

ODAA....5, 6, 7, 8, 16, 17

P

passwords....11, 17
Patch management....13
PKI....19
privileged users....10, 17
Profile....7, 8, 9, 14
Protection Level....3, 5, 6, 13, 14
protection measures....5

R

responsibility....6
risk....1, 10, 13, 14, 17, 20

S

sanitization....8, 9, 19, 20, 21, 22
security controls....14
Security Relevant Objects....17
security-relevant items....9
software testing....9
special category....13, 15, 16
SSP....5, 6, 10, 11, 12, 14, 17, 18

U

unclassified software review....9
USB....23

V

vulnerability....10, 17, 19

W

WAN....18