DEPARTMENT OF DEFENSE • DEFENSE SECURITY SERVICE, INDUSTRIAL SECURITY PROGRAM OFFICE

INDUSTRIAL SECURITY LETTER

Industrial Security letters will be issued periodically to inform Industry, 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 for the internal use of addressees is authorized. Suggestions and articles for inclusion in the Letter will be appreciated. Articles and ideas contributed will become the property of DSS. Contractor requests for copies of the Letter and inquiries concerning specific information should be addressed to their cognizant security office, for referral to the Industrial Security Program Office, Headquarters, DSS, as appropriate.

ISL 2006-02 **August 22, 2006**

The following previously published ISL articles are still pertinent with regard to the issuance of the revised NISPOM dated February 28, 2006 and are hereby reissued. Some have been modified slightly to account for changes in policy, practice, or procedure since their original publication. Previous ISL articles pertaining to Chapter 8, Information System Security will be reissued separately. The NISPOM paragraph to which the article pertains is indicated in ( ).

1. (1-200) Security for Wireless Devices, Services and Technologies (ISL 05L-1 #10)

2. (1-206) Security Review Ratings (ISL 04L-1 #8)

3. (1-302) Reporting Participation in Rehabilitation Programs as Adverse Information (ISL 00L-1 #3)

4. (1-301, 1-302, 1-303, 1-304) Reports Submitted to the CSA (ISL 02L-1 #9)

5. (1-303 and 4-218) Notification to Recipients Regarding the Inadvertent Dissemination of Classified as Unclassified (ISL 00L-1 #8)

6. (2-102 and 7-101) Facility Security Clearances (FCLs) for Service Contracts (ISL 05L-1 #8)

7. (2-108) Clearing Branch Offices (ISL 03L-1 #8)

8. (2-200) Personnel Security Clearances (PCLs), the Internet, and Job Seeking (ISL 03L-1 #13)

9. (2-201) Interim Access to JPAS – Based on a National Agency Check (NAC) (ISL 03L-1 #11)

10. (2-201) Fingerprint Cards Not Required for Periodic Reinvestigations (ISL 05L-1 #7)

11. (2-210) Access Limitations of an LAA

12. (2-212) PCL/FCL Requirements for Self-Employed Consultants (ISL 03L-1 #6)

13. (3-105) SF 312 Date in JPAS (ISL 05L-1 #6)

14. (3-105) Q&A – SF-312 (ISL 02L-1 #18)

15. (5-306a) Structural Integrity of Close Areas (Reissue of ISL 03L-1 #4):

16. (5-306a) Closed Areas and Open Storage (ISL 04L-1 #11)

17. (5-309b) Changing Combinations (ISL 89 L-2 Q&A)

18. (5-408 and 5-409) General Services Administration Carriers for Overnight Delivery of SECRET and CONFIDENTIAL Classified Information within the Continental United States (revised from ISL 97L-1 #7)

19. (5-902) Intrusion Detection System (IDS) Monitoring Over Data Networks (ISL 05L-1 #11)

20. (6-104) Visit Authorization Letters for the Department of Energy (DOE) (ISL 03L-1 #10)

21. (10-102) Bilateral Security Agreements (ISL96L-1 #1)

22. (10-307, 10-509 and Appendix C) Definitions of "Foreign National" and "U.S. Person, (ISL96L-1 #3)

23. (10-306) Q&A re Storage of Foreign Government Information on an Information System (ISL 05L-1)

24. (10-508c) Q&A re CSA Notification of Assignment of Foreign Nationals to US Contractor Facilities (ISL 96L-1 #33)

25. (10-508d) Q&A re Technology Control Plan (TCP) Requirement When Foreign Nationals are Assigned to US Contractor Facilities (ISL 96L-1 #34)

1. (1-200) Security for Wireless Devices, Services and Technologies (ISL 05L-1 #10)

NISPOM paragraph 1-200 states that "Contractors shall protect all classified information to which they have access or custody." Therefore, industry should implement security procedures to mitigate risks associated with wireless devices in areas where employees are working with classified information and/or where classified discussions may be held. Facility Security Officers must consider the capabilities of the wireless device and use sound judgment in developing appropriate security countermeasures. Depending on the device/technology, appropriate security countermeasures may range from ensuring a wireless device is turned off or not used in classified areas to, in some cases, not permitting the devices in the area.

2. (1-206) Security Review Ratings (ISL 04L-1 #8)

DSS assigns a security rating to contractor facilities at the conclusion of each security review. The security rating is the Industrial Security Representative's overall assessment of the effectiveness of the security systems and procedures in place to protect classified information at the facility. Following is a brief summary of the criteria for each rating category.

- **Superior**: A Superior rating is reserved for contractors who have consistently and fully implemented the requirements of the NISPOM in an effective fashion resulting in a superior security posture, compared with other contractors of similar size and complexity. The facility must have documented procedures that heighten the security awareness of the contractor employees and that foster a spirit of cooperation within the security community. This rating requires a sustained high level of management support for the security program and the absence of any serious security issues. For more complex facilities, minimal administrative findings are allowable.

- **Commendable**: A Commendable rating is assigned to contractors who have fully implemented the requirements of the NISPOM in an effective fashion resulting in a commendable security posture, compared with other contractors of similar size and complexity. This rating denotes a security program with strong management support, the absence of any serious security issues and minimal administrative findings.

- **Satisfactory**: Satisfactory is the most common rating and denotes that a facility's security program is in general conformity with the basic requirements of the NISPOM. This rating may be assigned even though there were findings in one or more of the security program elements. Depending on the circumstances, a Satisfactory rating can be assigned even if there were isolated serious findings during the security review.

- **Marginal**: A Marginal rating indicates a substandard security program. This rating signifies a serious finding in one or more security program areas that could contribute to the eventual compromise of classified information if left uncorrected. The facility's size, extent of classified activity, and inherent nature of the problem are considered before assigning this rating. A compliance security review is required within a specified period to assess the actions taken to correct the findings that led to the Marginal rating.

- **Unsatisfactory**: Unsatisfactory is the most serious security rating. An Unsatisfactory rating is assigned when circumstances and conditions indicate that the facility has lost, or is in imminent danger of losing, its ability to adequately safeguard the classified material in its possession or to which it has access. This rating is appropriate when the security review indicates that the contractor's security program can no longer preclude the disclosure of classified information to unauthorized persons. When an Unsatisfactory rating is assigned, the applicable government contracting activities are notified of the rating and the circumstances on which that rating was based. In addition, a compliance security review must be conducted after a specified interval to assess the corrective actions taken before the contractor's security rating can return to the Satisfactory level.

3. (1-302) Reporting Participation in Rehabilitation Programs as Adverse Information (ISL 00L-1 #3)

There is some confusion regarding the requirement to report participation in rehabilitation program as adverse information, particularly when the company promises "confidentiality" to employees who enroll. Therefore, the following guidance is provided:

- Self-enrollment in a rehabilitation program is not necessarily reportable. However, alcohol and drug abuse, or observation of behavior which is indicative of alcohol or drug abuse is reportable.
- Mandatory enrollment in an Employee Assistance Program is reportable.
- Refusal to accept rehabilitation assistance when offered is reportable.
- Incomplete or unsuccessful participation in a rehabilitation program is reportable.

The above policy interpretation is intended to provide a balance between industry's need for rehabilitation programs which do not necessarily have adverse consequences for enrollment, and the Government's need to properly monitor cleared individuals' continued eligibility for access to classified information. Participation in a rehabilitation program should not be used as a shield to prevent scrutiny by the Government. Keep in mind that the adverse information report is never the sole basis for suspension or revocation of a clearance.

4. (1-301, 1-302, 1-303, 1-304) Reports Submitted to the CSA (ISL 02L-1 #9)

The following report relating to NISPOM paragraph 1-302 will be made in JPAS

- Change in Cleared Employee Status

The following reports relating to NISPOM paragraph 1-302 will be submitted to DISCO:

- Adverse Information
- Citizenship by Naturalization
- Employees Desiring Not to Perform on Classified Work
- Refusal by an employee to execute the SF-312

The following reports relating to NISPOM paragraph 1-302 will be submitted to the DSS Field Office:

- Suspicious Contacts
- Changed Conditions Affecting the FCL
- Change in Storage Capability
- Inability to Safeguard Classified Material
- Security Equipment Vulnerabilities
- Unauthorized Receipt of Classified Material
- Employee Information in Compromise Cases
- Disposition of Classified Material Terminated from Accountability
- Foreign Classified Contracts

Reports of Loss, Compromise or Suspected Compromise in accordance with NISPOM Paragraph 1-303, will be submitted to the DSS Field Office

Individual Culpability Reports in accordance with NISPOM Paragraph 1-304, will be submitted to DISCO

5. (1-303 and 4-218) Notification to Recipients Regarding the Inadvertent Dissemination of Classified as Unclassified (ISL 00L-1 #8)

Contractors are reminded that when classified information is transmitted or disseminated as unclassified, notification of the actual classification to recipients who are cleared for access to the material is, at a minimum, CONFIDENTIAL. Therefore, if the material was originally transmitted electronically, contractors must provide the classification notification via secure channels (e.g., cleared network, STU-III, secure fax). The notification should also provide the classification source as well as declassification instructions. When control of the material has been lost, or if unauthorized personnel have had access to the information, such as when the recipient is not cleared for access, the matter is to be reported to your DSS Field Office as a report of compromise. Regardless of whether the recipient is a cleared or uncleared contractor/individual, if the transmission occurred by an unsecure means, (i.e. unsecure fax, Internet, unclassified server, etc.), the control of the material is deemed lost.

6. (2-102 and 7-101) Facility Security Clearances (FCLs) for Service Contracts (ISL 05L-1 #8)

DSS continues to receive requests to process companies for FCLs in order to perform service-oriented tasks (janitorial services for example). A fundamental requirement for FCL sponsorship is that the contractor must require access to classified information in connection with a legitimate U.S. Government or foreign government procurement. A request to clear a company solely to avoid implementing basic security procedures that would otherwise preclude access to classified information (e.g., escort by an authorized person in combination with appropriate area sanitization), is not justification for an FCL, and could lead to security vulnerability.

There may be rare exceptions when a company would genuinely need an FCL to perform service-oriented tasks. An example is when a cleaning company is under contract to clean an

area that, due to the nature of the classified material involved, cannot be adequately sanitized to preclude access to classified information even with appropriate escort. In those rare exceptions, the letter to DSS sponsoring the company for an FCL must clearly explain the rationale for the FCL. Such requests will be carefully scrutinized, and the validity for maintaining the FCL, once granted, will be a point of emphasis during recurring DSS security reviews.

7. (2-108) Clearing Branch Offices (ISL 03L-1 #8):

Historically, multiple facility organizations (MFOs) have had the option to centralize and administer certain security functions such as personnel clearance administration, security education, and classified visit authorizations within home office locations, or other cleared locations. Companies exercising this option maximize security resources and, in requiring fewer facility security clearances, avoid the related additional (processing and maintenance) costs by government and industry. There are currently numerous non-possessing division or branch offices cleared under the NISP. These are facilities that already have viable security programs established at their home office locations. Those home office locations can, in most cases, effectively administer the limited security administrative functions for these branch office locations. Accordingly, DSS will no longer process new facility security clearances (FCL) for division or branch offices that do not require possession of classified material for contract performance, unless there is a sufficient contractual or critical operational need.

Contractors considering administrative termination of non-possessing division or branch offices may contact their assigned DSS Industrial Security Representative for further guidance.

8. (2-200) Personnel Security Clearances (PCLs), the Internet, and Job Seeking (ISL 03L-1 #13)

The NISPOM clearly prohibits the use of a Facility Clearance for advertising purposes (2-100c, NISPOM). However, individuals may address specific qualification requirements associated with a position by informing prospective employers that they have been granted a PCL at the requisite level identified for the position. Aside from addressing specific qualifications for a particular position at a cleared contractor or Government facility, it is a poor security practice to identify oneself in a public database as a cleared person and become flagged as a possible target for foreign interests. Examples of such flagging, or identifying oneself as a cleared person, include online Internet employment services that solicit clearance information as well as other personnel data, and make this publicly available by electronic means. It should be understood that the audience for the Internet is worldwide and includes a large number of domestic and foreign entities. Other examples of flagging are employment seminars or job fairs that invite only persons granted a clearance to attend and register. In general, these and similar situations may also provide opportunities for foreign targeting and collection efforts. Foreign entities may be interested in identifying individuals who access or can access classified information. It is recommended that persons granted a clearance should consider the prospective audience before identifying themselves as cleared.

9. (2-201) Interim Access to JPAS – Based on a National Agency Check (NAC) (ISL 03L-1 #11)

The minimum requirement for access to the Joint Personnel Adjudication System (JPAS) is a clearance "eligibility" determination based on a NACLC. The NACLC became the required investigative basis for all SECRET and CONFIDENTIAL clearances in January 1999. Therefore, some individuals requiring access to JPAS will have a SECRET or CONFIDENTIAL clearance based on a NAC. These individuals will be permitted interim access to JPAS provided they have submitted a request for a NACLC.

10. (2-201) Fingerprint Cards Not Required for Periodic Reinvestigations (ISL 05L-1 #7)

It is no longer necessary to submit Fingerprint Cards (FPC) for any type of Periodic Reinvestigation (PR) unless specifically requested to do so. In the past, FPCs had to be submitted with requests for Secret and Confidential PRs but not Top Secret PRs.

11. (2-210) Access Limitations of an LAA

An export authorization is required to release classified information to a non-U.S. citizen or intending citizen who has been issued a Limited Access Authorization (LAA). The LAA is a determination that the non-U.S. citizen or intending citizen is eligible to receive specified classified information. It cannot serve as an export authorization. Therefore, prior to submitting an application for an LAA to DISCO, the contractor must obtain a written disclosure determination from a principal or a designated disclosure official or obtain a State Department approved export license. This documentation must be submitted with the application for an LAA.

12. (2-212) PCL/FCL Requirements for Self-Employed Consultants (ISL 03L-1 #6)

Cleared contractors may process self-incorporated consultants for a PCL in accordance with NISPOM paragraph 2-213 provided the consultant and members of his/her immediate family are the sole owners of the consultant's company, and only the consultant requires access to classified information. In such cases, a facility security clearance (FCL) is not required. Should other employees of the consultant's company require access to classified information, it would constitute a classified subcontract, and as such, a DD Form 254 must be issued by the prime contractor, and the consultant's firm will require an FCL.

13. (3-105) SF 312 Date in JPAS (ISL 05L-1 #6)

Personnel records in JPAS often contain a date for the Classified Information Nondisclosure Agreement (SF 312). The date reflected is normally the day the SF 312 was entered by DISCO in the system, not the date the SF 312 was signed. It is very important that this date not be changed in JPAS. The filing system DISCO uses to enable retrieval of the SF 312s is based on the date the SF 312 was processed by DISCO. As such, changing the date in JPAS would make it nearly impossible to locate a SF 312 should it be necessary.

Contractors are now responsible for entering this date in JPAS prior to granting the employee access to classified information. If a contractor is entering the SF 312 date, it should be the date the employee signed the form. If there is already a signed SF 312 on file for the employee as noted in JPAS, the employee is not required to sign another SF 312.

14. (3-105) Q&A – SF-312 (ISL 02L-1 #18)

Question: Is the Facility Security Officer (FSO) the only facility employee that can sign the acceptance block on the SF 312?

Answer: No. In accordance with "Classified Information Nondisclosure Agreement (Standard Form 312) Briefing Booklet", dated Spring 2001, "an authorized representative of a contractor, licensee, grantee, or other non-Government organization acting as a designated agent of the United States Government is empowered to witness the execution of the SF 312 by another non-Government employee, and may accept it on behalf of the United States". In most cases, authorized representatives of a contractor would be the FSO, other security officials under the oversight of the FSO, or one of the KMPs (Key Management Personnel).

15. (5-306a) Structural Integrity of Closed Areas (Reissue of ISL 03L-1 #4):

When a Closed Area has a false ceiling and/or raised floor, the areas above the false ceiling and below the raised floor are part of the Closed Area. These areas are often not visible, and may provide opportunities for surreptitious entry, modifications or tampering. Contractors must develop and implement procedures to ensure the continued structural integrity of Closed Areas. One of the following options may be selected:

a) Alarming the area above the false ceiling and/or below the raised floor.

b) Establishing certain ceiling tiles or installing clear tiles to facilitate viewing around the periphery of the area so that the integrity of the walls above the false ceiling and below the raised floor can be verified during normal operations.

c) Establishing an internal procedure that all work orders involving closed areas must be approved by the FSO.

d) Periodically inspecting the areas above the false ceilings or below the raised floors by removing ceiling or floor tiles. Minimum intervals for inspecting the areas will vary depending on the nature of classified material stored in the Closed Area and overall security of the cleared contractor facility. The following matrix is provided as a guideline for determining an appropriate minimum inspection frequency. While this matrix provides a guide, in certain instances an accelerated or decelerated inspection frequency may be appropriate based on conditions at specific cleared facilities. The required minimum inspection frequency must be approved by your Industrial Security Representative, and properly documented on the DSS Form 147, "Record of Controlled Areas."

Nature of Classified Information	Security-in-Depth	Minimum Inspection Frequency
Classified Information Systems with unprotected transmission lines above false ceiling or below false floor	No	Monthly
	Yes	Every Six Months
Open Storage of Classified Documents	No	Monthly
	Yes	Every Six Months
Classified Hardware	No	Every Six Months
	Yes	Annually

16. (5-306a) Closed Areas and Open Storage (ISL 04L-1 #11)

We have received questions regarding open storage of classified material in closed areas. These questions pertain to whether classified materials incidental to the operation of IS maintained in the Closed Area must be stored in GSA approved containers. Closed areas are normally established to protect information systems processing classified information and/or classified hardware. Classified documents, which include magnetic media, printed materials, etc., (see definition of Document, NISPOM Appendix C) are to be stored in approved security containers within the Closed Area unless the area has been approved for open shelf or bin storage. As an exception, it is not necessary that large items essential to the operation of an IS be further secured in the Closed Area. Examples would include large removable hard drives, in-use magnetic tapes, technical manuals, etc. Following this guidance, limited classified materials (e.g., electronic media, printouts, etc) associated with unattended IS processing sessions do not need to be stored in security containers.

In addition to the above, the CSA may approve open shelf or bin storage of classified documents in accordance with NISPOM paragraph 5-306b if there is an operational necessity. The contractor request for open storage must provide justification that the use of GSA-approved security containers will have an adverse impact on contract cost and performance. The contractor must describe the security features and practices that will ensure that the documents are properly safeguarded. DSS may also require endorsement of the request by the government contracting activity.

17. (5-309b) Changing Combinations (ISL 89 L-2 Q&A)

Combinations must be changed upon the termination of employment of any person having knowledge of those combinations. Having knowledge and having access are not the same thing. A locksmith has access to every combination but may not have knowledge of any combinations other than his or her own. It is not realistic to require a contractor to change hundreds of combinations when a locksmith leaves. The only combinations which require changing are those for which the locksmith had personal knowledge and the combination to the container(s) housing the master list or copies of combinations.

18. General Services Administration Carriers for Overnight Delivery of SECRET and CONFIDENTIAL Classified Information (revised from ISL 97L-1 #7)

NISPOM 5-403 e allows for the use of qualified commercial delivery companies for transmission of Secret and Confidential material. These companies must be current holders of the General Services Administration carrier contract and approved for overnight domestic express delivery of Secret and Confidential information. Companies currently approved by GSA for domestic express delivery services under Multiple Award Schedule 48 are available through the GSA website www.gsa.gov. This article serves as notice of CSA approval to utilize these carriers in accordance with the procedures identified below.

Facility Security Officers utilizing the commercial delivery companies/commercial carriers identified on the GSA schedule must establish procedures to assure the proper protection of classified packages at each facility intending to use overnight service. These procedures must be formally approved by the Cognizant Security Office (CSO). Contractors must establish an approved street address for incorporation by DSS in the Industrial Security Facility Database Facility Verification Request (FVR) function before such shipments may begin.

The following requirements apply and must be reflected in the company procedures:

- The carriers may be used for urgent overnight transmission of SECRET and CONFIDENTIAL material within the continental United States when overnight delivery cannot reasonably be accomplished by the U.S. Postal Service. However, classified Communications Security information (COMSEC), North Atlantic Treaty Organization (NATO), and foreign government information may not be transmitted overnight. Please note that Controlled Cryptographic Information (CCI) that is unclassified may be shipped overnight.

- Carrier personnel should not be notified that the package contains classified material.

- Material must be prepared for transmission as described in NISPOM paragraph 5-401a, except that a carrier's mailing envelope may be used as the outer wrapper.

- The outer address label should contain only the office or position/title, e.g., the "Security Office" or the "Facility Security Officer," of the destination facility.

- Senders may not use a Post Office Box as the destination address. Instead, a street delivery address approved for overnight shipments by the recipient's CSO shall be obtained from the FVR for contractors or from the security office of a government activity. Identification of a contractor's address in the FVR listing as an authorized overnight delivery address indicates CSO approval of the receiving facility's ability to securely accept such packages.

- A release signature block on the receipt label shall not be executed under any circumstances. The use of external (street side) collection boxes is prohibited.

- As a general rule, packages may be shipped on Monday through Thursday only to ensure that the package does not remain in the possession of the carrier service over a weekend. However, the CSO may grant local approval to ship material on a Friday provided the receiver has appropriate procedures in place. These procedures must ensure that a cleared person will receive and sign for the package on Saturday, and that he or she is able to secure the package in approved storage.

- The sender is responsible for ensuring that an authorized person will be available to receive the delivery and for verification of the correct mailing address. The receiving contractor must have procedures detailing how incoming overnight shipments will be received, transferred within the facility, and protected.

- Employees who handle incoming overnight shipments addressed to the "Security Office" or the "Facility Security Officer" must be cleared.

19. (5-902) Intrusion Detection System (IDS) Monitoring Over Data Networks (ISL 05L-1 #11)

Minimum acceptance criteria for the utilization of data networks for intrusion detection systems (IDS) are appended to this ISL. These criteria were developed in close coordination with representatives from industry, government and Underwriter's Laboratories (UL), and establish baseline security requirements for alarm system monitoring using data networks. These data networks may include private data networks (e.g., intranets or virtual private networks), or public data networks (e.g., the internet).

For the Department of Defense (DoD), all IDS equipment used to monitor classified information/equipment and sensitive arms, ammunitions and explosives, to include those utilizing data networks must be UL listed (in this case, UL listed to operate in a data network environment), and installed in accordance with UL standards. In addition, UL 2050 requires that any IDS utilizing data network monitoring must have the Cognizant Security Office (CSO) representative sign an Alarm System Description Form before a UL CRZH certificate will be issued. However, IDS approved by another government agency that meet DCID 6/9 standards may be accepted as outlined in the attachment to this ISL.

20. (6-104) Visit Authorization Letters for the Department of Energy (DOE) (ISL 03L-1 #10)

The Department of Energy requires requests for access to Restricted Data in the possession of DOE or other Federal Agencies designated by DOE to be made utilizing DOE Form 277, "Request for Visit or Access Approval." For contractors, the need for access to Restricted Data will, in all cases, be certified by a Government Contracting Officer (GCO). Failure to utilize the DOE Form 277 has caused unnecessary delays for some cleared contractor employees in gaining access to information required for job performance.

21. (10-102) Bilateral Security Agreements (ISL96L-1 #1)

The NISPOM refers to a variety of security agreements negotiated between various governments. How do the terms of these agreements apply to contractors?

General Security of Military Information Agreements (GSOMIA) are negotiated by the United States with a foreign government and obligate each government to provide substantially the same degree of protection to each other's classified information. On occasion, annexes to the GSOMIA, called Industrial Security Agreements, are negotiated with the foreign government for handling classified information entrusted to industry. Program agreements (e.g., co-production) either reference the GSOMIA and Industrial Security Agreement or include security language that is substantially the same as that in those agreements. Further requirements are contained in NATO security regulations. The requirements in Chapter 10 also are drawn from the security agreements and NATO regulations. Therefore, Chapter 10 obligates contractors to comply with the security requirements of the agreement, albeit indirectly.

22. (10-307, 10-509 and Appendix C) Definitions of "Foreign National" and "U.S. Person, (ISL96L-1 #3)

The NISPOM definition of a "U.S. person" is different from the definition found in the State Department's International Traffic in Arms Regulation (ITAR). Only a U.S. citizen is eligible for a personnel security clearance. Therefore, the NISPOM definition of U.S. person is an individual who is a U.S. citizen. The ITAR uses a broader definition of U.S. person based on a person's right to be hired if he or she is qualified for a job (employment). Such employment does not establish the eligibility basis for a security clearance.

Procedures must be in place to ensure that non-U.S. citizens do not have access to U.S. classified and foreign government information. If the procedures to preclude such access are not deemed adequate by the IS Rep, a detailed Technology Control Plan will be required that includes special briefings, non-disclosure statements and more stringent access control measures.

23. (10-306) Q&A re Storage of Foreign Government Information on an Information System (revised from ISL 05L-1)

NISPOM paragraph 10-306 requires that foreign government information be controlled generally in the same manner as U.S. classified material of an equivalent classification, and stored to avoid commingling with other material. This storage requirement is normally accomplished by establishing separate files in a storage container.

This requirement also applies to foreign government information stored on an information system. The preferable method for accomplishing this is to use periods processing with separate drives. Other options include: separating the foreign government information into different directories or folders on the system and protecting the foreign government information storage locations; or use of mandatory access controls (MAC) to label the data and control its location on the system;

However, there are instances where the contract actually requires foreign government and other classified information to be commingled in an information system; for example, in connection with a joint international program. If commingling is required, files must be marked to allow identification of foreign government information.

24. (10-508c) Q&A re CSA Notification of Assignment of Foreign Nationals to US Contractor Facilities (ISL 96L-1 #33)

Q: Does the requirement to notify the CSA in advance of all extended visits and assignments of foreign nationals to cleared contractor facilities apply to visits related to unclassified, non-defense, commercial programs?

A: No. This requirement applies to all foreign nationals on extended visits and assignments who are performing on classified contracts.

25. (10-508d) Q&A re Technology Control Plan (TCP) Requirement When Foreign Nationals are Assigned to US Contractor Facilities (ISL 96L-1 #34)

Q: Is a separate Technology Control Plan required for each CSA notification?

A: A facility may have an overall Facility Technology Control Plan that can be referenced with each notification. The contractor should contact his/her local DSS Field Office to ensure that the specific controls and limitations are threat appropriate.

APPENDIX

Intrusion Detection System (IDS) Monitoring Over Data Networks

PURPOSE: This document identifies minimum acceptance criteria for the utilization of data networks for IDS alarm monitoring for the protection of classified material under the National Industrial Security Program Operating Manual (DoD 5220.22-M) (NISPOM). These data networks may include private data networks (intranets or virtual private networks/VPNs)) or public data networks *("the internet"*). This guidance establishes baseline security policies and requirements for sensitive, national security related applications and systems used for such alarm monitoring.

1. BACKGROUND:

A. The NISPOM and the DoD Arms, Ammunitions & Explosives (AA&E) Manual (DoD 5100.76-M), specifies requirements regarding the use of IDS for the protection of classified material and certain risk categories of classified and unclassified AA&E. IDS utilized as supplemental protection for classified material as well as AA&E must comply with the Underwriters Laboratories standard for National Industrial Security Systems (UL 2050) for installation, testing, operations and maintenance. UL 2050 also identifies physical security measures for IDS when utilized for protection of DoD AA&E.

B. UL 2050 provides the option of utilizing a ***data network***[1] for alarm signal monitoring. While UL 2050 allows monitoring over data networks and specifies technical performance specifications,[2] it does not address security requirements, policies and procedures for IDS that utilize information systems (IS) for alarm signal monitoring over public or private communication lines. As NISPOM requirements apply only to classified information systems, additional guidance is needed to establish baseline security policies and requirements for sensitive, national security related applications and systems used for alarms.

C. IDS' using data networks may range from the relatively simple (i.e. a contractor protected area connected directly through a static internet protocol (IP) network address to a Central Station Monitoring Service (CSMS), to the significantly complex [for example, hundreds of installations being remotely monitored over a corporate network at a Government Contractor Monitoring Station (GCMS).]

[1] UL 2050 describes data network transmission as "switching that sends packets of information from the alarm control/transmission panel in an alarmed area to a monitoring station by way of private data networks (intranets or virtual private networks/VPNs)) or public data networks *("the internet"*). A private data network is also known as a local area network (LAN) or a wide area network (WAN). "For the purpose of the standard, public data networks may also include WAN and/or Internet Protocol (IP) networks.

[2] Installation criteria, power, signal transmission, system operation, response personnel and procedures, timeframes, records, etc.

2. GUIDANCE:

A. IDS' utilizing data network transmission shall be installed in conformance with appropriate UL 2050 requirements. All IDS equipment that is used to communicate with the data network shall be listed by UL for use with a data network, and the installation must result in the issuance of an appropriate UL 2050 certificate.

B. Prior to installing an IDS [utilizing data networks for alarm system monitoring] for supplemental protection under the NISPOM, contractors will submit a request for approval to the CSA including the following information:

(1) UL Alarm System Description for National Industrial Security Alarm System Certificate (Form No. CS-ASD-NISS);

(2) Proposed IDS hardware configuration and connectivity diagram (e.g. LAN/WAN schematic diagram) detailing the components (e.g. control panel, network interface cards, and method of data transfer (e.g. encryption implementation in hardware/firmware/software, etc.) between the protected area(s) and monitoring station locations. Hardware components and software will be identified by product name and release version.

C. Depending on the type of installation (e.g. subscriber or monitoring station) and complexity of the IDS (as reflected in the hardware configuration and connectivity diagram,) the request must also address and certify compliance with the following requirements, as applicable:

(1) **Government Contractor Monitoring Station (GCMS) or Central Station Monitoring Service (CSMS) IDS IS Server(s)/Host Computer:** The IDS IS Server(s) that receive and convert alarm signals to human readable form for appropriate assessment and response shall meet applicable UL requirements. The IS Server(s) running the IDS alarm signal processing software will be dedicated to the security system and staffed by monitoring personnel cleared to the Secret level. When monitoring personnel are not in attendance, the IDS IS [running IDS application software] will be secured within a locked room[3] with UL certified Extent 3 IDS protection.[4]

(2) **Remote Terminals:** Networked terminals that allow privileged access to the IDS IS host computer (i.e. can program or modify system operating parameters or user accesses, etc.) shall be continuously staffed by authorized personnel or protected within a locked room[3] with UL certified Extent 3 IDS protection. There shall be no capability for changing the mode of operation or status of the protected area(s) IDS from locations outside the authorized IDS staffed terminals or protected area(s).

[3] Rooms securing unattended IDS monitoring servers/host computers, remote terminals and/or workstations shall be comprised of walls, floors and ceilings that are fixed in place and constitute a solid physical boundary.
[4] "Extent of Protection" is defined in paragraph 5.18 and Table 23.1, UL 2050.

(3) **Workstations:** Workstations are terminals that only provide for acknowledgement of alarm signals. Unattended workstations will be secured within a locked room[3] with UL certified Extent 3 IDS protection.

(4) **User ID's and Passwords: A** unique user ID (UID) and password is required for each individual granted access to the IDS IS Server, remote terminal and workstation. Passwords shall be a minimum of eight characters; consist of alpha, numeric, and special characters; and shall be changed a minimum of every six months.

(5) **Personnel Security Clearance (PCL) Requirements:**

a. **Authorized Alarm Service Company (ASC) Representatives:** No clearance required. When working in IDS protected areas ASC representatives will be precluded from access to classified information and will be escorted/supervised by appropriately cleared personnel.

b. **System Administrator (SA):** The SA responsible for ensuring IDS IS server configuration, IDS communications signal processing software installation and updates, user account administration and maintenance will be cleared to the Secret level. For less complex IDS installations where the SA's duties are limited to the assignment of a network address/enabling of a network path for signal transmission between the protected area and monitoring station, a PCL will not be required. If the SA requires unescorted access to closed areas storing information above the Secret level, they will be cleared to the appropriate level consistent with the level of access and need-to-know.

c. **Information Technology (IT) Personnel:** There is no PCL required unless they have privileged access to the IDS server. Privileged access requires a Secret PCL. If IT personnel require full unescorted access to closed areas storing information above the Secret level, they will be cleared to the appropriate level consistent with the level of access and need to know.

d. **Users:** Personnel working in closed areas who arm/disarm the system will be cleared to the appropriate level of classified access

e. **Monitoring Personnel:** Secret PCL required.

(6) **Intrusion Detection Software:** IDS IS server(s) and remote terminals running IDS application and signal processing software will utilize intrusion detection software to monitor and log access attempts and all changes to IDS applications. The SA and facility security supervisor will be notified of unauthorized system access attempts and/or modifications for investigation or other appropriate action. Records will be retained for a period of 12 months (from the date of entry.)

(7) **IDS Signal Transmissions:** All IDS signal transmissions between the protected area (closed area) and the monitoring station shall be:

a. Protected though firewalls or similar enhancements (e.g. routers, Virtual Private Networks/VPNs, etc.) that are configured to allow only protective signaling data transfers between IDS components and addresses; and

b. Encrypted using a National Institute of Standards (NIST) Federal Information Processing Standards (FIPS) [5] approved algorithm with a key length of 128 bits[6] (or greater); and,

c. Polled at a minimum of six minutes regardless of protected area alarm system status, i.e. open or closed.

(8) **Service and Maintenance:** IDS IS testing, diagnostics, maintenance or programming will only be accomplished by the SA or ASC personnel, as appropriate. The ASC certifying alarm system installation and performing service, modifications or maintenance must be appropriately UL listed. While working in IDS protected areas, ASC personnel will be precluded from access to classified information and will be escorted by cleared and technically knowledgeable contractor employees. Unapproved use or substitution of non-UL listed IDS equipment or components can result in withdrawal of the UL certificate.

(9) **Annual IDS Testing.** After initial testing and approval, the IDS shall be inspected and tested annually to provide assurances that the IDS is functioning properly in accordance with UL 2050 and the NISPOM.

(10) **IDS Failure / Emergency Procedures.** In the case of IDS failure, closed areas storing Secret or Top Secret material, GSA approved security containers storing Top Secret material, or substandard security containers storing no higher than Secret classified material will be periodically inspected by appropriately cleared personnel in accordance with NISPOM standards for providing supplemental controls. Areas storing DoD AA&E material will be continuously staffed. Emergency procedures will remain in effect until the system is restored to operational status.

D. The CSA will review the contractor's request for approval. The CSA representative (IS Rep or in the case of AA&E, the designated Contracting Officer Representative) may consult with the appropriate UL POC regarding compliance with UL standards. If the IDS request and Alarm System Description form reflects compliance with these requirements, the designated CSA representative will sign [on page 4 – Alarm Transmission for Data Networks] the Alarm System Description Form (CS-ASD-NISS) and maintain a copy of the form with the contractor documentation in the official facility file. The original will be provided to UL by the ASC or contractor, as appropriate. The CSA representative may then formally approve the proposed IDS as supplemental controls under the NISPOM.

E. The ASC will submit the signed Alarm Systems Description for National Industrial Security Alarm System Certificate (CS-ASD-NISS) along with the [ASC completed] Alarm System

[5] UL 2050 also requires that the cryptographic modules must be certified in writing by the equipment manufacturer as complying with the NIST FIPS 140-2. The NIST validation list is available at http://csrc.nist.gov/cryptval/140-1/140val-all.htm.

[6] Both the *three-key* Triple Data Encryption Algorithm (TDEA) and the Advanced Encryption Standard (AES) algorithm (FIPS 197) are acceptable.

Certificate Request (CS-R2) to UL for issuance of the CRZH certificate for the protected space. Form CS-R2 is a multi-copy form. A completed copy will remain with the alarm customer as proof of [UL] submittal until the completed certificate arrives.

F. IDS currently approved in writing by a US Government cognizant security authority as meeting the requirements of DCID 6/9 for protection of SCI may be approved under the NISP provided the CSA approval was issued without waiving any requirements of the DCID 6/9 for Networked IDS. Alarm systems, procedures and related records approved for NISP use will be accessible for verification and review by DSS.

G. If an IDS approved under these procedures are subsequently determined not to be in compliance with UL and NISPOM requirements, the approval will be rescinded and the contractor will be required to implement an alternative procedures for supplemental protection of classified material.