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 05L-1 **January 18, 2005**

1. 2004 James S. Cogswell Award Recipients
2. Welcome Ms. Mary Griggs as DSS Deputy Director for Industrial Security
3. DOD Transfers Personnel Security Investigations Function to Office of Personnel Management
4. Closure of the Office of Security Services International
5. JPAS Implementation & Personnel Clearance Notifications
6. SF 312 Date in JPAS
7. Fingerprint Cards Not Required for Periodic Reinvestigations
8. Facility Clearances for Service Contracts
9. DSS Academy Training
10. Security for Wireless Devices, Services and Technologies
11. Intrusion Detection System (IDS) Monitoring Over Data Networks
12. Auditing Clarification
13. Tactical, Embedded, Data-Acquisition and Special Purpose Systems
14. Trusted Downloading
16. Frequently Asked Questions Regarding Information Systems (IS)

1. 2004 James S. Cogswell Award Recipients

Mr. Stephen F. Lewis, Acting Deputy Director for Industrial Security, DSS, announced the 2004 DSS James S. Cogswell Outstanding Industrial Security Achievement Awards on September 29, 2004, during the Annual Seminar of the American Society of Industrial Security (ASIS) in Dallas, TX. Eight facilities were selected for the annual award honoring organizations that establish and continue to maintain a superior industrial security program. Congratulations to the following facilities:

BBNT Solutions, LLC Middletown, RI	Keith Carlson, Manager Renai Chapman, FSO DSS IS Rep – John Oliver
Computer Sciences Corporation Huntsville, AL	J. Daniel Jones, Vice President Teresa Garland, FSO DSS IS Rep – Bonnie Fuqua
Controls and Structures Division of Vertex RSI Richardson, TX	Ralph N. White, VP and General Manager Robert G. Schwalls, FSO DSS IS Rep – Ernest Rhodes
Digital Receiver Technology, Inc. Germantown, MD	Acie Vickers, President/CEO Craig Heidemann, FSO DSS IS Rep – Colleen Nicholson
KEI Pearson, Inc. Arlington, VA	Robert F. Urso, President and CEO Raymond W. Rugen, FSO DSS IS Rep – Stephen Raymond
Northrop Grumman Information Technology (TASC) San Antonio, TX	Curt Armbruster, Executive Director, Security Phillip B. Mahoney, FSO DSS IS Rep – Richard Stogsdill
Raytheon Company Huntsville, AL	Peter E. Fryberger, Manager Charley Ann McMinn, FSO DSS IS Rep – Jeanne West
Raytheon Company Aurora, CO	Ray Kolibaba, Vice President Space Systems Pete Short, FSO DSS IS Rep – Andrea Schwalbe

2. Ms. Mary Griggs, Defense Security Service Deputy Director for Industrial Security

We are pleased to welcome Ms. Mary Griggs as the DSS Deputy Director for Industrial Security. Ms. Griggs' office administers the National Industrial Security Program (NISP) for the Department of Defense (DOD) and 22 non-DOD federal agencies of the Executive Branch, providing oversight, advice and assistance to over 11,000 NISP cleared contractor facilities.

Ms. Griggs' career includes extensive experience in investigative, security and counterintelligence operations with both the Departments of State and Defense. Ms. Griggs has also served in several senior level positions with the President's Foreign Intelligence Advisory Board, the National Counterintelligence Center, the Office of the Secretary of Defense and the Counterintelligence Field Activity (CIFA).

3. DOD Transfers Personnel Security Investigations Function to Office of Personnel Management

The Department of Defense (DOD) and the Office of Personnel Management (OPM) have finalized an agreement to transfer the DOD personnel security investigative (PSI) function and investigative resources. The transfer of personnel will take place on or about February 20, 2005 and will result in a more effective system for performing personnel security investigations. Detailed and/or updated information regarding this transfer will be posted to the www.dss.mil website. Please remember that this transfer of investigative resources does not change your facility's relationship with DSS. You continue to process personnel security investigations as you have in the past and continue to contact DISCO if you have questions on personnel security issues that cannot be resolved through your use of JPAS.

4. Closure of the Office of Security Services International

Effective March 31, 2005, DSS will close the last of its overseas offices and end the on-site industrial security oversight support that it has provided to US Government activities around the world. Although DSS will no longer be visiting overseas locations, Industrial Security Representatives responsible for the oversight of cleared US facilities dispatching cleared employees overseas will be available to provide advice and assistance to contractor organizations and government activities. DoD components overseas will continue to be responsible for providing the day-to-day oversight and management of contractors collocated with and supporting government customers. Questions of a general nature may be submitted via electronic mail to ipmd@dss.mil.

5. JPAS Implementation and Personnel Clearance Notifications

As announced in ISL 04L-2, the Joint Personnel Adjudication System (JPAS) became the personnel security system of record for contractors under the security cognizance of the Department of Defense on October 1, 2004. If you have not requested a JPAS account, you must do so immediately. Procedures for obtaining access to JPAS and JPAS training were provided in ISL 04L-2.

Effective February 14, 2005, all contractors under DoD security cognizance will use JPAS for personnel security actions. As of this date, DISCO will discontinue issuing Letters of Consent and DISCO Forms 562 will no longer be accepted. DISCO Forms 562 received prior to February 14th (for actions other than multiple facility transfers) will be processed. If you need to notify DISCO regarding a change you cannot currently complete in JPAS such as Social Security Number changes, Overseas Assignment/Return Requests or cases in which there is no record in JPAS for a subject, please submit a research, re-certify, or upgrade (RRU) action via JPAS.

Companies that have not registered for JPAS as of February 14, 2005 will only receive notifications regarding withdrawals of interim clearances, suspensions, and revocations of final clearances.

6. SF 312 Date in JPAS

Personnel records in JPAS often contain a date for the Standard Form 312 (SF 312), Classified Information Nondisclosure Agreement. 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.

7. Fingerprint Cards Not Required for Periodic Reinvestigations

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.

8. Facility Clearances for Service Contracts

DSS has received several recent requests to process companies for facility security clearances (FCL) 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 (NISPOM 1-202 & 7-102). 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 a facility clearance, 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.

9. DSS Academy Training

NISPOM Chapter 8 Independent Study Course - An online, independent study version of the NISPOM Chapter 8 Security Requirements Course will soon be available from the DSS Academy. The course has been designed and developed to cover the same content as the three-day NISPOM Chapter 8 Requirements course that is offered in a traditional classroom setting. To register for the online NISPOM

Chapter 8 Requirements Course please visit the DSS Academy web site. Go to www.dss.mil and click on "Academy." Then sign into the ENROL system and follow the instructions on the screen.

JPAS Training - The DSS Academy offers a variety of training products for users of the Joint Personnel Adjudication System (JPAS) /Joint Clearance and Access Verification System (JCAVS). Products include:

a) JPAS/JCAVS Training for Security Professionals – This course is presented at the DSS Academy twice each month by the JPAS Program Office.
b) Desktop Resource for JCAVS – the Desktop Resource provides detailed instructions on the use of JCAVS version 2.1.1. This is an instructional tool and job aide.
c) JPAS Overview - this is a Power Point presentation designed to introduce the JPAS version 2.1.1, and its capabilities to Department of Defense personnel and NISP contractors. This product provides an overview for personnel hoping to expand their familiarity with JPAS regarding vocabulary changes, user levels, benefits, system access requirements, and JPAS screen shots and explanations.
d) A new JPAS/JCAVS Tools for Security Trainers course is in development. This course is intended for current JPAS users who will provide JPAS training. After attending this course, each student will be able to present JPAS/JCAVS training using tools available from the DSS Academy and the JPAS Program Office.

10. Security for Wireless Devices, Services and Technologies

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.

There is a DoD Directive regarding the use of commercial wireless devices, services and technologies in the Department of Defense. Please be advised that this directive is an internal DoD publication and that any security requirements contained therein are not applicable to cleared industry unless specified in the NISPOM or directed in a classified contract. A copy of this directive is available at http://www.dtic.mil/whs/directives/corres/pdf/d81002_041404/d81002p.pdf

11. Intrusion Detection System (IDS) Monitoring Over Data Networks

Minimum acceptance criteria for the utilization of data networks for intrusion detection systems (IDS) are appended to this ISL, and approved for immediate use. 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.

12. Auditing Clarification

A number of questions have been received regarding the auditing exception stated in ISL 04L-1 for older operating systems and when it applies. Auditing is a NISPOM requirement; and systems that are capable of auditing must have auditing enabled. 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.

The exception noted in ISL04L-1 applies only to those rare situations when a government contracting activity requires the use of an operating system that is not capable of meeting Chapter 8 audit requirements. In such 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 directs the use of these operating systems 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). A formal contract modification is not necessary.

13. Tactical, Embedded, Data-Acquisition and Special Purpose Systems

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.

14. Trusted Downloading

[1] The NISPOM defines an Information System (IS) as an assembly of computer hardware, software, and firmware configured for the purpose of automating the functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating, or otherwise manipulating data, information, and textual material.

Numerous inquiries have been received from industry for clarification as to whether trusted downloading procedures must be followed when classified information is downloaded from a PL-1 IS storing the same level classified information from multiple programs.

Trusted downloading refers to a CSA approved procedure or series of procedures, for the secure transfer of classified information of different levels (e.g. Top Secret, Secret, Confidential), or sensitivities (e.g. NATO, Foreign Government Information/FGI, Restricted Data/CNWDI, COMSEC, etc.) to media that will be handled at a lower classification or sensitivity level, or unclassified level, than the IS from which the data was transferred.

The transfer of data from IS accredited/operating at PL-1 to media that will remain under the same or higher level classified environment/controls (i.e. access controls, safeguarding, etc.) does not require the use of trusted downloading procedures. Rather, a review must be accomplished to ensure only designated files were transferred to the new media. This could include a review of hard copy output and/or a short visual review of the electronic file. In instances where information such as NATO, FGI, CNWDI, RD, etc. is stored on the IS and information is downloaded to electronic media, trusted downloading procedures do apply.

15. Frequently Asked Questions Regarding Information Systems (IS)

Following are several frequently asked questions and clarifying guidance relating to IS used to process classified information.

Question: Can an IS that is used by more than one person be considered a single-user standalone?

Guidance: A single user standalone IS 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.

Question: For PL-1 systems, what is required to satisfy the System Security Plan (SSP) certification requirement of NISPOM Paragraph 8-103g?

Guidance: For a PL-1 system, a written statement from the IS Security Manager (ISSM) that the SSP has been implemented, that specified security controls are in place and properly tested and that the IS is functioning as described in the SSP satisfies the requirement.

Question: In a multiple facility organization (MFO), can an ISSM who has been granted self-certification authority self-certify systems across the MFO structure?

Guidance: The CSA may approve an employee to serve as ISSM for multiple facilities within a defined area. The facilities should be within an approximate one-hour ground travel time of the ISSM's duty station, and the number and complexity of the classified information systems/security programs must be appropriate to the ISSM's oversight capability (i.e. work-hours, authority, etc.). On a temporary basis (i.e. a period not to exceed 60 days), and subject to the prior approval of the DSS Field Office [with cognizance over the facility without a permanent ISSM], an ISSM may be appointed to self-certify systems for facilities where the travel distance is greater than the approximate one-hour ground travel

time provided the ISSM has been delegated that authority by contractor management. To request such approval, the contractor will provide a plan to the cognizant DSS Field Office detailing how ISSM responsibilities will be implemented and managed.

Question: Can an IS being upgraded to process classified information be booted from a floppy disk or CD-ROM?

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

Question: Is a Memorandum of Understanding (MOU) required when accredited mobile systems are relocated to government activities or test sites?

Guidance: The contractor must have a signed "Letter Acknowledging Relocation of IS by Government Activity" prior to shipment, thus an MOU is not necessary. The letter template is available on the DSS.mil website.

Question: Should new media be used when doing trusted downloading?

Guidance: Use of new media would facilitate compliance with the guidance in NISPOM 8-302a, 8-305 and 8-309. New media would mitigate 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 standard is available at http://www.dss.mil/infoas/index.htm

Question: What does unclassified software review and/or testing required by NISPOM paragraph 8-302a encompass? (This issue was previously addressed in ISL 01L-1, Question 25.)

Guidance: If the contractor chooses to conduct a review of unclassified software, it must be a line-by-line source code review. If the contractor chooses testing, the testing must include a review of all functionality for security-relevant issues, as well as resolving those issues. For example, if the software writes to a file, the file must then be reviewed utilizing a hexidecimal editor to ensure that only the intended information was written.

Question: Do the provisions of NISPOM Paragraph 10-306, which 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, also apply to foreign government information stored on an information system?

Guidance: Yes, this does include electronic media. Classified foreign government information must be stored separately to avoid commingling with other material. The preferable method for accomplishing this is to use periods processing with separate drives.

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/VPN's)) 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***[2] for alarm signal monitoring. While UL 2050 allows monitoring over data networks and specifies technical performance specifications,[3] it does not address security requirements, policies and procedures for IDSs 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).]

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

[2] 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/VPN's)) 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.

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

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[4] with UL certified Extent 3 IDS protection.[5]

(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) **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.

[4] 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.
[5] "Extent of Protection" is defined in paragraph 5.18 and Table 23.1, UL 2050.

(5) **Personnel Security Clearance (PCL)[6] 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/VPN's, 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) [7] approved algorithm with a key length of 128 bits[8] (or greater); and,

---

[6] A Personnel Security Clearance (PCL) is an administrative determination, based on an appropriate investigation, that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted.

[7] 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.

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

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 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.