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

## INDUSTRIAL SECURITY

# LETTER



**ISL 04L-1** **February 27, 2004**

## 1. 2003 James S. Cogswell Award Recipients

Mr. William A. Curtis, Acting Director, DSS, announced the 2003 DSS James S. Cogswell Outstanding Industrial Security Achievement Awards on June 10, 2003, during the National Classification Management Society (NCMS) annual seminar in Salt Lake City, UT. Fifteen 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:

**Capital Region**

Association of American Railroads
Washington, D.C.

Hewlett-Packard Company
Gaithersburg, MD

Lockheed Martin Mission Systems
Federal Security Programs Office
Gaithersburg, MD

Technology Service Corporation
Bird Associates Operations
Vienna, VA

Northrop Grumman Space & Mission Systems
Columbia, MD

**Northeast Region**

Bath Iron Works
A General Dynamics Company
Bath, ME

**Central Region**

ITT Industries, Inc.
Advanced Engineering & Sciences
Colorado Springs, CO

L-3 Communications Corporation
ComCept Division
Rockwall, TX

Lockheed Martin
Naval Electronics & Surveillance Systems
Akron, OH

Lockheed Martin Corporation
Space Systems Company
Space & Strategic Missiles
Denver, CO

**Southeast Region**

Lockheed Martin Information Systems
Orlando, FL

**West Region**

Honeywell International, Inc.
Engines, Systems & Services
Phoenix, AZ

NewTec
White Sands Missile Range, NM

Veridian Systems Division, Inc.
Tucson, AZ

XonTech, Inc.
Pleasant Hill, CA

## 2. May 1, 2004 Implementation Date

The deadline for complying with the provisions of NISPOM Chapter 8 published May 2000 is fast approaching. All accredited contractor information systems are to meet current NISPOM requirements by May 1, 2004. If you are not yet in compliance, you must provide your Industrial Security Representative with a plan prior to the May 1st deadline for how you will get into compliance. There is no plan to grant extensions or exemptions to this deadline. However, contractors that have been operating in good faith to meet the deadline and have provided acceptable plans for compliance will not have accreditations withdrawn for systems that are not reaccredited by May 1st. Additionally, we have identified an exception when the government contracting activity (as evidenced in the contract documentation or classification guidance) requires the contractor to maintain an IS which was accredited under previous policy, and whose operating system is not capable of implementing the current Chapter 8 audit requirements. All other provisions of NISPOM Chapter 8 will apply to these systems.

## 3. Audit Requirements (NISPOM Paragraph 8-602)

The May 2000 NISPOM Chapter 8 revision modified/added audit requirements for contractor IS systems accredited to operate at Protection Level (PL)-1. The revision required that automated auditing features available with operating system software be enabled to capture and record [in the form of an audit trail or log] users activities in relation to security relevant objects (e.g. files, applications, directories, etc.) for PL-1 systems.

The majority of operating systems are delivered [in a default configuration] with security features (e.g. auditing) disabled or turned-off. Most operating systems can be configured to meet NISPOM paragraph

8-602(a) and 8-602(b) Audit requirements. However, some operating systems do not have this capability and will require third party software[1] to meet the NISPOM audit requirements.

**MICROSOFT** operating systems (i.e. Windows 2000, XP, and NT) can be configured to meet NISPOM Audit requirements. Microsoft Windows includes audit capabilities to directories/folders and to individual files. Microsoft Windows can be configured to audit individual success or failure to system accounts, directory service access, object access, and system and user activity. Guidance regarding Windows profiles containing the appropriate audit settings/configurations is available on the DSS internet website at http://www.dss.mil/infoas/index.htm. To access the information, click on Windows Security Settings. This will take you to a log in screen for the closed portion of the DSS website. If you don't already have a User ID and password, instructions are provided on the website for establishing a user account.

**UNIX** operating system capabilities will vary. Some Unix type operating systems (e.g. Linux) require the addition and local configuration of third party software while others (e.g. IRIX, Solaris) can be configured to meet Audit requirements using products delivered with the operating systems software. IRIX includes a product called System Audit Trail (SAT) that can be configured to meet Audit 1 and Audit 2. The Solaris operating system includes a utility called Basic Security Module (BSM) which can be configured to meet Audit 1 and Audit 2 requirements. However, both SAT and BSM processes generate large amounts of audit data. DSS has developed a filter that can reduce the aforementioned audit data/files by approximately 75%. The filter, as well as other guidance and utilities that will assist in configuring the most widely used operating systems, is available on the DSS Internet website at http://www.dss.mil/infoas/index.htm. To access the information, click on Audit Filters, where you will be directed to the log in screen for the closed portion of the DSS website.

### 4. Security-Relevant Objects

NISPOM paragraph 8-602a(1)(c) requires auditing of security-relevant objects and directories beginning at PL-1. Security-relevant objects and directories are part of all operating systems but are not identified the same or may not reside in the same folders/directories. The following table represents a standard configuration of security relevant objects to be audited for Windows NT and Unix. Please note that while the security-relevant objects and directories will remain constant, directory examples can vary by installation, by administrator and by operating system.

| **Security relevant objects** | **Directory Examples (can vary by installation)** | |
|---|---|---|
| | *Windows* | *Unix* |
| Operating system executables | C:\WINNT or C:\Windows | /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[2] | C:\Program Files\Nisp_Utilities | /usr/local or /opt |

[1] All auditing software, to include third party software, is security-relevant and is subject to the provisions of the system configuration management program. The ISSM shall notify DSS of requests for changes to any third party audit software that might deviate from the requirements of the approved SSP.

| | | |
|---|---|---|
| User files/classified data beginning at PL-2 | C:\Profiles or C:\Documents and Settings | /home |

**5. Access to Security-Relevant Objects and Directories**

Question 55 of ISL 01L-1 was published with the intent to modify the Audit 1 requirement of capturing only unsuccessful accesses to security relevant objects and directories for PL 1. That change was the result of security testing that demonstrated that auditing successful [as well as unsuccessful] accesses to security-relevant objects and directories at PL 1 adversely affected system operations and dramatically increased the time required for the weekly review, without added benefit to the protection of the information.

For systems accredited at PL-1 and PL-2, only unsuccessful access/attempts to security-relevant objects and directories must be audited. At the PL-2 level, where need-to-know is a factor, auditing is required for successful and unsuccessful attempts to access user files/classified data. At PL 3 and PL 4, auditing is required of both successful and unsuccessful access to security-relevant objects and directories and to all User files and classified data.

| **Security relevant object** | **PL-1** | **PL-2** | **PL-3** | **PL-4** |
|---|---|---|---|---|
| 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[2] | U | U | S, U | S, U |
| User files, classified data | (no auditing) | S, U | S, U | S, U |

S-Successful
U-Unsuccessful

**6. Update on Transfer of Personnel Security Investigations Program**

The transition of the personnel security investigations (PSI) program to the Office of Personnel Management (OPM) is still underway but the process is moving at a much slower pace than we had anticipated. OPM and DoD continue to resolve a large number of details associated with this transfer; however, progress is being made with the expectation that the transfer of function and personnel will occur before the end of this fiscal year. In the interim, OPM has begun to process DoD investigations that were submitted since October 1, 2003. Cases received prior to that date continue to be worked and completed by DSS.

Although we had hoped that the transition would be transparent to our customers, we have recently been advised that some Facility Security Officers at cleared contractor sites have been contacted by OPM's

[2] Examples of security related software include anti-virus software, audit reduction software, word-text search software, hexadecimal editors, password generators, password strength-testing software, sanitization software, and trusted downloading process software

investigative provider asking for additional information on PSIs submitted for their employees. DSS is working with OPM to resolve this issue in order to prevent unnecessary contact with industry. We have asked that OPM advise their provider to contact the DISCO Helpdesk at DSS to resolve any discrepancies or obtain any additional information and not to contact industry directly. If you are contacted for additional EPSQ information on your employees, we ask that you refer the caller to the DISCO Help Desk at 1-888-282-7682.

We apologize for any confusion this may have caused and ask for your patience as we work with OPM to resolve the remaining issues and details of the transfer.

**7. Joint Personnel Adjudication System (JPAS)**

DoD is now ready for industrial users of JPAS to begin the process of reconciling the data contained in JPAS for their cleared facility. If your facility does not yet have a JPAS account please see the guidance below on obtaining training and access to JPAS. We request that all DoD cleared facilities gain access to JPAS as soon as possible.

For those facilities that are accessing JPAS, please review all of your personnel security records and make necessary changes within the next 60 days. Changes that the contractor can make include: terminating access for individuals identified at your facility that are no longer your employees; bringing into your Personnel Security Management Network employees whose eligibility for access to classified information is in JPAS but not reflected at your facility to include adding and separating the Person Category, category classification, and cage code; entering SF 312 signature date; correction of identifying data - name, date and place of birth; and maintaining an employee's access.

Changes that require notification to DISCO by use of the "RRU' function in JPAS are an incorrect eligibility; Social Security Number change, Overseas Assignment/Return requests or no record reflected in JPAS for the subject. The contractor accessing JPAS will take all actions with these exceptions. Contractors using JPAS no longer need to submit DISCO Form 562s to DISCO for any personnel security actions. If you need to notify DISCO of information, e.g. the subject has an SSBI open and there is a name or marital status change, this should be accomplished via an RRU.

**Instructions for Acquiring a JPAS Business Organizational Account**

To obtain an account, the company must submit an Appointment Letter on company letterhead to identify their top hierarchical primary and alternate account managers who are to be issued active account manager user ids and privileges. The account manager may serve this role not only for all facilities within a multiple facility organization, but also for first and lower tier subsidiaries. A corporate officer or other Key Management official must sign the letter. Letters must include the account managers' full names, social security numbers, and contact information (i.e., telephone numbers, office addresses, and work email addresses). The letter must also include contact information for the corporate officer or other Key Management official making the request.

In addition to the letter, the company must complete a System Access Request (SAR) form that may be obtained from https://jpas.osd.mil/betaTestInfo/registrationForms.asp. The letter and the SAR must contain the same authorization signature. The SAR will require that a user level be identified for each of the accounts. This information may be obtained from the table at the bottom of this document. Questions regarding the completion of the letter, the SAR or management of the account, should be directed to the JPAS Help Desk, 202.404.6692 or 202.404.2923. The JPAS Help Desk hours are Monday through

Friday, 0600 - 1800 EST. Other Help Desk phone numbers, a fax number and email account may be found at: https://jpas.osd.mil/betaTestInfo/pocs.asp#desk. The company should allow the JPAS Help Desk one business day to process the request before following up on the submission.

Once the JPAS Help Desk processes the request for the account, the company will be notified of the account being issued via email. There will be two emails sent: one to identify the account password and one for the account user id. After sending these messages, the Help Desk personnel will call the company to ensure can get logged on and to discuss privileges.

With JPAS access comes the responsibility to maintain the information for the company. To fully utilize the system, it is recommended that training be accomplished prior to using the system. Information on training sessions may be obtained from the JPAS web site, https://jpas.osd.mil/betaTestInfo/events.asp, or from the DSS web site, under the Academy services, http://www.dss.mil/search-dir/training/courses.htm. The DSS Academy course is IS301.01 - JPAS/JCAVS Workshop For NISP Contractors.

Due to security concerns associated with .edu or .org Internet addresses, those addresses will not be able to access JPAS at this time. Such facilities could acquire a .com, .gov or .mil account to facilitate access to JPAS.

*Account Manager User Levels*

| | | |
|---|---|---|
| Level 2 – Corporate Officers (SCI) | SSBI/SBPR | SCI/SCI Access Eligibility |
| Level 3 – Company FSO Officers/Managers (SCI) | SSBI/SBPR | SCI/SCI Access Eligibility |
| Level 4 – Corporate Officers/Managers (Collateral) | NACLC/NACLC-PR | Secret Eligibility |
| Level 5 – Company FSO Officers/Mgrs (Collateral) | NACLC/NACLC-PR | Secret Eligibility |
| Level 6 – Unit Security Manager/Visitor Control | NACLC/NACLC-PR | Secret Eligibility |
| Level 7 – Guard Personnel (Collateral) | NACLC/NACLC-PR | Secret Eligibility |
| Level 8 – Guard Personnel (SCI) | SSBI/SBPR | SCI/SCI Access Eligibility |

## 8. Security Review Ratings

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 exceeded the basic requirements of the NISPOM, compared to other contractors of similar size and complexity, and have established a proactive security program. The facility must have 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 level of management support for the security program and absence of any serious security issues.

- **Commendable**: Commendable is our newest rating category. A Commendable rating indicates a facility's security program exceeds the basic requirements of the NISPOM, but is not at the level required to achieve a Superior rating. This rating denotes a security program with strong management support, minimal administrative findings, and the absence of any serious security issues. To achieve this rating, contractors must go beyond basic NISPOM requirements in one or more areas of their security program, and consistently sustain a high level of protection of classified information.

- **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.

**9. Closed Areas, Miscellaneous Openings (NISPOM 5-801h) and Supplemental Protection**

We have received several inquiries requesting clarification regarding methods for securing miscellaneous openings into closed areas. The NISPOM specifies physical construction standards for closed areas. In addition to the construction requirements, supplemental protection (normally a CSA approved intrusion detection system) is required for all closed areas storing Secret and Top Secret classified information. Intrusion detection systems (IDS) supplement NISPOM physical security construction standards.

Miscellaneous openings (vents, ducts, registers, etc) into closed areas that meet or exceed the minimum dimension requirements require installation of barriers such as rigid metal bars, 18 gauge expanded metal or wire mesh. NISPOM 5-801h allows the option of utilizing CSA approved IDS (in lieu of the aforementioned barriers) in the miscellaneous opening to detect unauthorized access. Protective grid-wiring/bread-wiring are examples of IDS equipment that can be used for this application. Barriers or IDS used to secure miscellaneous openings should be installed to facilitate periodic inspections.

**10. The Mental Health Question on the EPSQ**

Item 19 of the EPSQ asks whether applicants have received mental health treatment during the past seven years. If the answer is "yes," applicants are asked to provide the dates of treatment and the name and address of the therapist or doctor if the treatment was not limited to marital, family, or grief counseling. Many applicants provide additional information in the remarks section though it is not required. This additional information is helpful to DISCO in making interim security clearance determinations. For example, counseling for work related stress is viewed much differently than hospitalization for a serious psychological condition. For this reason, we encourage use of the remarks section to describe the reason for treatment, the diagnosis, frequency of treatment, and whether applicants have taken medication or been hospitalized for their condition.

**11. Closed Areas and Open Storage (NISPOM 5-306a):**

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 need not 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 5-306a 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.

**12. Maintaining Signed Copies of the EPSQ**

As a reminder, before electronically transmitting EPSQs, a copy of the EPSQ must be printed and signed by the clearance applicant, and retained by the contractor facility. The original hand signed certification must match exactly the certification statement on the transmitted EPSQ, and made available upon the request of the investigative provider (e.g., DSS or OPM). With the upcoming transfer of the PSI function, you may see an increase in the number of requests by investigative providers for the original signed EPSQ.