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 02L-1 **April 22, 2002**

1. Industrial Requests Affected by Operation Enduring Freedom

Due to the overseas deployment of military/civilian personnel in support of Operation Enduring Freedom, the Defense Security Service (DSS) will encounter investigative leads that cannot be conducted. In such instances, DSS will complete all pending investigative work that can be accomplished, and hold the remaining leads in abeyance until the individual returns from deployment. The Defense Industrial Security Clearance Office (DISCO) will notify contractors when such investigations cannot be completed. Upon the clearance applicant's return from deployment, contractors should send notification to DSS, Attn: Mr. Douglas McKim via facsimile at (301) 677-5034 if the individual still requires a personnel security clearance (PCL). The notification must include the individual's current location (i.e., residence, facility location and actual work site). In the event the individual will be transferring to a different facility, the new location should be provided so that the remaining investigative work can be accomplished as quickly as possible. No action by the contractor is necessary if the individual no longer requires a PCL unless the individual was previously granted an Interim PCL. In such cases, the contractor must terminate the Interim clearance using the DISCO Form 562.

2. Resumption of Industry's Sensitive Compartmented Information and Special Access Program Personnel Security Investigations by Defense Security Service

Beginning March 15, 2002, industrial investigative requests for access to Sensitive Compartmented Information (SCI) and/or Special Access Programs (SAP) that were previously diverted to the Office of Personnel Management (OPM) for processing were again to be directed to the Defense Security Service (DSS). Facility Security Officers (FSO) must use the Electronic Personnel Security Questionnaire (EPSQ) version 2.2. Version 2.2 allows better tracking and management of your requests and permits the assignment of special project codes as indicated in ISL 01L-2. Any industrial investigative requests for SCI or SAP received by OPM after March 15th will be rejected and must be resubmitted electronically to DSS. As you may be aware, a portion of the DSS workload was temporarily moved to OPM in 2001 to help reduce the large backlog of pending investigations at DSS. Please contact your Industrial Security Representative should you have any questions regarding this issue.

3. Joint Personnel Adjudication System (JPAS) – General Information

JPAS is DoD's automated system that will maintain all collateral and SCI security clearance (eligibility and access) and adjudication information for DoD contractor and government personnel. The DoD adjudicative facility will enter "eligibility" determinations in JPAS and contractors will complete the "access" field. JPAS allows you to both read information for all personnel on the system and to perform personnel security actions for personnel within your span of control in real time. Notification of clearance eligibility will arrive electronically. The contractor without waiting for action by DISCO will do reinstatements and conversions. Once all contractors have the opportunity to come on line (within the next 2 years) use of JPAS for personnel security actions will be mandated for all contractors.

Obviously this will change the way you and DSS do business. When JPAS is fully operational, there will be no more letters of consent and DISCO Forms 562 for routine clearance actions. Everything will be on line. You will be able to see a person's eligibility and accesses whether they are contractor, government, reserve or active duty military. You will annotate the employee's file when required briefings are performed to include SCI briefings/debriefings. You will be able to see when a new employee has already executed an SF 312 or orally attested negating the need for you to do either. You will also be able to create reports for your facility and any facilities within your span of control (no more waiting for a listing of your cleared employees from DISCO).

There are varying levels of access granted to this system from the basic "read only" function that you would normally associate with a visitor control function to read and write capability for all records under your span of control.

With this privilege comes a lot of responsibility. You will maintain your records within JPAS and must ensure that whoever in your facility is responsible for this function, has been properly trained. Although you will not be able to grant access in JPAS to an employee unless the investigative basis is there, it will be your responsibility to accurately and expeditiously maintain your records, as other DoD users will be granting access to your employees based on your data.

Industry Beta Testing. Beta testing for industry has begun, with the following companies participating:

Lockheed-Martin
Boeing Corp.
Raytheon Corp.
TRW
Northrop-Gruman

These facilities have been working with DoD for the past two years to develop the industrial security application for JPAS. They have conducted training for their personnel and identified all members of their corporate families that will come on-line within the next two months. Once all of their cleared facilities are on line, additional facilities will be added. Those facilities have already been contacted and will soon be receiving information on training and facility identification. Once they are on line, we will gradually add additional companies until everyone who is interested, will have access.

Clearance Requirements for Users. Persons who can access JPAS whether in a read only or read and write capacity must have at least a Secret clearance. Persons who will enter information concerning SCI briefings/debriefings must have a clearance based on a single-scope background investigation (SSBI).

FREQUENTLY ASKED QUESTIONS ABOUT JPAS

a. What is the Joint Personnel Adjudication System (JPAS)?
JPAS is the Department of Defense (DoD) migration system used to automate personnel security management. JPAS facilitates virtual consolidation of the Department's nine Central

Adjudication Facilities (CAFs), and linkage between Non-SCI security program managers, Special Security Officers and DoD contractor Facility Security Officers with the CAFs and each other to obtain real-time, up to date, accurate, eligibility and access information on cleared DoD personnel. JPAS is the single, authoritative DoD source for eligibility and access information needed by authorized users in order to grant immediate access to classified information. JPAS uses a centralized database and application programs based on standardized core DoD personnel security processes and data elements. JPAS also interfaces with other automated information systems managed by the Defense Security Service (DSS), the Defense Manpower Data Center (DMDC), the Defense Civilian Personnel Data System, the Office of Personnel Management and Air Force Personnel Center. Telecommunications and automated information systems interface software serve as the cornerstone for JPAS.

b. What applications support JPAS?

There are two applications in JPAS to support both the adjudication and personnel security management processes. The Joint Adjudication Management System (JAMS) is available only to adjudicative personnel assigned to one of the nine DoD CAFs. The Joint Clearance and Access Verification System (JCAVS) is used by non-SCI and SCI personnel security managers, entry control personnel, key personnel organizations, contractors and other entities as approved by the JPAS Executive Steering Committee/Configuration Management Board (JPAS ESC/CCB).

c. What are the software and hardware requirements for JPAS?

JPAS is a “web-based” application and requires no special software. However, users should ensure Port #443 is open at their local firewall. The minimum hardware requirements to use JPAS are:

Pentium computer, 133 MHz or higher
128 MB RAM
NETSCAPE 4.7 or higher (but not Netscape 6.0 or higher)
Public Key Infrastructure (PKI) certificate/token

Netscape is the DoD-mandated web browser. Internet Explorer may be used, however JPAS may not operate properly. In addition, the Defense Information Systems Agency (DISA) has made PKI certificates obtainable only by using Netscape.

d. How and when will JPAS users be trained?

Initially, JPAS will use the “train-the-trainer’ concept. Training will be accomplished by the JPAS program office as well as by contractor associations such as the National Classification Management Society. Training CDs are also available. After deployment, JPAS will become part of the curriculum in courses offered by the Defense Security Service Academy (DSSA) and the Defense Intelligence Agency (DIA), both resident and mobile courses.

e. What should Industry do at this time?

This information is being provided for information only. As we are able to add more contractors to JPAS, we will make more information available on procedures and training.

4. Sending Releases to Defense Security Service (DSS)

Signed releases are an important element of every investigative request sent to DSS. Much of the basic investigative work cannot be initiated without the necessary releases. The most efficient method for sending signed releases to DSS is by attaching a scanned image of the release (i.e., ".tif" file) when transmitting the Electronic Personnel Security Questionnaire (EPSQ). Transmitting the release electronically with the EPSQ improves the efficiency of the investigative process, and helps ensure the release is associated with the proper investigative request.

The following guidelines should be followed for signed releases:

1. Send Authorization for Release of Information with **EVERY** investigative request submitted to DSS. Also send the Authorization for Release of Medical Information if appropriate. These releases are part of the SF86 and SF85P and are contained in the EPSQ software.

2. Ensure that releases are signed, complete, and legible. The minimum information needed to ensure that a release is usable is a signature, typed or printed name, SSN, and signature date.

3. Provide signed releases on a single page if possible. EPSQ will often print releases on two pages depending on the amount of information entered on the SF86 or SF85P. While these are acceptable, it is preferred that you provide a single page release. A blank copy of these releases is available for download at: http://www.dss.mil/epsq/download_release.htm.

Detailed information regarding how to attach scanned images to EPSQ data transmissions can be found at http://www.dss.mil/epsq/epsqfaq/epsqfaq7.htm. In addition, questions can be directed to DSS' Customer Call Center (1-800-542-0237).

If you are unable to transmit the releases electronically, they may be mailed either on diskette or in hard copy to the address below. This address should also be utilized for transmitting Fingerprint Cards and/or any other supporting documentation to DSS, and is appropriate for either U.S. Mail or an overnight delivery service such as Federal Express.

National Agency Records Processing Group (NARP)
Defense Security Service
601 10th Street Suite 125
Fort George G. Meade, MD 20755-5134

5. Facilitating Reinstatements/Conversions of Personnel Security Clearances for Industry

Since January 29, 1999, there has been a waiver of the requirements of paragraphs 2-215 and 2-217 of the NISPOM. Contractors can reinstate a clearance by receiving from the losing facility a copy of the letter of consent, a copy of the DISCO Form 562 that terminated the clearance, and submitting a DISCO Form 562 to DSS. We have received numerous inquiries as to whether this waiver applies to the reinstatement of interim clearances. The waiver does apply to interim clearances. The same procedures should be used as are used for reinstating final clearances.

6. Periodic Reinvestigations (PR)

When requesting a PR via EPSQ, contractors have the choice between requesting an SBPR or an SPR. SBPR stands for Single Scope Background Investigation (SSBI) Periodic Reinvestigation. This choice should only be selected in cases where the applicant has already been the subject of a completed SSBI. In most of these cases, the applicant will have a Top Secret clearance. SPR stands for Secret Periodic Reinvestigation and should be selected in cases where the applicant has a Secret or a Confidential clearance based on a National Agency Check (NAC), or NAC, Local Agency Check, and Credit Check (NACLC). DISCO has noticed that some contractors request an SBPR when they actually need an SPR. This can result in processing delays. All contractors are asked to keep the above information in mind when requesting PRs. Also, fingerprint cards must be submitted for SPRs (Secret and Confidential PRs). Fingerprint cards are not required for SBPRs (Top Secret PRs), though occasionally, DISCO may request a fingerprint card after they receive a SBPR request.

7. Important EPSQ Privacy Warning

There is an EPSQ compatibility problem for Industrial/Contractor subjects. EPSQ 2.2 Subject Edition allows the subject of the investigation to use a password to shield certain required information from the facility security officer while simultaneously making the data available to the Government. Under certain circumstances, EPSQ 2.2 Subject Edition may not preclude access to this information by the Facility Security Officer (FSO). This occurs when the FSO uses an earlier version of EPSQ Security Officer Edition to process the request for investigation.

In order to ensure that the privacy interests of individuals are properly protected in accordance with NISPOM paragraph 2-218, immediate conversion to version 2.2 for Subject and Security Officer Edition must occur. If you have any questions regarding this matter, please contact the EPSQ Help Desk at 1-800-542-0237 or email to epsq_questions@mail.dss.mil.

EPSQ version 2.2 software can be downloaded from the DSS website at
http://www.dss.mil/epsq/

We apologize for any problems caused by this error.

8. Shut Down of .MIL Web Servers

Last year, the Code Red Worm Virus impacted a large number of computer systems and flooded the Internet with useless computer network traffic that threatened to overwhelm it. In response to this threat, the Department of Defense (DoD) closed their computer network called the NIPRNET (Non-Classified Internet Protocol Routed Network) to certain kinds of computer traffic coming from the Internet. As a result, while DoD traffic could pass back and forth to the Internet, users outside the NIPRNET that tried to access web locations on the NIPRNET were unable to do so. This meant that contractors and non-DoD government employees who did not have direct access to the NIPRNET could not gain access to DoD sites to include the DSS web site.

Because of the continued cyber threat future shutdowns of .mil web servers are possible for a given time period. If this occurs IS Reps will notify DoD contractors via e-mail. Also, below are direct links to automated DSS services that may be utilized:

-To download the most current version of EPSQ:
https://sclient.dss.mil/download/

-To access your EPSQ Receipts and Electronic LOCs:
https://sclient.dss.mil/epsq/

-To access the DSS Academy ENROL system:
https://enrol.dss.mil/enrol/default.asp

-To access the DSS CVA system:
https://sclient.dss.mil/isscva/index.htm

9. Reports Submitted to the CSA – NISPOM Paragraphs 1-302, 1-303, and 1-304

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

  - Adverse Information
  - Change in Cleared Employee Status (via EPSQ Form 562)
  - Representative of a Foreign Interest
  - Citizen by Naturalization (via EPSQ Form 562)
  - 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

This supercedes the guidance provided in ISL 95L-1, item 5.

10. Verification of Facility Clearance (FCL) Associated With Classified Visits

Contractors hosting classified visits and receiving Visit Authorization Letters (VAL) must verify that the contractor requesting the visit has the appropriate FCL level. This requirement is implied but not specifically stated in NISPOM paragraph 6-109. If the visit is contract-related, the contractor may have already verified the FCL when the DD Form 254 was issued. However, if the visit is non-contract related, the host contractor must verify the FCL level of the requesting contractor prior to accepting the VAL. FCLs can be verified by calling the Central Verification Activity (CVA) at 1-888-282-7682 or via the DSS web site at www.dss.mil (click on Information Utility and follow the instructions to access the CVA).

11. Clarification Regarding Receipt and Dispatch Records for Classified Information Transmitted Electronically

Article 7 of Industrial Security Letter (ISL) 00L-1, titled "Receipt and Dispatch Records for Classified Information Transmitted Electronically," reminded contractors that receipt and dispatch records (NISPOM paragraph 5-202) are required when transmitting classified information electronically. Discussed in the Article was the option of utilizing either manual or automated record systems provided each include the required five reflected items. Numerous questions and concerns have been received from industry regarding this article resulting in a second look at the implementation of this requirement.

The intent of requiring receipt and dispatch records for classified information transmitted electronically remains valid. Contractors are required by paragraph 5-200 to establish an information management system and control all classified information in their possession. The problem facing industry with this requirement is the volume of receipt and dispatch records that can be generated by an accredited Information System (IS). The following guidance is intended to assist in that regard:

a. Protection Level 1 (formerly Dedicated Security Mode), connections between entities with direct contractual relationship. Record in document control each facility that information is transmitted to or received from by CAGE code, contract number, expiration date and classification level. This information is recorded once and updated upon change in contract status. Records shall be retained for 2 years from the termination of the contract or when the connection is no longer required, which ever is sooner.

b. Protection Level 1, connections between entities without direct contractual relationship. For each classified session, the audit requirements identified for Audit 1 (May 1, 2001 NISPOM Chapter 8, paragraph 8-602a) will record the required information. In the event the IS cannot provide an automated audit capability, the contractor is required to capture the information in a manual receipt and dispatch log. Records shall be retained for 2 years.

c. Protection Levels 2, 3 and 4 (formerly System High, Compartmented and Multilevel Security Mode). For each classified transmission, the audit requirement identified for Audit 1 (May 1, 2001 Chapter 8, paragraph 8-602a) will record the required information. All receipt and dispatch records shall be retained for 2 years. For IS that utilize an automated audit capability, an audit reduction tool can be used to extract the required information from the raw audit records or the entire automated audit records must be retained for 2 years.

12. Certified Mail Transmitted Over the Internet

The United States Postal Service (USPS) recently began providing certified mail service over the internet. The USPS is promoting this service to save time, money and eliminate errors. **The use of the USPS certified mail process over the internet is not approved for the transmission of classified information.**

13. Intrusion Detection Systems (IDS) – NISPOM Paragraph 5-901

As a reminder, in accordance with NISPOM paragraph 5-901, previously approved Intrusion Detection Systems (IDS) used for the protection of classified information were required to be in compliance with UL Standard 2050 or Director of Central Intelligence Directive (DCID) 1/21 by January 1, 2002. Facilities with IDSs currently in use that do not meet either of these standards must take immediate action to bring their systems into compliance. Questions regarding this issue should be referred to your Industrial Security Representative.

14. Disclosure of Unclassified Information Pertaining to Classified Contracts to the Public

DSS has received several inquiries from contractors regarding implementation of NISPOM paragraph 5-511 which prohibits disclosure of unclassified information relating to classified contracts to the public without prior review and clearance as specified in the Contract Security Classification Specification or as otherwise specified by the [Cognizant Security Agency] CSA or [Government Contracting Activity] GCA.

The NISPOM, Appendix C, defines the public as "any contractor, subcontractor, Government official, or "other" individual who does not require access to information (classified or unclassified) in furtherance of the performance of [a] classified contract under which the information was provided to the contractor or as authorized by [the NISPOM]." Viewed strictly, this definition would include uncleared employees that do not possess the requisite need-to-know for unclassified information relating to a classified contract, as well as cleaning crews, maintenance personnel or others operating within a cleared facility. As the CSA, DSS believes a literal interpretation of NISPOM paragraph 5-511 is too restrictive, unproductive, and unenforceable.

The intent of the requirement is for contractors to request release authority before making unclassified information related to classified contracts available to the general public. It is recognized that operationally it is impractical for contractors to implement such a requirement for the individuals such as those identified in the above paragraph, who are provided access to contractor space. Therefore, such individuals are not considered "the public" in regard to NISPOM paragraph 5-511, and public release authorization is not required. Instead, contractors should make a good faith effort to incorporate security procedures that would minimize such individuals' capability to access unclassified contract information. Such security measures could include procedures already in place at many contractor facilities to protect proprietary information, Technology Control Plans (TCP) in place to protect unclassified controlled technology and/or information from disclosure to foreign national employees, subcontractors, owners, or visitors, or other applicable security measures.

15. DSS Academy Schedule of Courses for Fiscal Year 2002

Listed below are the schedule of Facility Security Officer (FSO) Program Management and Information Systems Security Procedures for Industry courses scheduled for the remainder of Fiscal Year 2002:

FSO Program Management Course

May 7-9, 2002	Los Angeles, CA
May 14-16, 2002	Buffalo, NY
July 9-11, 2002	Minneapolis, MN
August 20-22, 2002	Atlanta, GA
September 10-12, 2002	Seattle, WA
September 17-19, 2002	Linthicum, MD

Information Systems Security Procedures for Industry Course*

May 7-9, 2002	Los Angeles, CA
May 14-16, 2002	Buffalo, NY
July 9-11, 2002	Minneapolis, MN
August 20-22, 2002	Atlanta, GA
September 10-12, 2002	Seattle, WA
September 24-26, 2002	Linthicum, MD

* Note: Course Previously called AIS Security Procedures for Industry

16. Updated DD Forms 441, 441-1 and Standard Form 328

The "Department of Defense Security Agreement"(DD Form 441), "Appendage to the Department of Defense Security Agreement"(DD Form 441-1) and the "Certificate Pertaining to Foreign Interests" (SF-328) have been revised and are to be used immediately. The forms have an issue date of July 2001, and expire June 30, 2004. DD 441, 441-1 and SF 328 forms executed prior to July 2001 remain valid. However, the new forms must be utilized when there are changed conditions requiring the forms be re-executed.

You may access the forms from the Web Sites listed below:

http://web1.whs.osd.mil/icdhome/DDEFORMS.HTM (DD Form 441 and 441-1)
http://web1.whs.osd.mil/icdhome/SFEFORMS.HTM (SF-328) or
http://www.dss.mil/seclib/forms.htm

You must have Adobe Acrobat Reader on your system to view and download the form(s). Copies of the forms will also be available from your local DSS Industrial Security Representative.

17. Revised Standard Form 312

Effective June 30, 2001 the "Classified Information Nondisclosure Agreement" Standard Form 312, revised January 2000 was to be used instead of the January 1991 version. It is not necessary to re-execute SF 312s that have already been accomplished using the old version. SF 312s must be executed by cleared employees prior to being granted access to classified information (paragraph 3-105, NISPOM).

The SF 312 and the supporting pamphlet were revised by the Information Security Oversight Office (ISOO) to incorporate the provisions of Executive Order 12958, "Classified National Security Information", which superceded Executive Order 12356, and Title 18, Section 1924, "Unauthorized Removal and Retention of Classified Documents or Material". Copies of the pamphlet, dated Spring 2001, can be ordered by sending an e-mail request to: isoo@nara.gov or by calling (202) 219-5250. The pamphlet can also be obtained on the National Archives and Records Administration's Web Site:

http://www.nara.gov/isoo/training/seced.html

18. Q&A – SF-312

Question: Is the Facility Security Officer (FSO) the only facility employee that can sign the acceptance block on the SF 312? ISL 95L-2 only addresses FSOs, but does not address other security officials under the FSO in the same office.

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 a KMP (Key Management Personnel).

19. Q&A – Formerly Restricted Data (FRD)

Question: Can an individual with an Interim personnel security clearance (PCL) be permitted access to FRD at the level of the Interim PCL?

Answer: Yes. While there appears to be conflict between NISPOM paragraphs 9-105e-f and 2-212a, the provisions of paragraph 2-212a govern. An Interim PCL is valid for access to FRD information at the same or lower level as the interim PCL.