1-3-EXB- CR

DEPARTMENT OF DEFENSE • DEFENSE INVESTIGATIVE SERVICE • DIRECTORATE FOR INDUSTRIAL SECURITY

INDUSTRIAL SECURITY LETTER

07 SEP 1988

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. Information contained herein does not represent a change of policy or requirements until and unless officially incorporated in the Industrial Security Manual. 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 or ideas contributed will become the property of DIS. Contractor requests for copies of the Letter and inquiries concerning specific information should be addressed to the cognizant security office, for referral to the Directorate for Industrial Security, HQ DIS, as appropriate.

ISL 88L-3 August 04, 1988

1. NEW DIRECTOR OF THE DEFENSE INVESTIGATIVE SERVICE
2. CLASS 2, 3 AND 4 GSA APPROVED CONTAINERS
3. DESK INSPECTIONS
4. ACCESS LIMITATIONS FOR IMMIGRANT ALIENS ISSUED LIMITED ACCESS AUTHORIZATIONS (LAA's)
5. ACCESS LIMITATIONS OF FIRMS GRANTED A RECIPROCAL FACILITY SECURITY CLEARANCE
6. COMSEC BRIEFINGS
7. SINGAPORE SECURITY CLASSIFICATIONS
8. SECURITY BRIEFINGS
9. PURPOSE OF PIC-CVA
10. FEDERAL SUPPLY CODE (FSC) OR COMMERCIAL AND GOVERNMENT ENTITY (CAGE) NUMBER REPORTING REQUIREMENT
11. TELEPHONE CALLS TO DISCO
12. PREEMPLOYMENT CLEARANCE ACTION
13. NSA STU-III HOTLINE
14. ADVERSE IMPACT OF BUDGET CUTS UPON DISCO PROCESSING TIMES
15. DEPARTMENT OF DEFENSE SECURITY INSTITUTE (DoDSI) SCHEDULE OF COURSES FOR FISCAL YEAR 1989

1. NEW DIRECTOR OF THE DEFENSE INVESTIGATIVE SERVICE (DIS)

Effective August 3, 1988 Mr. Thomas J. O'Brien, Director DIS, officially retired and Mr. John F. Donnelly, Assistant Deputy Under Secretary of Defense (Counterintelligence & Security), succeeded him.

Mr. Donnelly has had several significant assignments in his distinguished 37 years of Federal Service. He spent 30 years with the Naval Investigative Service (NIS) in a variety of key positions. In 1981 he was selected as the Director for Counterintelligence and Investigative Programs, Office of the Deputy Under Secretary of Defense for Policy, where he served until he was elevated to his prior position.

Mr. Donnelly's career has been characterized with numerous awards to include the Rank of Meritorious Executive which was bestowed to him by President Reagan in 1985.

2. CLASS 2, 3 AND 4 GSA APPROVED CONTAINERS

Recently, questions have been raised concerning utilization of class 2, 3 and 4 GSA approved security containers for safeguarding SECRET material. Providing the integrity of these containers has never been altered, they are still GSA approved and may be used to safeguard SECRET information. All repairs on such containers must be in accordance with the requirements of paragraphs 14f and g of the ISM.

3. DESK INSPECTIONS

Most misunderstandings of the DIS office/desk inspection policy can be traced to a lack of awareness on the part of the cleared contractor employee as to the nature and scope of an inspection.

DIS' inspections are designed to review the handling and safeguarding of classified material. Proper handling of classified material is the responsibility of every person entrusted with a clearance.

It is incumbent upon each cleared individual to be aware of his/her responsibilities and duties with respect to handling and storing of classified material. In this regard it is the contractor's responsibility to remind all cleared employees regarding the proper handling, safeguarding and storage of classified material (5g, ISM). Contractors should also inform their employees that their work area is subject to inspection by both the government and the contractor, to include desks, credenzas and other repositories not approved to store classified material. This notification should be accomplished in a positive manner so as to increase security awareness.

We believe that by so informing your employees, misunderstandings regarding this inspection technique will be eliminated and avoided in the future.

4. ACCESS LIMITATIONS FOR IMMIGRANT ALIENS ISSUED LIMITED ACCESS AUTHORIZATIONS (LAA's)

Significant changes were made in the November 1986 edition of the ISM regarding access to classified information by immigrant aliens. Immigrant

aliens are no longer eligible for a Personnel Security Clearance (PCL); however, they may be eligible for an LAA provided certain conditions are met. These conditions are specified in paragraph 31.1a of the ISM.

Any request that an immigrant alien be permitted access to classified information for performance on a specific government contract must be endorsed by the UA authority with jurisdiction over that contract. The UA endorsement of the request must be based upon an assessment that considers possible damage to the U.S. from a technology and military capability standpoint should the information be compromised. The assessment must also include a statement as to whether the information would be releasable to the individual's country of citizenship. Once the LAA has been granted by DISCO, the contractor is required to maintain a record of the information listed in paragraph 31.1d. By way of emphasis, access to classified information must be limited to that identified in the above mentioned record maintained by the contractor. Therefore, this record must be specific as to the information approved for access. Access to any other classified information is prohibited without first obtaining another endorsement from the contracting officer which must also include the information required in an initial LAA application. An LAA is valid only as long as a need remains to access information approved under a specific contract. When the last of any such contracts expire, prompt administrative termination of the LAA must be reported to DISCO.

5. ACCESS LIMITATIONS OF FIRMS GRANTED A RECIPROCAL FACILITY SECURITY CLEARANCE

We have recently received questions concerning paragraph 31.3b, ISM. Some contractors are of the opinion that if a contract does not specifically state that information is not releasable, then the information can be released to the country from which foreign ownership, control or influence is derived. The restrictions apply to all classified information unless specifically designated as releasable to a particular foreign country.

6. COMSEC BRIEFINGS

Paragraph 11 of the March 17, 1988 COMSEC Supplement (CSISM) indicates that the employee's briefing would be recorded on the Classified Information Nondisclosure Agreement (Industrial/Commercial/Non-Government) (SF-189A). Subsequent to the time the CSISM was transmitted to the Government Printing Office for publication, use of the SF-189A was prohibited. Until further notice, the employee's record of briefing/debriefing need not be on a particular form but must continue to be kept for a minimum of five years from the date of the debriefing.

Appendix II, COMSEC Briefing, Paragraph G, lists the laws which apply to the protection of COMSEC materials. Most applicable sections of Title 18, U.S. Code, are among those printed in Appendix VI to the Industrial Security Manual (ISM). However, one of the cited sections, §952, is not included in the ISM. The wording of §952, in its entirety, is as follows:

§952. DIPLOMATIC CODES AND CORRESPONDENCE

Whoever, by virtue of his employment by the United States, obtains from another or has or has had custody of or access to, any official diplomatic code or any matter prepared in any such code, or which purports to have been prepared in any such code, and without authorization or competent authority, willfully publishes or furnishes to another any such code or matter, or any matter which was obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States, shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

This statute section will be added to Appendix VI when the next change is published.

7. SINGAPORE SECURITY CLASSIFICATIONS

The Government of Singapore (GOS) advises that their classification levels are as follows: TOP SECRET, SECRET, CONFIDENTIAL, and RESTRICTED. According to our General Security of Military Information Agreement, the United States will protect Singapore classified information in the same manner as we protect U.S. classified information. Since the U.S. does not have a RESTRICTED classification, we have historically protected foreign RESTRICTED information as if it were U.S. CONFIDENTIAL. The GOS advises that based on their comparison of U.S. procedures for safeguarding "FOR OFFICIAL USE ONLY" information and the security measures required for the GOS's security classification of RESTRICTED, GOS RESTRICTED information may be protected in the same manner as U.S. FOUO material.

The specific requirements governing handling and storage of GOS RESTRICTED material follow:

1. A security clearance is not required for access to GOS RESTRICTED material.

2. During normal working hours, the material must be placed in a location not visible to personnel without a need-to-know if the work area is accessible to them. While in use, documents shall not be left unattended, but shall be in the physical possession or under surveillance of an authorized person at all times. An authorized person is an individual whom management has determined needs access to the specific project.

3. At the close of business, GOS RESTRICTED records may be filed with other unclassified material in unlocked file cabinets or desks if internal building security is provided during non-duty hours. If such internal security is not provided, locked buildings or rooms normally provide adequate after-hours protection. If this is not the case, the material should be stored in locked receptacles such as file cabinets, desks, or bookcases.

4. GOS RESTRICTED material will be destroyed by burning or other means approved for destruction of classified information.

5. GOS RESTRICTED material hand-carried short distances does not require an envelope or wrapping; however, if it is being carried by a person in official travel status, it must be placed in a gum sealed envelope.

6. GOS RESTRICTED may be mailed using first class mail and may be single wrapped.

7. When transferring GOS RESTRICTED, the dispatch/receipt must be recorded by the sender/recipient respectively.

8. GOS RESTRICTED material may be transmitted over non-secure electronic means.

8. SECURITY BRIEFINGS

Industrial Security Letter 88L-1 advised that the SF 189A was no longer to be utilized but that briefings of cleared personnel were to be continued and a record maintained of all personnel briefed. We have subsequently been asked what should be included in the record.

There is no prohibition against the use of the obsolete DD Form 482; however, this form can no longer be procured from DISCO. You may also create your own briefing statement, if you wish.

As a minimum, the record should include: 1) the name and signature of the person being briefed; 2) the name of the person who performed the briefing; 3) date of the briefing; and 4) a statement whereby the individual is aware of sanctions that may result from unauthorized disclosure of classified information. Although not a requirement at this time, it is an excellent practice to retain a copy of the briefing in order that there is evidence of what the employee was told. This evidence is especially beneficial to a thorough investigation and resolution of security violations.

9. PURPOSE OF PIC-CVA

Recently the number of telephone calls to the Personnel Investigations Center-Central Verifications Activity (PIC-CVA) for purposes other than verification of clearance and safeguarding capability of cleared contractor facilities (i.e., to determine mailing address, telephone number, etc.) have increased. Please limit calls to the PIC-CVA to legitimate verification requirements. To do otherwise detracts significantly from the PIC-CVA mission and results in additional expense to the government. It is requested that other sources be utilized for obtaining general information regarding cleared contractor facilities. Your cooperation is greatly appreciated in this matter.

10. FEDERAL SUPPLY CODE (FSC) OR COMMERCIAL AND GOVERNMENT ENTITY (CAGE) NUMBER REPORTING REQUIREMENT

Cleared contractors or contractors in process for a facility clearance are reminded that any change in the facility's name or address is required to be reported by letter to the Defense Logistics Service Center (DLSC), ATTN: DLSC-FBAB, 74 North Washington, Battle Creek, Michigan 49017-3084, as they occur. Failure to report this information to DLSC could result in administrative problems associated with verification of the facility's FSC and CAGE numbers which are necessary for procurement distributions and/or processings. You are reminded that you must also report any such changes to your Cognizant Security Office in accordance with paragraph 6a(4) of the ISM.

DIS is aware of the fact that the same information is reported to two different government offices and we are attempting to work out a solution; however, in the meantime, please help yourself and the government to keep your facility's name and address records current.

11. TELEPHONE CALLS TO DISCO

The DISCO status line, (614) 238-2265, was created for the purpose of providing status of in-process industrial security clearance applications. Two operators (three operators during peak hours) handle approximately 228,000 inquiries per year. A survey conducted by a DISCO Quality Circle indicated that over 40% of these inquiries are for verification of existing clearances or to obtain investigative data. In order to reduce the number of these telephone inquiries, the type of investigation and the date of investigation will now appear as the last two columns of the MEAD System Validation List.

Facility Security Officers may request this listing in writing from the Defense Industrial Security Clearance Office, ATTN: S0823, P.O. Box 2499, Columbus, Ohio 43216-5006. The following information must be included on the request:

Name of Facility - Facility Code - Address (with attention line) of requester.

The request should be initiated at least four weeks prior to your need for this information. Anyone with questions concerning the MEAD Validation List should telephone (614) 238-2329 or AUTOVON 850-2329.

As you know, DIS started to reflect the type of investigation and the date of investigation on letters of consent printed after January 1, 1988. The addition of this data to the validation lists should eliminate all such requests by telephone. Therefore, DISCO will not respond to telephone inquiries for this information after July 1, 1988.

12. PREEMPLOYMENT CLEARANCE ACTION

The contractor shall not initiate any preemployment clearance action except as provided for in this paragraph. An applicant for employment in a position that requires access to classified information may be informed that a PCL will be required. A personnel security questionnaire may be given to such an individual being considered for employment, but the contractor shall not obtain or review the completed form until after the individual is employed and placed on the payroll. However, in exceptional cases the completed application forms may be obtained and submitted to DISCO prior to the date of entry on duty. The exception is limited to cases in which a written contract for future employment has been executed between the prospective employee and the employer that prescribes a fixed date for entry on the payroll, normally not to exceed 120 days from the effective date of the employment contract.

13. NSA STU-III HOTLINE

During the next few months, over 80,000 STU-III low-cost terminals will be delivered to government users and defense contractors. To assist with implementation of the STU-III system, NSA has established a toll-free hotline.

For callers outside the state of Maryland, the number is 1-800-328-STU3 (328-7883); within Maryland, dial commercial (301) 688-5718. Autovon subscribers may call 235-5718.

The NSA User-Relations Staff will answer questions pertaining to STU-III policy, doctrine, operating procedures and security issues. The previous numbers (688-7214/7897/8255) are no longer accessible to the User Relations Staff. However, other members of the STU-III Special Project Office can still be reached on these numbers.

14. ADVERSE IMPACT OF BUDGET CUTS UPON DISCO PROCESSING TIMES

Most of you are already aware that the DIS budget was significantly reduced for FY 88. Continuing reductions are anticipated for FY 89. As a result, an agency-wide hiring and promotion freeze was implemented for 1988, and lowered personnel resource ceilings have been established for 1989. DISCO has experienced a reduction of approximately 20% of its work force and more losses are anticipated in the near future. You should already be noticing an increase in processing times for DISCO actions. These increases are most noticeable in the area of initial security clearance requests, which are now taking DISCO as long as 4 weeks to act upon. DIS has taken measures to try to control these increasing processing times. However, delays will be largely unavoidable until hiring can commence.

In order to speed the processing of clearance record update actions, DISCO has temporarily suspended the confirmation of multiple facility transfers, downgrades and consultant status changes. You will continue to receive confirmation of all other actions as you have in the past.

We appreciate your patience and understanding in helping us to cope with these budget cuts. We anticipate most of these inconveniences will be temporary.

15. DEPARTMENT OF DEFENSE SECURITY INSTITUTE (DoDSI) SCHEDULE OF COURSES FOR FISCAL YEAR 1989

The Department of Defense Security Institute (DoDSI), Richmond, Virginia, offers a variety of courses for personnel in industry.

The Industrial Security Management Course (ISMC) is designed to provide U.S. contractor personnel with a general understanding of the Defense Industrial Security Program as it applies to requirements and administrative procedures involved in safeguarding classified defense information in the possession of U.S. industry. It is offered in both resident and field extension formats. [NOTE: All Facility Security Officers (FSO's) who assumed their positions after July 1, 1987 are required to attend the ISMC within twelve months of their assignment if their facility has safeguarding capabilities (see paragraph 5a, ISM).]

The AIS Security Procedures for Industry Course is designed to provide practical experience in development of AIS Standard Practice Procedures (SPP's) and an understanding of the requirements pertaining to the processing

of classified defense information in data processing and office automation systems located in U.S. contractor facilities. This course is offered only as a field extension.

INDUSTRIAL SECURITY MANAGEMENT COURSE AND AIS SECURITY PROCEDURES FOR INDUSTRY COURSE

DATE	HOST REGION	LOCATION
Oct 3-7, 1988	Southeastern	Richmond, VA
Oct 31 - Nov 4, 1988	Southwestern	Richmond, VA
Nov 14-18, 1988 (*)	New England	Woburn, MA
Dec 12-16, 1988	Mid-Western	Richmond, VA
Jan 9-13, 1989	Mid-Atlantic	Richmond, VA
Feb 27- Mar 3, 1989 (*)	Northwestern	San Francisco, CA
Mar 6-10, 1989	Northwestern	San Francisco, CA
Mar 13-17, 1989 (*)	Southeastern	Atlanta, GA
Apr 17-21, 1989	Pacific	Costa Mesa, CA
Apr 24-28, 1989 (*)	Pacific	Costa Mesa, CA
Jun 12-16, 1989	New England	Richmond, VA
Jun 19-23, 1989	Southwestern	Dallas, TX
Jul 10-14, 1989 (*)	Capital	Washington, DC
Jul 17-21, 1989	Capital	Washington, DC
Aug 14-18, 1989 (*)	Mid-Western	Chicago, IL
Sep 25-29, 1989 (*)	Mid-Atlantic	Cherry Hill, NJ

NOTE: Registration for ISMC's held in residence at DoDSI will still be handled through the respective DIS host Region.

(*)- INDICATES THOSE INSTANCES WHERE THE AIS SECURITY PROCEDURES FOR INDUSTRY COURSE WILL BE HELD CONCURRENTLY.

Robert G. Schwalls

ROBERT G. SCHWALLS
Deputy Director
(Industrial Security)

Attachment

1. STATEMENT OF QUESTION/PROBLEM: Paragraph 5aa, ISM, states in part that contractors are required to make employment and security records available for review on request by DIS Special Agents conducting personnel security investigations. Are company "investigative records" included in the term security records?

ANSWER: The intent of this requirement is to allow DIS Special Agents conducting personnel security investigations access to all information maintained by the facility which reflects upon that individual's integrity, character and overall ability to safeguard classified information. Investigative records certainly fall into this category.

2. STATEMENT OF QUESTION/PROBLEM: In a job announcement a contractor cannot say that the job requires a security clearance. What can the contractor state?

ANSWER: Cleared contractors may not advertise the fact that a PCL is a condition of or a prerequisite for employment. This policy exists to ensure that employment opportunities are not limited to only those individuals who may presently possess a PCL or are eligible for reinstatement, transfer or conversion of a clearance. The writing of help wanted ads is not a matter under the purview of the DISP so long as the ad's wording complies with the above.

3. STATEMENT OF QUESTION/PROBLEM: What level of clearance must a guard acting as supplemental controls in accordance with 14a(2) and (4) possess?

ANSWER: A guard who performs supplemental controls will be cleared to the level of SECRET regardless of the level of classified information involved. This is reflective of the fact that guards who perform supplemental controls are cleared, not because they have access to classified information, but rather because they are an integral part of the contractor's system to protect classified information. Guards should have the ability or opportunity to gain knowledge of classified information only if someone else commits a security violation. Even in those cases, their instructions should be such that we can be reasonably sure that the guard does not obtain knowledge of classified information in such a situation. Of course, if a guard has an independent need to access TOP SECRET information, then of course he or she must be cleared TOP SECRET.

4. STATEMENT OF QUESTION/PROBLEM: Paragraph 20a, ISM, requires that the supervisor certify the need for access when a clearance is requested. Does this mean that some record must be kept of the certification and that it be available for review by the IS Rep during inspection?

ANSWER: The contractor must have a system, detailed in the SPP, for limiting PCLs. The system must identify those required to make the deliberate decision as to a particular individual's need for a clearance and those who review the decision. Thus, an IS Rep should only approve an SPP which sets forth a system of documentation which can be inspected to assure it is effective.

Attachment 1

Normally, the certification should be by the individual's supervisor and submitted by the supervisor to the security office for retention. The justification should be sufficiently detailed to include a description of the individual's duties that necessitates access to classified information. The contract(s) involved should be identified on the justification unless to do so makes the justification classified. However, simply listing the contract number without a description of duties that require access would not meet the intent of paragraph 20.

5. STATEMENT OF QUESTION/PROBLEM: Do the policies and procedures contained in the Industrial Security Manual (ISM) pertain only to cleared employees, and personnel in process for a PCL, or do they also pertain to certain uncleared personnel? As a case in point, paragraph 5u(2) ISM makes reference to the fact that contractor "employees engaged in marketing activities with representatives of Designated countries shall also be provided with a defensive security briefing based on the guidance contained in Appendix VII, ISM." Paragraphs 4a, b, c, and d of Appendix VII elaborate upon the role of the marketing representative and the reasons for an awareness briefing. However, clarification is requested as to whether or not this requirement applies to personnel who do not have and are not being processed for a PCL.

ANSWER: Actually, the requirements in the ISM pertain to cleared facilities. The facility then has the responsibility for developing procedures to ensure that the requirements of the ISM are met. In some cases, this may involve the briefing of uncleared employees. A defensive security briefing in accordance with paragraph 5u and Appendix VII, ISM is necessary to adequately ensure and prevent an uncleared employee from unintentionally divulging to a representative of a Designated country, even unclassified information if it relates to a classified contract. Thus, it is essential that all personnel who participate in visits and/or engage in marketing activities with representatives of designated countries be provided with the briefing.

6. STATEMENT OF QUESTION/PROBLEM: Must a Visit Access Request (VAR) be on file for a visitor to a facility who is only releasing classified material to the facility visited?

ANSWER: NO. A person acting solely as a courier, similar to your local postman, is not considered a visitor within the context of the ISM.

7. STATEMENT OF QUESTION/PROBLEM: Paragraph 73c of the ISM states that if only classified documents are provided to another facility within an MFO and the documents themselves provide the necessary classification guidance, no further classification guidance need be provided. What is considered necessary guidance? Are the classification markings required by paragraph 11, ISM considered to be adequate?

ANSWER: YES. The classification markings required by paragraph 11, ISM can be adequate classification guidance depending upon the performance requirements of the receiving facility.

8. STATEMENT OF QUESTION/PROBLEM: Does a package (containing classified material) left overnight at a cleared facility have to be entered into the facility's accountability or receipt and dispatch records if it is only left at the facility for temporary (overnight) storage?

ANSWER: YES. An entry should be made in the facility's accountability or receipt and dispatch records to identify the dates on which a classified sealed package was received and dispatched from the facility. The package should not be opened and the receipt system will not apply.

☆U.S. Government Printing Office: 1988—202-277/80002

Declassified and Approved For Release 2013/08/28 : CIA-RDP91B00390R000200120012-2

DEFENSE INVESTIGATIVE SERVICE
DIRECTORATE FOR INDUSTRIAL SECURITY
1900 HALF STREET, S.W.
WASHINGTON, D.C. 20324 -1700

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

BULK RATE
POSTAGE & FEES PAID
DEFENSE INVESTIGATIVE SERVICE
PERMIT No. G -131

ATTN: SECURITY SUPERVISOR