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

INDUSTRIAL SECURITY LETTER

ISL 2006-01 **April 14, 2006**

This Industrial Security Letter (ISL) coincides with the release of the revised National Industrial Security Program Operating Manual, DoD 5220.22-M (NISPOM), dated February 28, 2006. All previously published ISLs and other previously published guidance regarding NISPOM implementation are hereby rescinded. Previous ISL articles that are still pertinent will be reissued in subsequent ISLs. The revised NISPOM is available on the DSS website: www.dss.mil. A summary of the major NISPOM changes is also posted on the DSS website. The articles in this ISL provide additional guidance on selected NISPOM changes and are referenced by the appropriate NISPOM paragraph number.

1. **(1-102) Implementation of NISPOM Changes**
2. **(1-204) Cooperation with Contractors That Are Officially Credentialed Representatives of Federal Agencies**
3. **(2-200) Joint Personnel Adjudications System (JPAS)**
4. **(2-200 and 2-211) Interim PCLs**
5. **(2-202) Completion of Electronic SF86**
6. **(2-302) Procedures for Submitting Certificates Pertaining to Foreign Interests (SF 328)**
7. **(2-303) FOCI Action Plans**
8. **(4-107 and 4-216a) Material Marked for Automatic Declassification**
9. **(5-200) Information Management System**
10. **(5-202) Receiving Classified Material**

11. (5-202 and 5-401) Package Receipts and Receipt and Dispatch Records

12. (5-306) Securing Closed Areas

13. (5-306) Self-Approval Authority

14. (5-311) Container Repairs

15. (5-412 and 10-402) Escorts and Transfers of Freight

16. (6-104) Visitor Authorization

17. (Chapter 9 Section 1) RD and FRD

18. (Chapter 9 Section 3) Intelligence Information

19. (10-303) Foreign Government RESTRICTED Information and "In Confidence" Information

20. (10-401) International Transfers of Classified Material

21. (10-702) NATO Restricted

1. (1-102) Implementation of NISPOM Changes

All changes reflected in the February 28, 2006 issuance of the NISPOM must be implemented no later than 6 months from the publication date; that is, by September 1, 2006.

When a change to the NISPOM eliminates a requirement, the contractor may elect to continue that particular practice or procedure for operational necessity or convenience. However, such practices or procedures will not be subject to DSS inspection or oversight. In addition, DSS will not cite contractors for imposing processes or procedures that are no longer required, unless they are expressly prohibited in the NISPOM.

2. (1-204) Cooperation with Contractors That Are Officially Credentialed Representatives of Federal Agencies

Contractor investigators and any other contractor personnel who may carry official credentials issued by the Department of Defense, the Office of Personnel Management (OPM), or any other Federal Agency are to be afforded the same level of cooperation as required for officially credentialed government representatives. Those most likely to be encountered are contractor investigators credentialed by OPM conducting personnel security (i.e. background) investigations.

3. (2-200) Joint Personnel Adjudications System (JPAS)

The Department of Defense has designated JPAS as its system of record for contractor eligibility and access to classified information. This means that JPAS is the "CSA-designated database" referenced in the revised NISPOM (paragraph 2-200b). Industry has been using JPAS since mid-2004. The first step for contractors using JPAS is to "take ownership" of their employees in the system. Guidance can be found in the "JCAVS Desktop Resource" on the JPAS Gateway website (https://jpas.dsis.dod.mil/) under the FAQs heading. Section #2 of the Desktop Resource explains "How to Establish a Personnel Security Management Network (PSM Net)".

After almost 2 years of industry use of JPAS, a review of records in JPAS indicates over 18,000 contractor personnel whose records have no company affiliation. Contractors should ensure that all of their employees show their company/CAGE affiliation in the JPAS record. All unclaimed records will be purged from JPAS within the next year.

4. (2-200 and 2-211) Interim PCLs

The prohibition on eligibility for access to SAP and SCI information based on an interim PCL has been deleted. Eligibility for access to SCI and SAP information based on an interim PCL is a determination made by the granting authority.

5. (2-202) Completion of Electronic SF86

With the transition to eQIP, industry has been unable to view the employee/applicant's SF 86 due to Privacy Act concerns. Now that industry is not reviewing the forms, the reject rate for eQIP has gone up. Based on that information, a new procedure has been developed and industry will be able to review the forms with the April 2006 update to JPAS. The new procedures must be implemented before your company reviews employees' e-QIP submissions. The six month implementation for other provisions of the revised NISPOM does not apply for this particular requirement. Contractors that do not follow this procedure cannot review the employee/applicant SF 86 unless the employee/applicant has waived their right to privacy in writing.

The NISPOM revision requires that the facility security officer (FSO) and/or designee review the information on the SF 86 solely for completeness and not share the contents of the form with anyone else within the company. It requires written notification to the employee explaining the use of the information. Written notice can be as simple as giving the employee a copy of NISPOM paragraph 2-202. There is no requirement for the employee to certify that he/she has received this notification.

In most companies the FSO will be the reviewing official. Where this is not the case, particularly where a centralized personnel security clearance process has been established, either the corporate FSO or the FSO at the centralized location can designate personnel to do the review. It is not necessary for every contractor in the corporate family that uses a centralized process to specifically designate those persons to review the SF 86.

During security reviews, IS Reps will ask to speak to employees who recently completed their SF 86 to ensure that they received the required notice.

6. (2-302) Procedures for Submitting Certificates Pertaining to Foreign Interests (SF 328)

NISPOM paragraph 2-302 now states that "in the case of a corporate family, the form shall be a consolidated response rather than separate submissions from individual members of the corporate family." In the case of an organization with multiple tiers of parent-subsidiary relationships, the SF 328 should be certified by the highest tier cleared entity. This would not preclude a subordinate entity from preparing the SF 328 as long as the top tier cleared entity certified the answers on the form. This principle applies equally to changed condition reports submitted in accordance with NISPOM paragraph 1-302g (5). Finally, please note that the requirement to update the form every five years has been eliminated. Reports are requested only when material changes to the previously submitted SF 328 occur.

7. (2-303) FOCI Action Plans

Access to proscribed information by a company cleared under a Special Security Agreement (SSA) may require that the GCA make a national interest determination (NID) that release of proscribed information to the company will not harm the national security interests of the United States. The preparation of the NID is the responsibility of the GCA. It is the responsibility of DSS to determine the need for a NID and to request the NID from the GCA. The determination of the need for a NID or its preparation is never the responsibility of the contractor.

If there is no indication to DSS that the GCA will decline to make the NID, DSS will not delay implementation of a FOCI action plan pending receipt of the NID from the GCA.

8. (4-107 and 4-216a) Material Marked for Automatic Declassification

The term "automatic" declassification would seem to indicate that when classified material is marked with a declassification date, the contractor is authorized to automatically declassify the document. However, certain government agencies are concerned that, with all of the changes that have occurred to the declassification policy over the years, information may still retain sensitivity and therefore should not be "automatically" declassified.

When the contractor has material marked for automatic declassification, and notes that the date or event for the automatic declassification has occurred, the contractor must seek guidance from the government activity that released the information using the procedures of NISPOM paragraph 4-104. In effect, contractors are not authorized to unilaterally declassify even when the material is marked for automatic declassification.

9. (5-200) Information Management System

While the requirement to maintain external receipt and dispatch records for SECRET and CONFIDENTIAL information is eliminated, there is a requirement in the NISPOM for contractors to establish an information management system to protect and control the classified

information in their possession. The purpose of this requirement is to ensure that contractors have the capability to retrieve classified material when necessary and to ensure the appropriate disposition of classified material in a reasonable period of time. There is no required format for such an information management system, no expectation that such a system must be in an electronic database, or that such a system incorporates any form of receipt and dispatch records. The contractor merely has to demonstrate capability for timely retrieval of classified information within the company and the capability to dispose of any and all classified information in its possession when required to do so.

10. (5-202) Receiving Classified Material

Classified material coming into a facility, regardless of delivery method, must be received directly by authorized personnel. An authorized person means a cleared person who has been assigned this duty and therefore has need-to-know. The personnel who pick up the mail or accept deliveries from commercial delivery companies approved for transmitting classified material must be cleared to the level of classified material expected to be received by the contractor.

11. (5-202 and 5-401) Package Receipts and Receipt and Dispatch Records

The requirement to maintain external receipt and dispatch records for SECRET and CONFIDENTIAL information, regardless of the media of the information, has been eliminated.

While the requirement to maintain external receipt and dispatch records for SECRET and CONFIDENTIAL information has been eliminated, the requirement to include a receipt in the transmittal package for TOP SECRET and SECRET material remains. CONFIDENTIAL information does not require that a receipt be included in the transmittal package unless the sender deems it necessary. The receipt that is included in a transmittal package must be signed by the recipient and returned to the sender. The sender is required to maintain a suspense system to track transmitted material until a signed copy of the receipt is returned.

12. (5-306) Securing Closed Areas

Closed areas storing TOP SECRET and SECRET material must have supplemental protection during non-working hours. During non-working hours and during working hours when the area is unattended, admittance to the area must be controlled by locked entrances and exits secured by either an approved built-in combination lock or an approved combination or key-operated padlock. During working hours when the area is unattended, closed areas must be locked, but need not be alarmed.

The definition of working hours is that time during which the work force in the closed area is working on a regularly scheduled shift.

13. (5-306) Self-Approval Authority

Paragraph 5-306d of the NISPOM allows for the CSA to grant self-approval authority to qualified FSOs in establishing closed areas. The FSO may delegate this responsibility. Examples of qualifying criteria include successful experience following CSA procedures in establishing a closed area, completion of training which included classified material safeguarding and closed area requirements, and the facility security program having a CSA rating of satisfactory or better. If a cleared contractor facility wishes to nominate the FSO or designee to be authorized to approve closed areas, the facility should forward a request to the attention of the IS Rep responsible for the facility. The CSA will designate personnel granted this authority in writing.

14. (5-311) Container Repairs

While the procedures for repairing approved security containers have been removed from the NISPOM, repair standards have not changed. Repairs, maintenance, or other actions that affect the physical integrity of a security container must still be accomplished by appropriately cleared or continuously escorted personnel specifically trained in approved methods of maintenance and repair of containers.

15. (5-412 and 10-402) Escorts and Transfers of Freight

The requirement for escorts for classified shipments applies only when an escort is determined to be necessary to ensure the protection of classified information during transport.

NISPOM paragraph 10-402 discusses transportation plans and the conditions under which international carriers (e.g., commercial airlines) may be used to transport classified material internationally. The requirement for an escort is a matter to be determined by the U.S. approving authority for the transportation plan in consultation with the foreign government counterpart. Therefore, depending on specific circumstances and the judgment of the U.S. and foreign government approvers of the transportation plan, cleared escorts may or may not be required for international transfers.

16. (6-104) Visitor Authorization

The requirement for a visit authorization letter for classified visits within the Department of Defense is eliminated so long as the information necessary to verify the clearance of the visitor is available in JPAS and the contractor is able to determine the visitor's need-to-know. This does not apply to visits to or from other government agencies (Department of Energy, State Department, Department of Homeland Security, Department of Justice/FBI, etc). Contractors must still submit visit authorization letters to non-DoD agencies.

Contractors can control only their own processes for receiving incoming notifications of classified visits. Contractors will have to comply with the classified visit requirements established by other contractors and DoD activities that their employees are visiting. Employees should be informed that they may have to provide their SSNs to either the host of a classified

visit or to the receptionist/security officer of another contractor or DoD activity they will be visiting as part of the necessary clearance verification process.

When companies check the JPAS Person Summary screen for incoming visitors, they should:

- Verify the visitor's name and SSN.
- Check **current** access level to ensure the visitor can have access to the level of classified information to be disclosed.
- Check to ensure that the JPAS record shows a current affiliation with the contractor the visitor is representing.

As the contractor sponsoring the visit is not required to notify the site to be visited that the employee is no longer representing that contractor, a one-time check of JPAS for an on-going visit will not be sufficient. JPAS must be consulted regularly to ensure the access level and employment status of the visitor remains unchanged.

If a contractor is aware of locations that an employee frequently visits on a classified basis, and the employee is terminated, as a courtesy and in keeping with sound security practices, the contractor should notify the visited activities that the person is no longer employed or sponsored for visits.

The contractor should contact the DoD activities and other contractors prior to the scheduled arrival date of a visiting employee to determine how each organization wants to receive visitor data in order to verify the visitor's eligibility and access level. This will help ensure that employees are not denied entry.

17. (Chapter 9 Section 1) RD and FRD

This section was provided by DOE and applies to those contractors that are under DOE cognizance. It does not apply to contractors under DoD cognizance and should be considered as information only. Guidance on marking RD and FRD material must be included in the contract document. If adequate guidance has not been provided, the contractor should request assistance from the GCA.

18. (Chapter 9 Section 3) Intelligence Information

This section was provided by the Central Intelligence Agency (CIA) and should be considered as information only. Specific guidance on marking intelligence information must be included in the contract document. If adequate guidance has not been provided, the contractor should request assistance from the GCA.

19. (10-303) Foreign Government RESTRICTED Information and "In Confidence" Information

Protection and marking requirements for foreign government RESTRICTED and "In Confidence" information are to be incorporated into the contract by the foreign government. If such guidance has not been provided the contractor should contact DSS for assistance.

The requirement to protect foreign government RESTRICTED as U.S. CONFIDENTIAL must be specifically required by the foreign government and so indicated in the contract. If the contract does not include this protection requirement, the RESTRICTED and "In Confidence" information does not need to be protected as classified. However, the information shall not be disclosed to anyone except personnel who require access in connection with the contract.

20. (10-401) International Transfers of Classified Material

The requirement for the U.S. Designated Government Representative (DGR) to be a U.S. Government employee has been eliminated. This change permits DSS to authorize the contractor's FSO, empowered official (as defined by the International Traffic in Arms Regulations (ITAR)), or other knowledgeable individual to act as the DGR for international transfers of classified material.

21. (10-702) NATO Restricted

The requirement to protect NATO RESTRICTED information as U.S. classified has been eliminated. For access to NATO RESTRICTED, no FCL is required for the company, PCLs are not required for personnel, and neither certification nor accreditation are required for information systems. However, the information shall not be disclosed to anyone except personnel who require access in connection with the contract.