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

INDUSTRIAL SECURITY

LETTER

Industrial Security letters are issued periodically to inform cleared Contractors, 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. Suggestions for Industrial Security Letters are appreciated and should be submitted to the local Defense Security Service cognizant industrial security office. Articles and ideas contributed will become the property of DSS. Inquiries concerning specific information in Industrial Security Letters should be addressed to the cognizant DSS industrial security office.

ISL 2010-01 **January 28, 2010**

1. (NISPOM 1-204) Cooperation with Federal Agencies and Officially Credentialed Representatives of Those Agencies.

This article provides clarification of the requirement in NISPOM paragraph 1-204 for contractors to cooperate with Federal agencies and their officially credentialed representatives during personnel security (i.e., "background") investigations of present or former employees and others. The term "cooperation" in this NISPOM paragraph means providing suitable arrangements within the facility for conducting private interviews with employees during normal working hours, providing relevant employment and security records for review when requested, and rendering other necessary assistance.

Relevant employment records include all personnel files, security records, supervisory files, and other records pertaining to the individual under investigation, and in the possession, or under the control of the contractor's representatives or offices. Simply referring an investigator to an automated (telephone or computer) employment verification service is not sufficient for a personnel security investigation. It is necessary that employment files be reviewed during the course of a personnel security investigation for purposes beyond merely verifying the date(s) of employment and eligibility for rehire. On-scene investigators must be able to compare information in the employment record with the information listed by the applicant on the personnel security questionnaire to determine if there are discrepancies or variances.

Investigators also need to ascertain if the records contain any information that pertains to or may be relevant to the adjudication of the person's eligibility for access to classified information, such as garnishments, excessive absenteeism, security violations, etc.

Contractor investigators and any other contractor personnel who carry official credentials issued by the Department of Defense, the Office of Personnel Management (OPM), or any other Federal Agency who are conducting personnel security investigations 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 investigations.

2. (NISPOM 2-200b) Security Management Office (SMO) Contact Information in JPAS.

JPAS is the system of record for contractor eligibility and access to classified information for the Department of Defense. Within JPAS, each contractor's security office is represented by a SMO, which operates at a specified level and can be connected to other SMOs in ways that reflect real-world associations. The following is provided in accordance with NISPOM paragraph 2-200b, which states that specific procedures for the use of the system of record will be provided by the cognizant security agency (CSA).

SMO Account Managers must update all SMO contact information in JPAS by March 31, 2010. The current SMO office name and other identifying characteristics (such as phone and fax numbers and email addresses) are necessary to help Government security managers and facility security officers (FSOs) locate and contact one another. Providing up-to-date email contact information is necessary to support future capabilities that will enable security officers to receive vital access and eligibility information without the need to be logged into JPAS.

The SMO Maintenance screen allows Account Managers to create, deactivate, and delete SMOs. It also allows Account Managers to update office information, view all associated users for a SMO and maintain its parental (superior) relationships. An Account Manager must have the proper user level and be within the same Service/Agency to establish and maintain a SMO. Within JPAS, the Joint Clearance Access and Verification System (JCAVS) tutorial link provides instructions for SMO Maintenance.

When creating and maintaining SMOs in JPAS, Account Managers must enter the email address and all contact information on the SMO Maintenance screen and must keep all contact information current. Account Managers may enter multiple email addresses in the email text box within the SMO Maintenance screen; however, it is important to enter only email addresses in this box (***separated by commas***) and not names or telephone numbers.

Procedures:

- Log in to JPAS/JCAVS as the “Account Manager”
- At the Main Menu, click on "Maintain Security Management Office"
- Enter the SMO Code in the “Search Criteria” box
- Click the SMO code link at the bottom of the window to select the SMO for maintenance
- The "Security Management Office Maintenance" screen is displayed. To update SMO Contact Information:
    - **"Commercial Phone" Text Box:** This is a required field. Enter the area code and phone number for a point of contact at the SMO.
    - **"Commercial Fax" Text Box:** Enter the area code and phone number for a fax number in service at the SMO.
    - **"Email" Text Box:** Enter the appropriate email address information for a point of contact at the SMO. **Multiple email addresses must be separated by a comma. Do not enter names or telephone numbers in this field.**
- Click the [SAVE] button

3. (2-208) Acceptable Proof of Citizenship

In July 2008, the U.S. Department of State began issuing a Passport Card for entry by U.S. citizens into the U.S. from Canada, Mexico, and the countries of the Caribbean and Bermuda at land border crossings or sea ports-of-entry. The U.S. Passport Card, current or expired, is acceptable proof of U.S. citizenship for purposes of NISPOM paragraph 2-208.

4. (3-102) Required Facility Security Officer (FSO) Training

The NISPOM specifies contractors shall ensure the FSO completes security training considered appropriate by the cognizant security agency.

Successful completion of the following courses and associated examinations by FSOs will constitute compliance with the training requirements of NISPOM paragraph 3-102:

For FSOs of facilities not possessing classified information:

- FSO Role in the NISP Web-based course
- Essentials of Industrial Security Management (EISM)

For FSOs of facilities possessing classified information:

- FSO Role in the NISP Web-based course
- EISM
- Safeguarding Classified Information in NISP
- Derivative Classification
- Marking Classified Information
- Transmission and Transportation for Industry

These courses are provided by the Defense Security Service Academy and are available at the following website: http://dssa.dss.mil/seta/fso_curriculum_descrip.html.

5. (NISPOM 6-104a) Release of JPAS records.

JPAS, as a U.S. Government information system, contains official government records. The information in JPAS must be protected from unauthorized disclosure and used only for authorized purposes. Contractor personnel may only use their JPAS accounts to manage the access records of their company's employees and consultants, and to verify the access levels and employment affiliations of incoming visitors who require access to classified information. Contractor personnel are not authorized to, and may not, release printed or electronic copies of JPAS records to any person or entity. The appropriate U.S. Government release authority (commonly in an agency Privacy Act Office) is responsible for making release decisions regarding all JPAS records in accordance with the Privacy Act of 1974.