



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 inquires concerning specific information should be addressed to the cognizant security office, for referral to the Directorate for Security Programs, Headquarters, DSS, as appropriate.

ISL 01L-2

March 2, 2001

- 1. Department of Defense Security Clearance/Access Investigative Priorities**
- 2. DISCO Relocation**
- 3. EPSQ Help Desk**
- 4. Reciprocity of Intrusion Detection Systems**
- 5. Industrial Base Clearance Requirements Office (CRO)**
- 6. Defense Clearance and Investigations Index (DCII) Systems Access Center**
- 7. Adverse Information as it Relates to the Office of Secretary of Defense (OSD) Reinstatements and Conversion Waiver**
- 8. Suspicious Contact Reports – NISPOM Paragraph 1-302b**

1. Department of Defense Security Clearance/Access Investigative Priorities

Last Fall, the Fiscal Year 2001 Defense Authorization Bill, under 10 U.S.C. 1564, directed the Department of Defense (DoD) to establish a process for expediting the completion of background investigations for DoD personnel as well as DoD contractor employees engaged in sensitive duties that are critical to the national security. In response, the Deputy Assistant Secretary of Defense (Security and Information Operations) (DASD(S&IO)) convened two meetings with the various DoD Components to develop a more current and realistic listing of DoD mission critical priorities. The result of those meetings is the tiered list of investigative priorities which follows this article. Tier I receives the highest priority. This list supersedes the existing 78 priority case types and will serve as the official DoD investigative priority policy. Expected questions and corresponding answers regarding this prioritization policy are also provided for your information.

Effective April 1, 2001, all contractor facilities should use the following list when submitting priority investigations to DSS. As of that date, requests for investigation citing superseded categories will no longer receive priority. However, such investigations submitted *before* that date will receive the previously established priority.

The success of this effort will be largely dependent on the deployment of the new DSS Electronic Personnel Security Questionnaire (EPSQ) Version 2.2, that is now scheduled for deployment in April 2001. The DSS web site should be checked periodically for further information on the EPSQ 2.2 deployment schedule. EPSQ 2.2 will include a two-position data field that will accommodate the priority designations identified in tiered list of investigative priorities. Prior to the availability of EPSQ 2.2, requesters may request prioritization of the following case categories submitted to DSS by selecting one of the following case categories in the Reason for Request block of the security officer's portion of the current EPSQ:

- Presidential Support
- Nuclear Personnel Reliability Program (PRP)
- NATO
- Sensitive Compartmented Information

All future additions or deletions to the following list of DoD priority investigative categories will be determined by the DASD(S&IO) in coordination with the DoD Components. Please direct any questions you may have regarding this matter to your assigned Industrial Security Representative or by electronic mail to priority@mail.dss.mil.

Listing of Investigative Priorities

Tier I (highest priority):

11 Presidential Support (Yankee White) – includes all positions where a candidate for Presidential Support duties cannot be put in the position without a completed SSBI;

12 Sensitive Compartmented Information (SCI) –where access cannot be granted without a completed SSBI; and,

All cases involving personnel who have been granted *interim SCI* access.

All candidates (civilian, contractor, military) physically assigned to NSA or NSA field locations, including Service Cryptologic Element candidates.

13 Special Access Programs (SAP) – only those programs where SAP access cannot be granted without a completed SSBI;

15 Nuclear Personnel Reliability Program (PRP) (SSBI only)

16 Key Management Personnel (KMP)- of business entities in process for an initial facility security clearance

Tier II:

21 Sensitive Compartmented Information Access – personnel requiring SCI access not covered under Tier I;

22 Special Access Programs (SAP) – where a completed SSBI is NOT required as a condition for initial access;

23 State Department investigations for contractor personnel employed in the construction of U.S. embassies (includes both NACLCS and SSBIs);

24 Nuclear Personnel Reliability Program (PRP) (NACLCS only);

25 Contract Linguists – personnel who possess a critical language skill in support of a DoD contingency mission (during a military exigency investigations may be submitted under Tier I);

26 Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI);

27 North Atlantic Treaty Organization (NATO) - personnel assigned to NATO/SHAPE billet (SSBI only)

Tier III:

31 North Atlantic Treaty Organization (NATO) – personnel assigned to a NATO/SHAPE billet (NACLCS only);

32 Communications Security (COMSEC) – personnel with routine access to cryptographic materials in the normal course of their duties (includes NACLCS and SSBIs);

33 Restricted Data – includes TOP SECRET, SECRET and CONFIDENTIAL RD access. Does not include access to Formerly Restricted Data (FRD);

Tier IV: (applies to both NACLCS and SSBIs non included in the above tiers)

41 Routine

42 Accelerated

Questions and Answers

Q: Why was this change put into place?

A: Requestors had established seventy-eight different priorities for the personnel security investigations (PSI) conducted by Defense Security Service (DSS). That number obviously diluted the concept and impact of priorities; in addition, the priorities did not necessarily represent the better interests, comparatively, of all of the Department of Defense. Within DSS, the mere identification of priority cases was draining the resources needed to get the cases completed. Something had to be done to rationalize the process.

Q: How was the change decided?

A: Two meetings were convened by the DASD(S&IO) with the various DoD Components to develop a more current and realistic listing of DoD mission critical priorities.

Q: What do I do if the case category of my submission is included in the list of investigative priorities but is not reflected in module 4 of the DD 1879 or module 6 of the NAC Security Information Sheet?

A: Until implementation of EPSQ version 2.2, you may only request prioritization of the following case categories that can currently be selected from pull down lists of the appropriate security forms within the EPSQ:

Presidential Support (DD 1879)

Nuclear Personnel Reliability Program (PRP) (NAC Security Information Sheet)

NATO (DD 1879 or NAC Security Information Sheet)

Sensitive Compartmented Information (SCI) (DD 1879)

Q: What are the timelines associated with the various categories of priority investigations?

A: There was no ceiling placed on the numbers of requests allowed to be submitted under each category of priority investigation. It is not possible at present to accurately predict how long an investigation falling under any given category will actually take to complete.

Q: Will this new prioritization policy increase the time to complete routine requests for investigation?

A: We are optimistic that this new scheme will improve the process. As stated above, we've had a prioritization scheme that became overly cumbersome. We will continue to monitor this initiative to assess the impact and determine options for corrective action.

Q: What is the purpose of the fourth tier?

A: Tier IV reflects all other cases and was added to permit requesters the ability to assign some level of priority within this category, albeit not at the level of Tiers I-III.

Q: Why not cite one of the categories to gain expeditious handling for a case that does not fall into one of the approved categories?

A: Requesters must be judicious in assigning priorities to cases, ensuring they do so only for those individuals who truly require such access in the course of their assigned duties and meet the definitions for each priority. If the prioritization scheme is misused, it will defeat the purpose and eliminate the benefit of this initiative. Similarly, even though a Personnel Security Investigation (PSI) may fall into one of the categories, the needs of the job may not require priority handling. You should exercise discretion in declaring a request to be a priority. The normal course of investigations will usually develop information that validates the basis for the priority requirements.

Q: What will happen if I don't include a priority code in an investigative request?

A: It will be handled as a routine request. The assignment of a priority category is the responsibility of the requester. With the use of automated processing, manual intervention by DSS to screen for uncoded priority requests is not practical.

Q: My company has contracts with the Department of State and some of the other non-DoD agencies listed in NISPOM paragraph 1-103b as using DoD's industrial security services. Are the investigations of our employees working on such contracts eligible for priority handling?

A: Yes, provided they fall into one of the tiered list of investigative priorities as shown above.

Q: Will proper implementation of this priority procedure be evaluated as part of DSS' oversight of cleared contractors?

A: No. This priority procedure is not addressed in the NISPOM. However, DSS will review contractor adherence to NISPOM paragraph 2-200d, which requires contractors to limit requests for personnel security clearances to the minimum necessary for contract performance.

Q: When EPSQ version 2.2 is released where will I enter the two-place priority designator?

A: EPSQ version 2.2 will collect this designator under the Certify - Certify User Form menu item. The Certification screen will contain an edit area entitled "Special Project Code (Not required unless applicable)".

2. DISCO Relocation

The Defense Industrial Security Clearance Office (DISCO) is moving to a new location effective March 12, 2001. The new mailing address and key telephone numbers are listed below. Please note that the customer service number has not changed. It is not anticipated that the move will result in any major disruption to service.

New Location:

2780 Airport Drive, Suite 400
Columbus, OH 43219-2268

Telephone Numbers:

Director's Office	(614) 827-1528
<u>Facility Clearance Division</u>	(614) 827-1535
Team Leader (Central Region)	(614) 827-1591
Team Leader (Southeast Region)	(614) 827-1595
Team Leader (Capital Region)	(614) 827-1578
Team Leader (Northeast Region)	(614) 827-1584
Team Leader (West Region)	(614) 827-1587
Plans & Projects Division	(614) 827-1521
Personnel Clearance Division	(614) 827-1634
<u>Customer Service</u>	(888) 282-7682

3. EPSQ Help Desk

The DSS Customer Service EPSQ experts are available from 7:00am to 5:00pm Eastern Time to assist you with any technical questions or problems you may be having with the EPSQ. They can be reached by phone at 1-800-542-0237 or via email at epsq_questions@mail.dss.mil. DSS also has many EPSQ related Frequently Asked Questions (FAQs) posted on our website at www.dss.mil/epsq/.

4. Reciprocity of Intrusion Detection Systems

Paragraph 5-901 of the National Industrial Security Program Operating Manual (NISPOM) requires that approval of new Intrusion Detection Systems (IDS) be based on the criteria of Director of Central Intelligence Directive (DCID) 1/21 or Underwriters Laboratories Standard 2050 as determined by the Cognizant Security Agency. DSS utilizes the criteria of UL 2050 when approving new IDS. However, when reciprocity is an issue (e.g., the cleared facility has a customer that has previously approved an IDS based upon the DCID 1/21) DSS can approve use of the IDS under the following conditions:

a) The contractor must submit a written request to their Industrial Security Representative that includes a written assurance from at least one active customer stating the IDS meets DCID 1/21 standards. The written assurance must describe any and all waivers to the DCID that may have been granted and include a point of contact from the customer to ensure any future issues regarding the IDS can be addressed. (NOTE – When the identity of the customer must be protected, the assurance from the customer will be coordinated with the DSS Special Programs Branch, Industrial Security Program Office).

b) DSS' consideration and acceptance of the assurance provided by the customer will be based on a review of any waivers that have been granted.

c) Any such approvals will be site specific.

d) The contractor must notify DSS of any changes to the IDS that affect the security of the system.

e) DSS will continually evaluate the areas and/or containers under DSS cognizance to ensure they are receiving proper alarm monitoring and response.

5. Industrial Base Clearance Requirements Office (CRO)

Effective January 1, 2001, Defense Security Service established an Industrial Base Clearance Requirements Office (CRO) to quantify current and anticipated requirements for investigations needed to support the classified and sensitive activities of the defense industrial base. This quantification will allow for suitable planning, programming and budgeting to meet that need. As the first step in this effort to quantify investigative requirements for industry, DSS requested the largest 242 cleared contractor facilities provide projections of investigations that will be required over the next five years to support existing and anticipated contracts. Once these projections are received, the CRO will work closely with industry representatives, DSS industrial security and investigative personnel, and government contracting elements to refine identified requirements to ensure they reflect actual need. As a follow up to that initial survey, the CRO plans to request similar data from all other cleared facilities during the summer of 2001. In addition, the CRO will monitor the overall adequacy of the clearance requests submitted by industry and look for patterns of rejects and marginal submissions (i.e., requests that are not immediately actionable). Further, the CRO will serve as an advocate to ensure that projected clearance requirements are properly identified as part of DoD's overall prioritization of investigations and that these investigations are receiving the established priority. Finally, the CRO will serve to assist those within DoD who are responsible for establishing investigative priorities to understand the requirements of industry. For more information about the CRO, please visit the DSS web site at www.dss.mil and click on "About DSS".

6. Defense Clearance and Investigations Index (DCII) Systems Access Center

The Defense Security Service (DSS) modernization initiative facilitates standardized data sharing with customers and end users. DSS utilizes a number of web-based systems that allow real-time communication and are designed to protect "For Official Use Only" (FOUO) information. The systems are the (i) Letter of Consent (LOC) and Receipt System, (ii) Central Verification Activity (CVA), and the Defense Clearance and Investigations Index (DCII). The products of these systems are restricted to authorized users.

The LOC and Receipt Systems are authorized for access by cleared contractor facilities in the National Industrial Security Program (NISP). Information contained in the CVA is provided to cleared contractor facilities, Department of Defense elements, U.S. Federal Government agencies under the NISP, and to military contracting and security authorities. The DCII System is an automated central index that identifies investigations conducted by DoD investigative agencies and personnel security determinations made by DoD adjudicative authorities. DSS operates and maintains the DCII on behalf of the DoD components and DASD (Security and Information Operations). DSS limits DCII access to the Department of Defense and other federal agencies that have adjudicative, investigative and/or counterintelligence missions.

General information relating to each of the above systems and how to establish the user accounts may be found at our website, (www.dss.mil). The Systems Access Center creates the DSS assigned USERID (for each individual) and maintains the user accounts for the above DSS information systems, which includes trouble-shooting problems that users may have accessing their user accounts. The previously identified telephone numbers for the Systems Access Center have been changed. Therefore, should you be experiencing problems associated with accessing either of the above systems, please call:

System Access Customer Service Center 1-800-542-0237

System Access Immediate Assistance(Only)..... (410)865-2595

7. Adverse Information as it Relates to the Office of Secretary of Defense (OSD) Reinstatements and Conversion Waiver

We have received numerous questions regarding the responsibilities of a company gaining a new, cleared employee under the OSD Reinstatement and Conversion waiver, dated January 7, 2000, if that contractor is aware that the losing contractor reported adverse information to the Defense Industrial Security Clearance Office (DISCO) specific to that individual. Most questions relate to whether the contractor is permitted to grant the individual access to classified information.

The OSD waiver states that contractors must submit a DISCO Form 562 at the time they grant access to classified information. When the Form 562 is received, DISCO will check their database(s) for any record of adverse information associated with the individual identified on the Form 562. If there is existing adverse information, the action taken by DISCO is dependent on the nature of the information. DISCO will either (a) reinstate the clearance with no further action, (b) reinstate the clearance and open an investigation or (c) not reinstate the clearance and recommend the interim suspension of the personnel security clearance. These actions are based on specific criteria and often are only taken based on an accumulation of information, and/or corroboration of the information. Only the U.S. Government has the authority to take any of the above actions with regard to an individual's personnel security clearance. Contractors should not deny access to an already cleared individual based solely on knowledge that the individual's former employer had submitted adverse information to DISCO. The gaining facility only has the responsibility to submit the DISCO Form 562 to DISCO and to verify existence of the personnel security clearance per the instructions outlined in the OSD waiver letter.

A subsequent question arises as to whether the losing contractor is obligated to inform the gaining contractor they have submitted adverse information to DISCO regarding the individual? The general answer is no. The losing facility has the sole obligation to report the adverse information to the U.S. Government. Should the reported adverse information result in further action related to the individual's personnel security clearance, the gaining facility will be appropriately notified. Should a contractor have knowledge of adverse information relating to a former employee whereby they reasonably believe the individual could be a danger to the public,

the contractor should discuss the appropriateness of release of such information and any potential liability with their legal counsel.

8. Suspicious Contact Reports – NISPOM Paragraph 1-302b

As recent events have indicated, suspicious contact reporting by cleared personnel to include cleared industry are important to the protection of sensitive information and technologies against threats from foreign adversaries. Suspicious contact reports submitted to DSS in accordance with NISPOM paragraph 1-302b are shared as appropriate with counterintelligence (CI) agencies (e.g., normally the CI element of the Government Contracting Activity (GCA) that owns the technology involved), who use the information in accordance with their missions. As an example, CI analysts from the Army, Navy & Air Force may incorporate this information into finished threat products (usually technology or country threat assessments) and/or Intelligence Information Reports (IIR) that can be distributed electronically to authorized personnel worldwide.

DSS compiles and analyzes information contained in industry suspicious contact reports to produce products that help improve the threat awareness of DSS and cleared industry personnel. The DSS CI Office produces two publications based on this information, for use primarily by DSS personnel and cleared industry. These are:

- “Technology Collection Trends in the US Defense Industry,” which is produced annually, and
- “Suspicious Indicators & Security Countermeasures for Foreign Collection Activities Directed Against the US Defense Industry,” which is produced as new information warrants.

“Technology Trends” is based upon end of the year analysis by the DSS CI Office of suspicious contact reports submitted to DSS that are assessed as likely unauthorized attempts to obtain US and defense technology. “Technology Trends” identifies the method of operation/“modus operandi” (MO), identified in suspicious contact reports that were used in an attempt to collect restricted U.S. technologies. Perhaps even more helpful from a threat awareness perspective, each of the top eight technologies sought in collection efforts appear in “Technology Trends” as individual pie charts, divided by the MO employed in an attempt to obtain the information. It is important to note that this tying of technology to MO, as well as the trend identification and projections made possible from this effort, is solely a result of industry reporting. DSS is also pleased to report that much of the analysis contained in both the unclassified and CONFIDENTIAL/NOFORN version of this publication is incorporated into the President's Annual Report to Congress on Foreign Economic Collection & Industrial Espionage (U).

The second publication, “Suspicious Indicators” is intended to assist users in evaluating the “suspiciousness” of requests for information or some other overture to your company and its personnel. After reading this publication, users may find that closer scrutiny of past incidents or on-going relationships (regardless of national origin) may justify a suspicious contact report.

Unclassified versions of the "Trends" and "Suspicious Indicators" are available via the worldwide web at http://www.dss.mil/cithreats/2001_trend.pdf and http://www.dss.mil/cithreats/scm_post_internet.pdf respectively. Both the classified and unclassified version of "Technology Trends" are also available from your Industrial Security Representative.