



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 DIS. 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 Industrial Security, HQ DIS, as appropriate.

ISL 96L-1

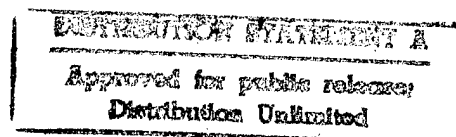
March 13, 1996

Industrial Security Letter *International Issues*

This is a special issue of the Industrial Security Letter (ISL) dedicated to answering questions that have been asked regarding requirements described in Chapter Ten of the NISPOM. (NISPOM Paragraph references are in parentheses after the item number.)

Note: The term classified information as used in this article refers to classified information in any form. Classified information may be part of technical data and defense articles, terms used in the State Department's International Traffic in Arms Regulation (ITAR).

Contractors must ensure that both the ITAR and the NISPOM are satisfied when conducting international business involving classified information. This information also is applicable to licensees, grantees, and certificate holders to the extent legally and practically possible within the constraints of applicable law and the Code of Federal Regulations. Any licensees, grantees, or certificate holders of the NRC who are affected by this letter and have questions should contact the NRC at the address in Appendix A of the NISPOM. Coordination between industry export and security officials is essential.



19960429 040

DTIC QUALITY INSPECTED 1

GENERAL

1. (10-104) **The NISPOM refers to a variety of security agreements negotiated between various governments. How do the terms of these agreements apply to contractors?**

General Security of Military Information Agreements (GSOMIA) are negotiated by the United States with a foreign government and obligate each government to provide substantially the same degree of protection to each other's classified information. On occasion, annexes to the GSOMIA, called Industrial Security Agreements, are negotiated with the foreign government for handling classified information entrusted to industry. Program agreements (e.g., co-production) either reference the GSOMIA and Industrial Security Agreement or include security language that is substantially the same as that in those agreements. Further requirements are contained in NATO security regulations. The requirements in Chapter 10 also are drawn from the security agreements and NATO regulations. Therefore, Chapter Ten obligates contractors to comply with the security requirements of the agreement, albeit indirectly.

2. (5-507, 5-508, 10-100, 10-508, 10-509) **If the NISPOM is dedicated to the safeguarding of classified information, why does Chapter Ten include references to export controlled, sensitive, or unclassified information?**

Certain basic principles of international security apply to both classified and unclassified information. These principles are included in Chapter Ten for information only and are not intended to apply security countermeasures to unclassified information except as otherwise required pursuant to the ITAR, contracts, or international agreements. For example:

- contractors must be aware that foreign government unclassified information, in many cases, is protected by laws in the country of origin.
- uncontrolled access to unclassified information can reveal details of classified information through compilation.
- the handling of unclassified information related to classified programs is necessary to understand 10-200g of the NISPOM.
- export control issues are discussed in Chapter 10 because government-approved programs, in some cases, constitute the basis for exemptions to the ITAR while industrial security policies still apply.

- unclassified export controlled information may be included in a Technology Control Plan if required by a State Department export authorization or by contract.

DISCLOSURE

3. (10-102, 10-307, 10-509) **Why is the NISPOM definition of an individual who is a U.S. person different from the State Department's International Traffic in Arms Regulation (ITAR) definition?**

Only a U.S. citizen is eligible for a personnel security clearance. Therefore, the NISPOM definition of U.S. person is an individual who is a U.S. citizen. The ITAR uses a broader definition of U.S. person based on a person's right to be hired if he or she is qualified for a job (employment). In other words, a U.S. contractor can employ a foreign national who has a certain immigration status as a permanent resident and give the person access to unclassified technical data without an export license. But, such employment does not establish the eligibility basis for a security clearance.

Procedures must be in place to ensure that non-U.S. citizens do not have access to U.S. classified and foreign government information. If the procedures to preclude such access are not deemed adequate by the IS Rep, a detailed Technology Control Plan will be required that includes special briefings, non-disclosure statements and more stringent access control measures.

4. (2-210) **Is an export authorization required to release classified information to a non-U.S. citizen or intending citizen who has been issued a Limited Access Authorization (LAA)?**

Yes. The LAA is a determination that the non-U.S. citizen or intending citizen is eligible to receive specified classified information. It cannot serve as an export authorization. Therefore, prior to submitting an application for an LAA to DISCO, the contractor must obtain a written disclosure determination from a principal or a designated disclosure official or obtain a State Department approved export license. This documentation must be submitted with the application for an LAA.

5. **What is the meaning of the word "proposal" in paragraph 10-202, Direct Commercial Arrangements?**

The term proposal in paragraph 10-202 means either an informal offering of a defense article or defense service during a marketing activity or the formal submission of a bid to a foreign entity for the purpose of providing a defense article or defense

service. The contractor may provide information that is in the public domain or that has specifically been authorized for public release; however, paragraph 10-200 of the NISPOM requires that contractors avoid creating false impressions of the U.S. Government's readiness to authorize release of classified information.

6. **Paragraph 10-204 requires contractors to submit two copies of the signed contract with the security clauses and the classification guidance to the local DIS Field Office as CSA. Does this mean a contractor has to send two copies of the entire contract?**

No, it is not necessary. A contractor should provide two copies of the security provisions (to include classification guidance, security clauses, and public release provisions) and the signature page identifying the authorized parties to the contract and Department of State approval (e.g., Contract, Technical Assistance Agreement or Manufacturing License Agreement) to the local DIS Field Office.

7. **Paragraphs 10-204b, 10-304, 10-719b refer to a requirement to maintain a written record that identifies the originator or sources of classified information released to foreign customers. Is it mandatory to keep a separate copy of the record with each export authorization?**

No. However, the contractor must have some system in place to readily identify the sources of classified information in a product per paragraphs 4-208a and 4-209 in the NISPOM, whether exported or not. If the source information is included with the export application, it greatly facilitates the government coordination, and thus expedites the decision on the application.

FOREIGN GOVERNMENT INFORMATION

8. **(1-101a, 10-102, 10-104, 10-306) The NISPOM has reduced accountability and recordkeeping requirements for U.S. classified information. Why are records still required for foreign government information (FGI)?**

The Presidential Executive Order 12958 of April 17, 1995 (which has replaced Executive Order 12356 dated April 2, 1982) and NATO policy and international agreements provide the basis for protecting foreign government information. The order specifies that: (1) foreign government information shall retain its original classification marking or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information and (2) an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the

government or international organization of governments that furnished the information.

Additionally, the United States has over 50 General Security Agreements with other governments that obligate each signatory to provide substantially the same degree of protection to each other's information. The NATO Security Agreement contains similar language. The Arms Export Control Act requires that international contracts and agreements include provisions on equivalent protection.

Other governments and NATO have not lessened the accountability requirements for their SECRET information. Therefore, we are required to provide a greater degree of control over foreign government information. Moreover, since it is the governments that are ultimately responsible for safeguarding each other's classified information under international agreements, there must be records reflecting the transfer of responsibility and accountability.

9. (10-306) What records are required for foreign government CONFIDENTIAL and RESTRICTED information (FGI)?

CONFIDENTIAL FGI recordkeeping is limited to receipt and dispatch records which are not required for foreign government RESTRICTED information. Classified material receipts are required for all international transmissions.

10. (10-305) Are there special briefings and acknowledgment requirements for contractor employee access to foreign government information?

Paragraph 10-305 of the NISPOM requires that contractor employees will be briefed and acknowledge in writing their responsibilities for handling foreign government information prior to access being granted. Contractors may include these requirements in initial and periodic briefings for U.S. and foreign or international organization classified information. An employee's signing of the Classified Information Nondisclosure Agreement (SF-312) will satisfy the acknowledgment requirement, provided it is made clear that the certification also covers foreign government classified information.

11. What is the difference between the intent of paragraph 10-307 titled Disclosure and Use Limitations and paragraph 10-312 titled Subcontracting?

Foreign government information shall not be disclosed to representatives or nationals of a third country, including permanent residents of the United States who are from a third country, or be used for other than the purpose for which it was provided, without

the prior written consent of the originating foreign government. Disclosure to U.S. subcontractors, in accordance with paragraph 10-312 of this manual, is authorized unless specifically prohibited by the originating governments.

12. (10-307, 10-312) What are the appropriate U.S. Government channels for obtaining third country or third party disclosure approval for classified foreign government information?

Depending on the type of international program, either the Government Contracting Activity (GCA) or the Office of Defense Trade Controls is the appropriate point of contact for obtaining authority for the re-export of classified foreign government information:

- (1) If the contractor received the foreign government information under a U.S. Government contract, the GCA has responsibility for obtaining the foreign government's written consent for release of the information to a third country.
- (2) If the contractor received the information through a direct commercial contract, the contractor will obtain written consent from the originating foreign government and attach the consent to the re-export request sent to the Office of Defense Trade, Department of State.

The contractor will provide a copy of the re-export approval obtained through the previously described channels to the local DIS Field Office upon receipt.

13. (10-304) On occasion, a foreign government contract will require that US unclassified information be classified by the terms of the contract. Is a visit request required to access what a foreign government considered classified but the United States Government considers unclassified?

Yes. Security clearances and access authorization must be verified by the visitor's government. Some foreign governments classify the existence of a contract, the contents of a contract, and the deliverables for their internal national security reasons. In some cases, U.S. unclassified information available in the public domain may be classified to satisfy the foreign government national security requirement. If a contractor encounters this situation, the local DIS Field Office should be contacted immediately. The Field Office will request that DIS Headquarters attempt to clarify the classification guidance. Until the issue is resolved, the contractor must comply with the contract security requirements.

14. (10-309) ISL 95L-2 described the provisions of Executive Order 12958 that allow a change to be made to the handling procedures for foreign government information (FGI) marked RESTRICTED. As noted, the U.K. has agreed that

U.K. RESTRICTED information need not be transmitted through government-to-government channels. Does this mean that transmission can be contractor-to-contractor without direct government involvement?

Yes. However, U.K. RESTRICTED information is still a classification designation. The United States Government is responsible for information so marked while it is under U.S. jurisdiction. Prior to transmission from the U.S., a U.S. contractor will request verification from DISCO (ATTN: Linda Harris, Dean Stavrides, Diane Greer, telephone 614-692-2136, facsimile 614-692-1055) that the receiving U.K. company has an appropriate clearance and safeguarding capability. (Note: The use of DISCO to process all U.S. contractor requests for verifications of foreign contractor facility security clearances is a change from ISL 95L-2.) Once the verification is received, the material may be transmitted directly by one of the following methods:

- Military Mail Channels (First Class Mail)
- Overnight Commercial Delivery Services
- Handcarry (courier certificate issued by the FSO)
- Secure Transmission (fax, computer -to-computer): (Government-approved encryption device is required)

Reminder: U.K. RESTRICTED information is still classified foreign government information. It is still export controlled by definition and requires a DSP-85 in accordance with the ITAR unless the information is in its original form and is being returned to its original source of import. The provisions of 10-408 apply with the following exception: notification does not have to be made to the appropriate DGR but a copy of the certification by an empowered official or his/her designee must be provided prior to the transmission.

15. (10-317) Is a personnel security clearance required to process RESTRICTED information on a computer system?

Yes, except in the instance where only U.K. RESTRICTED information is processed on an approved standalone computer system. Otherwise, Chapter 8 requirements apply.

INTERNATIONAL TRANSFERS

16. (10-401, 10-201) What is meant by the terms government-to-government transfer and government-to-government channel and what is the significance?

Pursuant to international security agreements, governments are ultimately responsible for the safeguarding of classified information provided by another government. The

decision to release (transfer) classified information is based in part on an assurance by the recipient government that the information will be protected, as specified by the Arms Export Control Act and the National Disclosure Policy. Therefore, government control must be maintained even though a contractor may have custody, hence "government-to-government transfer." The government channels for transmitting classified information are diplomatic pouch, military courier, military postal registered mail, military transportation and secure electronic transmission. On occasion, the sending and receiving governments may agree on alternative channels such as hand carriage by cleared contractor personnel in accordance with specific transfer instructions. Taken together, the government channels and alternative mutually agreed channels comprise "government-to-government channels."

17. (10-200, 10-201a) **Since CONFIDENTIAL and SECRET information can only be released through "government-to-government" channels, why does a contractor have to get a separate export authorization in order to initiate a transfer of classified material to a foreign interest?**

The export of classified information to a foreign entity involves two processes: (1) U.S. Government export authorization (i.e., the authority to disclose or transfer the data or article); and (2) the physical transfer through government-to-government channels. The export authorization process is the responsibility of the Office of Defense Trade Controls, Department of State. The process ensures that the release of classified information is consistent with U.S. national security interests and it results in the export or release decision. Authorization to export classified information can be granted only by designated U.S. Government officials. (See NISPOM Paragraph 10-101.) The government-to-government transfer process is a separate process which ensures that the classified information to be transferred complies with the terms of the export authorization and that it is transferred to the responsible recipient government through secure channels.

18. (10-405) **What is the role of the cleared Freight Forwarder in the government-to-government transfer process?**

A cleared Freight Forwarder is a U.S. company under contract to a U.S. firm or the U.S. Government or a foreign government to facilitate transportation arrangements of classified material to and from foreign governments. The Freight Forwarder usually functions as an intermediate facilitator for classified shipments and is used only with the concurrence of both the sending and receiving governments. The Freight Forwarder normally doesn't have an inherent commercial carrier capability. If not, it may subcontract for a commercial carrier, if contractually required.

(1) Under a Foreign Military Sales (FMS) case, the name and address of the cleared Freight Forwarder and any commercial carrier (which must be cleared in the absence of a cleared company or government courier or escort) must be included in the Letter of Offer and Acceptance and identified in the Transportation Plan or Transmission Instructions. The level of clearance and safeguarding capability may be verified by calling DISCO. In an FMS case, the foreign government and the responsible User Agency jointly develop the Transportation Plan or Transmission Instructions from the point of origin to the point of ultimate destination.

(2) Under a Commercial Sale, the name and address of the cleared Freight Forwarder and carrier (which must be cleared in the absence of a cleared company or government courier or escort) must be included in the U.S. Government export authorization and identified in the Transportation Plan. The level of clearance and safeguarding capability may be verified by calling DISCO. The Defense Investigative Service and the foreign government jointly approve the Transportation Plan from point of origin to the point of ultimate destination.

For both the FMS and Commercial Sale the point of ultimate destination identified in the Transportation Plan must be in the recipient country, not a U.S. Freight Forwarder location. If military transportation is used, it also must be identified in the Transportation Plan or Transmission Instructions.

19. (10-402, 10-405 and 10-406) Are escorts required for overseas shipments of classified material?

Yes (5-412, 5-413, and 10-402c). Moreover, if a courier or escort is used, the types of international transportation carriers described in 10-402d, titled International Carriers, must be used.

A cleared commercial carrier which provides its own cleared courier or escort may be used. Such carriers also must be identified in the Transportation Plan or Transmission Instructions as described in paragraph 18 above.

If a foreign government chooses to designate one of its cleared government or contract employees to serve as the courier or escort or to use one of its cleared commercial carriers, such escorts, couriers and commercial carriers must be identified in the Transportation Plan and approved by both the sending and receiving governments.

20. Paragraphs 10-406 and 10-713 both address hand carrying of classified information across international borders. What is the role of the DIS Field Office (as CSA) and the GCA in approving use of the hand carriage procedure?

In paragraph 10-406, if the transfer is the result of a direct commercial arrangement, the contractor will receive the approval from the local DIS Field Office which will

request that DIS Headquarters obtain the concurrence of the recipient foreign government, since both governments must agree on the procedure. If the transfer is pursuant to a Government Agency contract or a bilateral or a multinational program international agreement between governments, the request must be approved in writing by the GCA which must coordinate with the other government or governments. In paragraph 10-713, GCA authorization is again required before the CSA may issue a courier authorization. In this case, however, the GCA may be a NATO organization or management office.

Note: Paragraph 10-406j references 10-403d. This is a typographical error. The reference should be 10-402d.

21. **Paragraph 10-408 states that an empowered official must provide certification or documentation to the U.S. Designated Government Representative (DGR) or government transmittal authority. Can this function be performed by an employee designated in writing by the empowered official?**

Yes. The function can be performed by an empowered official, an employee designated in writing by or his/her designee.

22. **Paragraph 10-409 addresses transfer of classified technical data pursuant to an ITAR exemption. Can a contractor provide the written export authorization to the Designated Government Representatives on the day of export?**

A classified export cannot take place without the appropriate security arrangements in place - regardless of whether the export is pursuant to a license or an exemption to the licensing process. These arrangements take time and require coordination with the receiving foreign government. Contractors must provide their local DIS Field Office with the necessary information, including the written export authorization to make the security arrangements. Such documentation should be provided at the earliest possible time and should cover exports for an entire program, not individual shipments.

INTERNATIONAL VISITS

23. (Section 5) **Why do requests for visit authorization that will involve access to classified information have to be processed through government channels?**

Because it is the responsibility of the governments to provide verification of facility and personnel clearances and provide the security assurances (protection, end-use, retransfer) required by the ITAR, the Arms Export Control Act, and the National

Disclosure Policy and render a disclosure decision, if it is required. A government disclosure decision made in the processing of a visit request may then constitute an exemption to the licensing requirements of the ITAR.

- 24. Paragraph 10-501 discussed foreign national “visitors” and “assignments” of foreign nationals to cleared facilities. What is the difference between the terms “visit” and “assignment”?**

A “visit” connotes a short stay (e.g., a few days); “assignment” connotes a more permanent visitor presence (e.g., the visitor is “stationed” at the site for contract monitoring purposes).

- 25. (10-506b) If a cleared contractor employee is traveling on DoD travel orders to visit a foreign government or foreign contractor facility, is a separate Visit Request required to be processed by the employee’s facility?**

No. The contractor should send a request visit authorization letter (VAL , 6-103) to the DoD activity preparing the travel orders, if a current VAL has not been provided. A separate request for visit request does not have to be processed through DISCO.

- 26. Paragraph 10-507 describes circumstances when a foreign government must submit a request for visit (RFV) authorization (contained on pages 10-5-4 and 10-5-5) . Paragraph 10-508c seems to contradict 10-507 by implying that a foreign national can be authorized access to classified information without a request for visit if a contractor has a U.S. Government export authorization on hand. Is this correct?**

No. A request for visit is always required for access to classified information whether or not a separate U.S. Government export authorization is needed. While the license approves the export, the visit request is the vehicle by which the foreign government provides the security assurance (e.g., clearance, access authorization) to the U.S. Government. The security assurance must be accepted by the U.S. Government before classified information actually may be released.

- 27. When is a visit request required for the release of unclassified information and what are the appropriate channels to process such a request?**

There are several channels available for a contractor to obtain authorization to release unclassified information during a foreign national plant visit. The contractor must first determine whether:

- a. the unclassified information has been approved for public release by the U.S. Government;
- b. the unclassified information is export controlled, e.g., whether it is technical data as defined in the ITAR;
- c. the release of the unclassified export controlled information may create the impression that the U.S. Government is willing to release classified information on the same subject; or
- d. the proposed visit is in support of a government-to-government or a direct commercial program.

Once these determinations are made, the following approval channels normally apply:

- If the unclassified information has been approved for release into the public domain, additional government approval (e.g., export license or visit request) is not required.
- If the unclassified information is not export controlled (that is, not technical data) but is not yet approved for release into the public domain, then a contractor must follow the public disclosure channels identified in contract language or the DD Form 254. A visit request is not required.
- If the visit involves unclassified information which requires an export authorization and it is in support of a classified government program (e.g., an international classified program between the U.S. and a foreign government, such as Foreign Military Sales or a U.S. co-production or co-development program), the visit request process may be used to obtain export authorization in the absence of the State Department export license or letter authorization from a DoD principal or designated disclosure authority.
- If the visit involves unclassified information that requires an export authorization, and is in support of a direct commercial program (e.g., an international contract between a U.S. contractor and a foreign government or contractor), the normal channel for requesting export authorization for a plant visit is the State Department licensing process. Visits involving the release of unclassified export controlled information specifically covered under an approved State Department export license do not require a visit request .

In instances where there is a question on which channel to use to obtain export authorization, the licensing process, specified in the ITAR, provides the most expedient channels.

28. (10-507) **Is a visit request with a security assurance required for a contractor to release foreign government classified information to a foreign national visitor even if the information is from the country of citizenship? If so, does the visit request have to be processed through government-to-government channels?**

Yes, to both questions. The visit request provides the required government security assurance, clearance verification, and the need-to-know (i.e., access authorization) and must be processed through government-to-government channels.

29. (10-507d) **Is a contractor required to adopt access controls in the case of a foreign national who is visiting a cleared facility when no classified information is to be released?**

Yes, to the extent required to ensure that classified information is not inadvertently released to unauthorized persons. The controls may be in the form of a company's internal procedures or a Technology Control Plan. A Technology Control Plan normally is used when the foreign national visitor is assigned or will remain at the facility for longer than 30 days (an extended visit).

30. **What types and degrees of access controls and security education are considered adequate to ensure that classified information is not at risk when foreign nationals are employed or at the facility on an extended visit?**

Contractors should contact their local DIS rep to ensure that the options chosen are rational, threat-appropriate and cost-effective for their particular situation. At a minimum, procedures must be in place to ensure that:

- a. access is controlled to classified information;
- b. employees are educated on the access limitations, controls and the reporting requirements for possible or actual unauthorized access; and
- c. the foreign national is informed of his or her obligations and responsibilities, the limitations of access and understands the duties to be performed at the facility.

31. (10-509) **Is a contractor required to place similar access controls on a foreign national who is an employee at a cleared facility when no classified information is to be released?**

Yes, to the extent required to ensure that classified information is not at risk.

32. **NISPOM paragraph 10-508 states that a foreign visitor shall not be provided temporary storage of classified material unless approved by the CSA. A former policy stated that a foreign visitor shall not be provided such storage without**

approval of the FSO. Do storage arrangements previously approved by the FSO need to be reapproved by the local DIS Field Office?

No, as long as the FSO retains control and cognizance of all information stored in the container. If the FSO has not provided notification to the local DIS Field Office of such arrangements, he or she should do so. This notification shall include a description of the controls on the container and the names of the visitors authorized access.

- 33. Paragraph 10-508c states that contractors shall notify the applicable CSA in advance of all extended visits and assignments of foreign nationals. Does this requirement apply to visits related to unclassified, non-defense, commercial programs?**

No. This requirement applies to all foreign nationals on extended visits and assignments who are performing on classified contracts.

- 34. (10-508) Is a separate Technology Control Plan required for each 10-508c notification?**

A facility may have an overall Facility Technology Control Plan or Standard Practice Procedures that can be referenced with each notification. The contractor should contact his/her local DIS Field Office to ensure that the specific controls and limitations are threat appropriate.

- 35. (10-510) Does a contractor have to report all export violations to the local DIS Field Office as CSA?**

The local DIS Field Office should be notified if the export violation involves classified information or any foreign government information as follows:

- (1) A violation that involves a cleared employee should be reported in accordance with paragraph 1-302a to DISCO and include the date the violation was reported to the appropriate export authority.
- (2) A violation involving a foreign national employee or visitor must be reported to the CSA and include the date the violation was reported to the appropriate export authority. The CSA will, in turn, notify the visitor's country of origin if foreign government information is involved.
- (3) Generally, violations by foreign visitors of security procedures for company proprietary information, not associated with NISPOM, need not be reported to the CSA.

36. Do foreign contractors who perform ISO 9000 quality control inspections at cleared facilities need to submit requests for visits?

Yes, ISO 9000 quality control inspections must be conducted within the parameters of the NISPOM and the ITAR. Contractors who hire foreign companies to perform the inspections must take great care to ensure that access is permitted only to information authorized for release by an appropriate export authority. It is recommended that security officials become involved in the company planning for ISO 9000 visits at the earliest possible time to avoid inadvertent disclosure of classified information.

Defense Contract Management Command (DCMC) Contract Administration Offices (CAOs) are now authorized to perform ISO 9000/ANSI/ASQC Q9000 qualification audits on selected contractors when a contract with ISO 9001-9003 requirements has been awarded or the contractor is moving to an ISO 9000 Quality and has current DoD business. The cognizant DCMC CAO will provide a statement on contractor capability and performance to buying customers and the contractor. For further information, please contact Richard Zell at telephone number: 703-767-2413, fax number: 703-767-3377 or E-mail: Richard_Zell@HQ.DLA.MIL

OVERSEAS ASSIGNMENTS

37. In paragraph 10-601c consultants are not permitted to be assigned overseas in positions that require access to classified information. Under what circumstances are consultants authorized to be assigned overseas?

None that involve access to classified information. (The term "assignment" is defined in paragraph 10-605.)

NATO INFORMATION

38. (10-713) A NATO document, classified SECRET and below, is being hand carried ultimately to a cleared foreign company. Does it have to be delivered to a U.S. organization at NATO in this circumstance?

No. NATO SECRET material may be handcarried between the NATO control points of the NATO Registry System at the sending and receiving organizations. The sending and receiving government security officials will approve the final arrangements to include issuance of the appropriate courier authorizations.

For NATO CONFIDENTIAL and RESTRICTED material, approval will be provided by the sending and receiving government security officials. Use of the registry system, to include transfers between control points, is not necessary, nor does it have to be delivered to a U.S. organization.

39. (10-708b) What is a NATO reference number and does it have to be applied to all pages, regardless of classification?

The explanation of the NATO reference number is discussed in the preceding paragraph (10-708a). The NATO reference number is applied to the first page of all NATO documents and must be applied to all pages of COSMIC TOP SECRET, ATOMAL and NATO SECRET documents.

40. (10-714, 10-715, 10-716) Is a chain of custody accountability system required for NATO CONFIDENTIAL and RESTRICTED material?

No, unless required by the originator. Receipt and dispatch logs are required. Reproduction and destruction certificates are not required unless specified by the originator. Receipts are required for international transfers.

41. Paragraph 10-707, Subcontracting for NATO Contracts, requires a request for written approval be forwarded through the CSA to the NATO contracting activity. Does this apply to a subcontract issued to another U.S. cleared company?

Yes, at this time. A proposal to change this requirement is under review at NATO HQ.

42. What is the requirement for protecting U.S. unclassified documents that contain extracts of NATO RESTRICTED information?

U.S. documents that contain extracts of NATO RESTRICTED information must be handled as NATO Restricted Documents. They should be marked "THIS DOCUMENT CONTAINS NATO RESTRICTED INFORMATION." The nature of the information and security obligations do not change by virtue of being placed in a U.S. document.

43. (10-718) **Does a document or media that contains extracts from other NATO documents need to be accounted for and controlled as a U.S. or NATO classified document?**

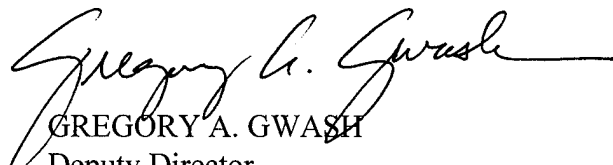
A U.S. document that contains NATO classified information must be marked with the U.S. classification and a notation that the document also contains NATO information.

Classified documents must be marked and protected based on the highest level of classified information contained therein. Therefore, U.S. documents containing NATO classified information may require higher levels of protection and accountability. They must be handled in accordance with Chapter 10, Section 7, as NATO information. However, it is not intended that all documents handled under previous policy be located and re-marked. The documents should, however, be re-marked pursuant to current policy as they are used.

PROCEDURES FOR MULTINATIONAL ARMAMENTS COOPERATION PROGRAMS

44. **What are the Multinational Industrial Security Working Group procedures?**

The Multinational Industrial Security Working Group, known as the MISWG, is an ad hoc organization established to develop common security practices and procedures that facilitate the exchange of information. MISWG procedures are generally applied to classified programs and contracts involving two or more foreign governments. Use of MISWG generated procedures often facilitate government-to-government approvals of security arrangements needed to support a multinational and/or bilateral government program and in some cases (e.g., hand carriage, Transportation Plan) can expedite transfers of classified information. Certain MISWG procedures have been adopted in Chapter 10; others are voluntary. However, the procedures may be contractually mandated.


GREGORY A. GWASH
Deputy Director
(Industrial Security)