CHAPTER 10

NORTH ATLANTIC TREATY ORGANIZATION (NATO) SECURITY PROCEDURES

A. INTRODUCTION

1. This Chapter provides basic security requirements necessary to comply with the procedures established by the United States Security Authority for the North Atlantic Treaty Organization Affairs (USSAN) for safeguarding North Atlantic Treaty Organization (NATO) information. DoD Directive 5100.55 *(reference ppp)* contains the Terms of Reference designating the Secretary of Defense as the USSAN for the United States (U.S.) Government. The requirements of this Chapter are consistent with USSAN Instruction 1-07*)*, and the National Industrial Security Program Operating Manual (NISPOM) *(reference z)*. The foregoing documents must be consulted for specific details.

2. **Classification Levels**. NATO security regulations prescribe four levels of security classification, COSMIC TOP SECRET (CTS), NATO SECRET (NS), NATO CONFIDENTIAL (NC), and NATO RESTRICTED (NR). The terms COSMIC and NATO indicate the material bearing the markings is the property of NATO and is to be protected in compliance with NATO procedures. Another marking, "ATOMAL," is applied to U.S. RESTRICTED DATA or FORMERLY RESTRICTED DATA and United Kingdom (UK) Atomic Information that have been released to NATO. ATOMAL information is marked COSMIC TOP SECRET ATOMAL (CTSA), NATO SECRET ATOMAL (NSA), or NATO CONFIDENTIAL ATOMAL (NCA). NATO has another category of information which is controlled, “NATO UNCLASSIFIED” information. It is to be used only for official purposes. Material bearing this marking is also supposed to contain administrative and dissemination markings.

3. **Access Requirements**

a. Department of Defense (DoD) employees and contractor employees may have access to NATO classified information only when access is required in support of a U.S. or NATO contract or program requiring such access (i.e., "need-to-know").

b. Additionally, access to NATO classified information requires a final DoD personnel clearance (except for RESTRICTED information) at the equivalent level and a NATO briefing as described in subsection D., below. A personnel security clearance is not required for access to NATO RESTRICTED information.

c. Citizens and nationals of non-NATO nations may have access to NATO classified information only with the consent of the originating NATO member nation or civil or military body. Access to NATO classified information involved in NATO contracts may be permitted for citizens of NATO member nations provided they have the requisite personnel security clearance, they have been briefed as described in subsection D., below, and the contracting NATO organization, staff, command or agency approves such access.

d. There are special procedures for access to NATO classified information by governments of other countries and by other organizations. Access in such cases requires, inter alia, that there be a security agreement with the other government or organization, or the negotiation of such agreement if one does not exist.

B. FACILITY AND PERSONNEL CLEARANCE CERTIFICATE REQUIREMENTS

1. A NATO Facility Security Clearance (FSC) Certificate is required for any contractor to negotiate or perform on a NATO classified contract or subcontract. The NATO FSC Certificate certifies the facility has a U.S. facility security clearance at the requisite level, its personnel who require access have been briefed on NATO procedures, and the requirements of the NISPOM are met. The Defense Industrial Security Clearance Office (DISCO), a Defense Security Service (DSS) subordinate office, will provide the NATO FSC Certificate to the requesting NATO command, agency or member nation, as applicable.

2. The NATO FSC Certificate is not required for DoD Component contracts involving access to NATO classified information. It may be required by a NATO nation that provides NATO classified documents to a U.S. contractor in support of a non-NATO contract. However, all personnel requiring access must be briefed in compliance with the requirements of section D., below, including the requirement for the briefing certificate, prior to having access to NATO classified information.

3. When a contractor becomes aware that a NATO FSC Certificate is required, through a request for proposal (RFP) or other procurement announcement, the contractor should contact the responsible DSS office for assistance in obtaining the necessary certificate. Upon determining the requirements of this Chapter are met, the DSS should request DISCO to forward the Certificate to the NATO contracting staff, command or agency. DISCO will notify the contractor when the NATO FSC Certificate has been issued.

4. The NATO Personnel Clearance Certificate. The DISCO also will provide NATO Personnel Security Clearance Certificates (PSCCs) for United States personnel who are seconded to a NATO civil or military body, for United States personnel who are direct hires at NATO, and for DoD and contractor visitors to a NATO body.

C. NATO CONTRACTS

1. NATO contracts involving NATO-unique systems, programs or operations are awarded by a NATO Production and Logistics Organization (NPLO), a designated NATO Management Agency, a NATO Research Staff or a NATO Command. In the case of NATO infrastructure projects (e.g., airfields, communications, etc.), the NATO contract is awarded by a contracting agency or prime contractor of the NATO member nation responsible for the infrastructure project.

2. Subcontracting under a NATO contract will be handled in the same manner as classified U.S. contracts, except that prior to awarding a subcontract, prior written approval must be obtained from the NATO contracting agency. The subcontractor must possess the requisite level of FSC, employees requiring access must be briefed on NATO procedures, and a NATO FSC Certificate must be issued prior to award of the subcontract. The contractor may sponsor a prospective subcontractor for a NATO FSC only after approval to subcontract has been obtained.

3. The contracting agency will provide classification guidance to the contractor. The guidance normally is in the form of a NATO security aspects letter and security requirements checklist for NATO contracts. A U.S. - type security classification guide may be used for some large NATO programs involving several nations. The DD Form 254 (Contract Security Classification Specifications) or similar written guidance will be used for non-NATO contracts involving access to NATO classified information. If the contractor does not receive adequate classification guidance, or is not able to obtain the guidance, the DSS should be contacted for assistance. For large programs, NATO procedures also require the preparation of a Program/Project Security Instruction (see Chapter 9).

4. When DoD Components award contracts to develop documents the DoD Component is to deliver to NATO, the DD Form 254 must contain a requirement for the contractor to provide a list identifying the elements of U.S., NATO and foreign government information included in the documents and the source of the information (See subsection I.5., below).

D. ACCESS AND NATO BRIEFINGS

1. Each U.S. Government agency and contractor facility must maintain a record of positions requiring access to NATO classified information and shall maintain a record of PSCs granted access to NATO classified information. The record must indicate the level, date, and duration of each clearance.

2. Prior to having access to NATO classified information, U.S. contractor and U.S. Government personnel must be given a NATO security briefing. The contractor Facility Security Officer (FSO) will initially be briefed by the DSS. Thereafter, the FSO shall ensure the required briefings are administered to employees who require access to NATO classified information. Government employees and military personnel will be briefed by their security manager or a designee. The

NATO briefing must cover security requirements and the consequences of negligent handling of NATO classified information. Annual refresher briefings will be conducted. When access to NATO classified information is no longer required, personnel will be debriefed, as applicable, and acknowledge their responsibility for safeguarding the NATO information. The briefing may be accomplished by requiring the person to read a documentary presentation and sign the certificate. A PSC is not required for access to NATO RESTRICTED information, however, a person having access shall be briefed on the requirements for protecting the information.

3. A record copy must be maintained of each annual briefing certificate until the next certificate is signed. The record of debriefings must be maintained for two years for NATO SECRET and NATO CONFIDENTIAL information, and three years for COSMIC TOP SECRET and all ATOMAL information.

4. Persons who travel to areas with special security risks must be briefed on security hazards that may be encountered and may be requested to report any occurrence that may have security implications.

5. NATO PSCs require revalidation very five years for access to NATO TOP SECRET information, and very 10 years for NATO SECRET and CONFIDENTIAL information. Personnel no longer assigned to positions requiring access to NATO classified information shall have their NATO PSCs terminated.

E. SPECIAL ACCESS BY NON-NATO NATIONALS

NATO has established special policy permitting access by citizens and nationals of non-NATO countries. The policy pertains to such persons who are seconded to the armed forces of a NATO member nation, employed by the government of a NATO member nation, or employed by contractors of a NATO member nation. The access is limited to citizens and nationals of specified countries, for information no higher than NATO SECRET, access is not permitted to ATOMAL or special category information (e.g., SAPs, crypto information), and access must be approved by the National Security Authority (NSA) of the country intending to permit access. Special controls must be adopted if access is approved. In light of the stringent approval and control requirements, proposals to permit such access shall be referred through channels to the Office of the Under Secretary of Defense for Policy, Attn: Deputy Under Secretary of Defense (Technology Security Policy and National Disclosure Policy)

F. MARKING AND HANDLING NATO DOCUMENTS

1. Classified documents generated by a U.S. contractor under a NATO contract or prepared by a DoD Component specifically for release to NATO are to be marked as described in subsection A.2., above, and this section. (Note: Documents prepared pursuant to DoD Component and

NATO member nation non-NATO contracts must be marked in compliance with subsection H., below.)

2. NATO documents now must be portion marked. All classified documents created by U.S. contractors and DoD Components will be portion-marked.

3. The following markings, as applicable, will be applied to NATO documents containing ATOMAL information:

a. "This document contains U.S. ATOMIC Information (RESTRICTED DATA or FORMERLY RESTRICTED DATA) made available pursuant to the NATO Agreement for Cooperation Regarding ATOMIC Information, dated 18 June 1964, and will be safeguarded accordingly"; or

b. "This document contains UK ATOMIC Information. This information is released to the North Atlantic Treaty Organization including its military and civilian agencies and member states on condition that it will not be released by the recipient organization to any other organization or government or national of another country or member of any other organization without prior permission from His/Her Majesty's (H.M.) Government in the United Kingdom."

4. NATO classified documents, and NATO information in other documents, may not be declassified or downgraded without the prior written consent of the originating NATO member nation or civil or military body. Recommendations concerning the declassification or downgrading of NATO classified information are to be forwarded to the Central U.S. Registry (CUSR) via the DSS by contractors and via command or organizational channels by U.S. Government personnel.

5. Contractors and DoD personnel will not release or disclose NATO classified information to a third country person, including a subcontractor, without the prior written approval of the controlling organization, command, agency or staff. Requests are to be submitted directly to the contracting agency for DoD Component contracts. They will be submitted through the DSS for NATO contracts and non-NATO contracts awarded by a NATO member nation.

G. STORING NATO DOCUMENTS

NATO classified documents, except for NATO RESTRICTED, are to be stored as prescribed in USSAN 1-07 and the NISPOM for U.S. documents of an equivalent classification level. However, NATO documents must not be co-mingled with U.S. or other documents. NATO RESTRICTED documents may be stored in locked filing cabinets, book cases, desks, other similar locked containers that will deter unauthorized access, or in a locked room to which access is controlled.

H. INTERNATIONAL TRANSMISSION OF CLASSIFIED NATO DOCUMENTS

1. NATO policy requires the establishment of a central registry for the control of the receipt and distribution of NATO documents within each NATO member nation. The central registry for the United States is the CUSR. The CUSR establishes sub-registries at U.S. government organizations for further distribution and control of NATO documents. Sub-registries may establish control points as needed within their activities for distribution and control of NATO documents. COSMIC TOP SECRET, NATO SECRET, all ATOMAL documents, and documents warranting special access controls must be transferred through the registry system. Other NATO classified information will be transferred in the same manner as U.S. classified information of the same classification level. Receipts are required for NATO material classified CONFIDENTIAL and above that is transferred internationally (although NATO policy does not specifically require a receipt for CONFIDENTIAL information). The originator may require a receipt for NATO RESTRICTED information.

a. **NATO Organization, Command, Agency or Staff Contracts**. Contractors normally will receive and send NATO classified information related to a NATO Production and Logistics Organization (NPLO), NATO Management Agency, Research Staff or command contract through the CUSR, a sub-registry, a control point or other office established at a DoD Component for this purpose. If instructions are not provided by the contracting agency, contractors should contact the DSS for guidance.

b. **Infrastructure and non-NATO Contracts**. Classified information involved in NATO infrastructure contracts or non-NATO contracts awarded by a NATO member nation will be transferred through channels described in Chapter 6.

2. COSMIC TOP SECRET, NATO SECRET, NATO CONFIDENTIAL and all ATOMAL documents must be double wrapped in the same manner as equivalent U.S. classified documents, except the inner wrapper is marked with the appropriate NATO markings. NATO RESTRICTED documents do not require double wrapping.

3. The hand carrying of NATO SECRET, NATO CONFIDENTIAL, and NATO RESTRICTED documents across international borders may be authorized provided an urgent situation exists, as described in Chapter 6. However, when carrying NATO SECRET and NATO CONFIDENTIAL information, the courier must be issued a NATO Courier Certificate (Appendix J). A courier certificate is not required for NATO RESTRICTED information, but the courier must be informed of and acknowledge the procedures for handling the information. COSMIC TOP SECRET and ATOMAL and other accountable documents may not be hand carried; they must be transmitted through the NATO registry system.

I. EXTRACTING FROM NATO DOCUMENTS

1. Except for COSMIC TOP SECRET and ATOMAL information, classified information may be extracted from NATO documents for incorporation into a classified document prepared for a U.S. or NATO nation non-NATO contract when the NATO documents have been provided in support of the contract under which the document is to be prepared. Contractors must obtain permission to extract from a COSMIC TOP SECRET or ATOMAL document from the CUSR through the DSS. Government personnel shall obtain permission from their local sub-registry.

2. If extracts of NATO information are included in a non-NATO document produced by a U.S. contractor or DoD Component, the document will be marked with U.S. classification markings. The overall classification of the document will reflect the highest classification of the material, NATO or U.S., contained in the document. The caveat, "THE DOCUMENT CONTAINS NATO (LEVEL OF CLASSIFICATION) INFORMATION" also is to be marked on the front cover or the first page if there is no cover, of the document. Additionally, each paragraph or portion containing the NATO information will be marked with the appropriate NATO classification marking, abbreviated in parentheses (e.g., NS) preceding the portion or paragraph. If information is extracted from NATO source material and U.S. source material contains conflicting classification requirements, consult the DSS or DoD Component security manager, as applicable.

3. The pages containing NATO portions are to be marked with a U.S. classification reflecting the highest level of classified information contained on the page. For example, if the page contains U.S. CONFIDENTIAL and NATO SECRET information, the highest overall classification would be SECRET. When all information on an internal page is NATO information, that page shall be marked with the highest NATO classification (e.g., NATO SECRET).

4. Extracted NATO RESTRICTED information may be included in U.S. unclassified documents provided the applicable marking requirements cited above are met. In addition, the U.S. document must be marked. "THIS DOCUMENT CONTAINS NATO RESTRICTED INFORMATION." The document must be controlled as described in USSAN 1-07 and the NISPOM.

5. A list is to be maintained in the U.S. document of all source documents from which extracts are included. Contractors must provide a copy of this list to the contracting DoD Component.

6. Declassification or downgrading of NATO information in a U.S. document requires the approval of the originating NATO member nation or civil or military body. Contractors are to submit requests through the DSS to the CUSR for NATO contracts, through the contracting DoD Component for U.S. contracts, and through the DSS for non-NATO contracts awarded by a NATO member nation. DoD Components will submit their requests directly to the CUSR. The response must be retained with the affected documents until they are returned to the originator, contracting agency or destroyed.

7. U.S. documents and documents prepared for a NATO nation in support of a non-NATO contract containing NATO classified information will be controlled, protected, and accounted for in the same manner as equivalent U.S. and foreign government classified documents. However,

they must be stored and accounted for in such a manner that they are not commingled with other classified documents. This can be accomplished by using separate drawers in the same container, or even by using file dividers in the same drawer. Access to the container will be controlled based on the classification of the NATO information.

J. RELEASE OF U.S. INFORMATION TO NATO

1. **Disclosure Authorization**. The release of U.S. classified information to NATO requires an export authorization or other written disclosure authorization in compliance with Chapters 2 and 3. When a DoD Component awards a contract for the preparation of material that the DoD Component is to release to NATO, the Component must obtain the necessary disclosure authorization from an appropriate disclosure authority identified by the list of originators required pursuant to subsections C.4. and H.5., above.

2. **Marking the Documents**

a. When a document containing U.S. classified information is being specifically prepared for NATO, the appropriate NATO classification markings will be applied to the document only after the U.S. information contained in the document is authorized for release to NATO. If the information is to be provided pursuant to a NATO contract, the requirements of the NATO security aspects letter and security requirements checklist will be followed. However, if U.S. classification guidance for the U.S. information is not consistent with NATO classification guidance, the matter must be forwarded to the DSS for resolution. The U.S. classified information will be identified in the document by paragraph markings.

b. Documents prepared for NATO that contain U.S. classified information, and U.S. classified documents that are authorized for release to NATO, must be marked on the cover or first page, as applicable, "THE INFORMATION IN THIS DOCUMENT HAS BEEN AUTHORIZED FOR RELEASE TO (cite the NATO organization) BY (cite the applicable license or other written disclosure authorization.)" If there are restrictions on further dissemination, the restrictions also must appear on the document.

3. **Transmission**. The supporting DSS industrial security representative will provide transmission instructions to the contractor. DoD Components will comply with Chapter 6. However, the following general rules apply

a. The material must be addressed to a U.S. organization at NATO (e.g., U.S. Mission to NATO, U.S. National Military Representative to Supreme Headquarters Allied Powers Europe (SHAPE), U.S. Representative to NATO Maintenance and Supply Agency (NAMSA) which will place the material into NATO security channels. The material must be accompanied by a letter to the U.S. organization providing the necessary transfer instructions and providing assurances the material has been authorized for release to NATO. The material will be properly wrapped as described in USSAN Instruction 1-07 and the NISPOM. However, the inner

wrapper will be addressed to the intended NATO recipient; the outer wrapper shall be addressed to the U.S. organization at NATO; and

b. Classified material to be sent to NATO via mail will be routed only through the U.S. Postal Service and U.S. Military Postal Service channels as registered mail to the U.S. organization affecting the transfer. The use of non-cleared express courier services is not authorized.

K. VISITS

1. **General**. Except as described below, visits by DoD and defense contractor employees to NATO organizations and visits by NATO employees to DoD and defense contractor facilities are to be handled in accordance with Chapter 7. The DoD Component security office (for DoD employees) or DISCO (for contractors) will provide the required NATO Personnel Security Clearance Certificate to NATO security authorities.

2. **Recurring Visits**. NATO has established special procedures for recurring visits involving contractors, government departments and agencies, and NATO commands and agencies participating in a contract or program. Recurring visits for these programs will be handled as follows:

a. The NATO Management Office or Agency responsible for the program or contract will prepare a list of government and contractor facilities participating in the program or contract. For NATO Industrial Advisory Group (NIAG) programs, the list will be prepared by the responsible staff element. The list will be forwarded to DISCO, which will forward it to the participating U.S. contractors and DoD Components for verification.

b. Each participating contractor and DoD Component will prepare a visit request listing all personnel who will be required to participate in international visits in connection with the program. See Appendix P for the visit request format.

c. The visit request will be submitted to DISCO or the DoD Component security office (as applicable) for security clearance verification and will then be forwarded to the sponsoring NATO organization and other NSAs of participating NATO member nations. For DoD contractors the request will be forwarded by DISCO; DoD Component requests will be forwarded according to DoD procedures. Visit requests received by DISCO from other NSAs will be forwarded to the participating U.S. contractors and DoD Components. Upon receipt of these visit requests, direct visit arrangements may be made between the security offices of the participating contractors and government organizations. To arrange the direct visits, a visit notification containing the purpose of the visit, the proposed date(s) of the visit, the name(s) of the visitor(s), the serial number on the appropriate facilities list, and the person to be visited will be forwarded directly to the facility to be visited at least 72 work-day hours in advance of the proposed visit. This may be accomplished by electronic message or telefax.

d. Contractors and DoD Components must notify DISCO when a person listed on the original visit authorization no longer requires access. DISCO will also be notified through individual visit requests, using the prescribed format, of any persons who must be added to the block list.

e. A separate visitor record for NATO visits, including those U.S. personnel assigned to NATO shall be maintained as an export authorization by contractors in compliance with the International Traffic in Arms Regulations (ITAR) (*reference c*).