



DEPARTMENT OF THE NAVY  
OFFICE OF THE CHIEF OF NAVAL OPERATIONS  
2000 NAVY PENTAGON  
WASHINGTON, D.C. 20350-2000

IN REPLY REFER TO

OPNAVINST 5510.100C  
DNS-34

APR 17 2007

OPNAV INSTRUCTION 5510.100C

From: Chief of Naval Operations

Subj: NATO SECURITY PROCEDURES FOR CONTROL POINTS UNDER THE  
ADMINISTRATIVE CONTROL OF THE CHIEF OF NAVAL OPERATIONS  
SUB-REGISTRY

Ref: (a) United States Security Authority for North Atlantic  
Treaty Organization Affairs (USSAN) 1-69  
(b) SECNAV M-5510.36

Encl: (1) Security Indoctrination Certification and Request for  
Clearance and Special Access  
(2) Instructions for Couriers of NATO Classified Documents  
(3) Sample Courier Authorization letter

1. Purpose. To update security policy and procedural guidance for the control and handling of North Atlantic Treaty Organization (NATO) classified material by Control Points within the National Capital Region and established under the administrative control of the Chief of Naval Operations (CNO) Sub-Registry (DNS-34B). This instruction is a complete revision and should be read in its entirety.

2. Cancellation. OPNAVINST 5510.100B

3. Scope and Applicability. Basic guidance is provided for the NATO Security Program for both military and civilian personnel assigned to those Department of the Navy (DON) commands for which the CNO Sub-Registry has been authorized to act as NATO Control Point under their administrative cognizance. This instruction supplements references (a) and (b).

a. References (a) and (b) establish and implement security procedures for safeguarding classified NATO and ATOMAL material within DON.

b. This instruction establishes how the policies and procedures contained in references (a) and (b) will be implemented by Control Points under the administrative control of the CNO Sub-Registry. In these procedures, the following definitions are used:

(1) "NATO material" applies to all NATO classified paper and electronic documents.

APR 17 2007

(2) "Accountable NATO material" applies to all COSMIC, NATO SECRET and ATOMAL (regardless of classification level) material.

c. General Regulations

(1) The CNO Sub-Registry is responsible for:

(a) The control, accountability, and distribution of all NATO material and accountable NATO material.

(b) The establishment, inspection, and dis-establishment of NATO Control Points.

(c) Maintaining up-to-date lists of all personnel authorized to have access to NATO classified information in the CNO and other commands served by the CNO Sub-Registry.

(2) CNO Sub-Registry personnel are the only authorized persons to reproduce, destroy, or make entry of changes or corrections to COSMIC and ATOMAL documents.

(3) NATO documents addressed to the CNO Sub-Registry shall be available for distribution to Control Points via SIPRNET computer terminals. All NATO documents classified Secret and above received via the SIPRNET router or hard copy paper by Control Points from sources other than the CNO Sub-Registry shall be delivered immediately to the CNO Sub-Registry for accountability and control.

(4) Requests to the Central U.S. Registry for establishment or disestablishment of Cosmic Top Secret, NATO Secret, or ATOMAL Subregistries shall be submitted via CNO (N09N2) per reference (a).

(5) Control Points are responsible for controlling NATO material below the Sub-Registry level.

(6) NATO Control Officer is responsible for controlling access to NATO material per reference (a) and maintains files showing custody of all accountable NATO material.

(7) Establishment Procedures

(a) A Control Point under the CNO Sub-Registry shall be established for each OPNAV/SECNAV/DON Staff Office that requires receipt of NATO material. The Command/Directorate Head shall submit a written request to the CNO Sub-Registry (CNO (DNS-34B)) justifying the need to be established as a Control Point. Upon approval by CNO (DNS-34), the Command/Directorate shall appoint in writing, one individual to

act as Control Officer and one or more alternates who will be responsible for the receipt, distribution, and keeping record of all NATO classified documents within the Control Point they service.

(b) Requests to be established as a Control Point by commands other than those listed in paragraph 3c(7)(a) above shall be submitted to the CNO (N09N2) per the requirements of reference (a). If approved by CNO (N09N2) and established under the cognizance of CNO (DNS-34), the command shall appoint the individuals as described in paragraph 3C(7)(a) above.

(c) Each Control Point must update and submit a Signature List, DAAG Form 29, located at <https://secureweb.hqda.pentagon.mil/cusr>, listing the Control Officer and Alternate(s).

(8) Dis-establishment Procedures. The command shall notify CNO Sub-Registry (DNS-34B) in writing when the need for a Control Point no longer exists. Accountable NATO material and records to be retained (not eligible for local destruction) shall be returned to the CNO Sub-Registry. Those records (such as destruction reports) eligible for destruction in the near future must be retained, and disposed of by the command when eligible.

(9) Change of Control Officer in a Control Point. When a Control Point notifies the CNO Sub-Registry of a change in the Control Officer, the CNO Sub-Registry will conduct an inventory of the Control Point to ensure their records and documents are in order for the new Control Officer. During this inventory, the CNO Sub-Registry will verify that the new Control Officer is aware of the proper procedures for the handling of NATO documents and briefing of personnel in the Control Point.

d. Access to NATO Material

(1) Control of Access to NATO Material. Only the Control Officer or alternate is authorized to and responsible for briefing all personnel under his/her cognizance requiring access to NATO material on NATO procedures, authorizations, and for processing requests for certificates of security clearance.

(2) General. COSMIC, NATO, and ATOMAL are not classifications, but indicate procedures for the handling and issuing. Access to NATO information is granted on the basis of:

(a) A U.S. security clearance of the same level as classified information;

(b) The assurance that the procedures are known and understood by the person; and

APR 17 2007

(c) The "need-to-know".

Authorization for access to COSMIC information permits access to NATO information (less ATOMAL).

(3) Procedures for Access

(a) Before granting access to ATOMAL information, all personnel must:

1. Have a final U.S. security clearance for the same level of classified information access is required;

2. Have an ATOMAL Briefing/Re-briefing Certificate stating that they have read and understand NATO security rules covered under attachment 3, section 6, paragraphs e through g of reference (a) and they understand the consequences that sections 793 and 794 of Title 18, U.S. Code, and have a "need-to-know".

(b) Before granting access to NATO Top Secret (COSMIC) information, all personnel must have a final U.S. Top Secret security clearance; have signed a Briefing/Rebriefing/Debriefing Certificate (OPNAV Form 5511/27) located at <https://secureweb.hqda.pentagon.mil/cusr>, stating that they have read and understand NATO security rules covered under attachment 3, section 6, paragraphs e through g of references (a) and they fully understand the consequences that Sections 793 and 794 of Title 18, U.S. Code provide when classified information passes into unauthorized hand either by intent or through negligence, and have a "need-to-know".

1. OPNAV Control Officer shall submit the original and one copy of the request for access, using the format provided in enclosure (1), to the CNO Sub-Registry who will then certify the level of the U.S. security clearance held by each person requiring access. For activities outside of OPNAV, the Control Officer shall send the request via the command or Commanding Officer to verify a U.S. security clearance is held by each person. Each request shall include an OPNAV Form 5511/27 that is signed by the person needing the authorization and verified by the Control Officer.

2. The Control Officer shall notify CNO Sub-Registry (DNS-34B), in writing, of personnel whose authorization is cancelled due to detachment, transfer, or when the "need-to-know" no longer exists.

(c) Before granting access to NATO Secret and NATO Confidential information, personnel must possess a U.S. final

APR 17 2007

security clearance, at a minimum, at the same level of the classified information they require access to, have signed a briefing certificate (OPNAV Form 5511/27), stating that they read and understand the proper security regulations in attachment 3, section 6, paragraphs e through g of reference (a), and know the penalties prescribed by law for negligence or intentional compromise of classified information, and have a "need-to-know".

(d) Once the CNO Sub-Registry has endorsed the request for authorization, the Control Officer is authorized to approve access to NATO documents, only when personnel meet the requirements above. The Control Officer and each office he/she serve shall maintain a list of persons permitted access to NATO information.

(e) Each Control Point must have on file with the CNO Sub-registry a signature list DAAG Form 29, which lists the Control Officer and Alternate(s). The Control Officer and Alternate(s) are the only personnel authorized to access NATO documents from the SIPRNET or pickup and deliver NATO to the Sub-registry for the Control Point.

(f) CNO (DNS-34B) will ensure access levels are entered into the local OPNAV Automated Security Information System (OASIS) and the Joint Personnel Adjudication System (JPAS) as official records.

e. Markings

(1) "COSMIC" appearing on a document reflects: the document is the property of NATO and the document is subject to special security procedures outlined in reference (a). These markings applied to documents indicate that the documents may be circulated throughout the entire NATO organization. NATO TOP SECRET material is marked "COSMIC TOP SECRET".

(2) ATOMAL information is either U.S. Restricted Data, Formerly Restricted Data, or UK ATOMIC information that has been officially released to NATO.

(3) NATO has four levels of classified materials and marked as: COSMIC TOP SECRET, NATO SECRET, NATO CONFIDENTIAL, or NATO RESTRICTED. The first three classifications are the same as the U.S. classifications and are given equivalent protection. RESTRICTED material will be protected equivalent to FOR OFFICIAL USE ONLY (FOUO) material. The U.S. does not have a security classification equivalent to "NATO RESTRICTED". NATO information classified as RESTRICTED shall be safeguarded in a manner that will prevent disclosure to non-government personnel.

NR 1 7 2007

(4) NATO RESTRICTED information may be stored in filing cabinets, desks, or other containers located in rooms where internal building security is provided during the non-duty hours by U.S. Government or government contractor personnel. Where such internal security is not available, locked buildings, or rooms usually provide adequate after-hours protection.

(5) NATO classified information included in U.S. classified documents shall be identified by applying the appropriate NATO marking to the extracted portions. The top and bottom of the page containing the NATO information shall bear only the U.S. classification marking except when all information on the internal page is NATO, that page should be marked with the highest NATO classification. The cover (or in the absence of a cover, the first page) of the document shall contain the following notation: "This document contains NATO (classification) information".

(6) When NATO information classified NATO CONFIDENTIAL and above is extracted and included in U.S. unclassified documents, the document shall be classified and marked with the highest classification in U.S. terms, and protected at the U.S. classification level equivalent to the level of classification of the extracted material. The cover (or in the absence of a cover, the first page) of the document shall contain the same statement as cited above.

(7) When NATO RESTRICTED information is included in U.S. unclassified documents, the following statement shall be affixed to the top and bottom of the page: "This page contains NATO RESTRICTED information and shall be safeguarded per USAAN Instruction 1-69". The cover (or in the absence of a cover, the first page) of the document shall contain the following notation: "This document contains NATO RESTRICTED information", and each extracted portion be marked with "NR".

f. Application of NATO Markings to U.S. Documents

(1) U.S. information shall retain its U.S. security classification (shall not bear COSMIC or NATO markings) until it is introduced into the NATO Organization.

(2) Documents prepared only for U.S. use shall not bear a NATO marking. This includes:

(a) Any U.S. comments on NATO papers where such comments are not intended for introduction into the NATO Organization;

(b) U.S. letters of transmittal which reference NATO documents.

APR 17 2007

(c) File copies of U.S. documents released to NATO containing the NATO markings, which remain in U.S. channels.

(3) Normally, NATO markings are applied by the CNO Sub-Registry (DNS-34B). In the case of bulk shipments of documents, the NATO marking may be applied by the preparing agency.

(4) Extracted ATOMAL information placed in U.S. documents will be appropriately portion-marked with the ATOMAL classification markings, the first page and/or cover containing the "RD/RFD or UK ATOMIC" caveat statement, and the document marked with the highest classification of U.S. terms.

g. Hand carrying of NATO Material within a command or immediate vicinity

(1) The Head, CNO Sub-Registry (DNS-34B) is the approval authority for hand carrying NATO materials. The Control Officer for the NATO Control Point may authorize the hand carrying of NATO classified material within the command or its immediate environs.

(2) When NATO classified material is being carried within the command or its immediate environs (your building) as part of normal duties, reasonable precautions, such as placing a U.S. classified cover sheet over the material, will be taken to prevent inadvertent disclosure and stamped with appropriate NATO classified markings.

(3) If the movement requires transportation other than walking, double-wrap and address the NATO classified material the same as you would a classified U.S. document. A briefcase may be considered the outer wrapping in this case.

(4) When the accountability of NATO classified material is actually being transferred to another command or Control Point, it must be processed according to the procedures outlined above in paragraph 3g(1).

h. Courier Cards

(1) Continental United States (CONUS) Courier Authorization Cards (DD Form 2501) are for use by individuals hand carrying classified material, by means of surface transportation within a commuting area of the command. CONUS Courier Authorization Cards will be issued to individuals by their issuing authority (Security Coordinators or Alternates for OPNAV, SECNAV, or DON Staff Offices), on an "as needed" basis for a period up to one year. Individuals will retain Courier Authorization Cards on a permanent basis to preclude unauthorized removal of classified material. Outside of the Continental

APR 17 2007

United States (OCONUS) Courier Authorization Cards for NATO classified material are issued only by the CNO Sub-Registry (DNS-34B) after receipt of classified courier's responsibility acknowledgment sheet at enclosure (2). A courier authorization request must be submitted on command letterhead to the command Security Manager to justify need to courier NATO material OCONUS. A courier certificate at reference (a), page 3-8, is signed by the Security Manager must accompany member in a travel status.

NOTE: The personal hand carrying of COSMIC Top Secret documents internationally is prohibited.

i. Authorization to hand carry NATO Classified Material in a Travel Status

(1) Because of the associated security risks inherent in hand carrying classified material while in a travel status, authority will only be granted when:

(a) The courier has taken all reasonable steps, however is unable to arrange for the information to be available when it is required;

(b) The courier is authorized for access to at least the level of the classification of the documents to be carried;

(c) Documents have been listed, checked against the list, and a copy of the list is retained by the courier's NATO Control Officer (for hand carrying within the immediate environs of the command) or the CNO Sub-Registry (for other hand carrying authorization);

(d) Courier is aware of any secure storage facilities on NATO or national premises available during any planned overnight stops;

(e) Courier has a suitable container or case, bearing a label with identification and instructions to finder, into which the documents can be locked and kept with the courier at all times;

(f) Package to be sealed contains only NATO official documents;

(g) Package is sealed with a NATO, national or company seal, or protected under procedures designed to prevent customs examinations;

APR 17 2007

(h) The blocks entitled "Details of Itinerary" and "Specimen of Seal Used" on the courier certificate are completed in accordance with the information at the bottom of the certificate;

(i) Courier is not routed by surface routes through non-NATO nations or by air routes over countries with special security risks (attachment 3 to enclosure (2) of reference a), and is not scheduled to travel in such country-owned aircraft or ships;

(j) Authorities at the destination of the courier are informed of the expected date, time, and place of arrival;

(k) Courier has read and signed the NATO acknowledgement and handling instructions at enclosure (2).

(2) When authorization has been granted to hand carry NATO documents across national frontiers between NATO nations, the following instructions must be read and adhered to:

(a) Accounting for documents

1. The documents you are to carry must be listed, and you must check them against the list in front of the authorizing official. A copy of the list must be left with the authorizing official or with your office.

2. If you have been authorized to carry the same documents on your return journey, you must have them checked against your list on your return.

(b) NATO Courier Certificate. You will be provided with a NATO Courier Certificate bearing an authorizing official's signature and stamp. Keep this certificate on your person.

(c) Sealing of Packages

1. The authorizing official will seal your NATO official documents in a package. A specimen of the seal used will be placed opposite the appropriate stage of your journey on the courier certificate.

2. If you have opened your package to use the documents, you must have it re-sealed (and a specimen of the seal used, placed on the courier certificate) for each stage of your journey which involves crossing a frontier.

3. If you are carrying documents for someone else, the sealed package must bear the name and address of the sender and of the addressee.

APR 17 2007

(d) Container. As soon as your package has been sealed, lock it in a briefcase and see that the case has a label on it with identification and instructions to finder.

j. Return with NATO Material. Upon your return to the command, any NATO classified documents acquired must be turned in to the Control Officer or Alternate for accountability. If documents are NATO Secret, the Control Officer/Alternate must bring them to the CNO Sub-registry to establish proper controls. Once the documents are controlled they will be returned to the Control Point for retention or appropriate action.

k. Accounting, Control, Receipt, and Transmittal

(1) Only the Control Officer or Alternate shall receive accountable documents from the CNO Sub-Registry.

(2) Only the Control Officer or Alternate shall return accountable documents to the CNO Sub-Registry.

(3) Only the Control Officer or Alternate shall request documents held by the Control Point.

(4) ATOMAL material shall not be maintained or controlled by a Control Point. If ATOMAL material is received from sources other than the CNO Sub-Registry, it must be brought to the Sub-Registry for control and accountability. All ATOMAL material must be controlled by the CNO Sub-Registry. Recipients may allow access to other persons if necessary, but they must be aware of the document's location, ensure anyone having access to it has a valid ATOMAL authorization on file with the CNO Sub-Registry, and make sure the name on the disclosure sheet is printed and signed. ATOMAL material held at a Control Point for more than six months must be justified to the CNO Sub-Registry in writing.

(5) Documents classified NATO Restricted shall be packed and mailed as U.S. First Class Mail and at a minimum be single wrapped.

(6) Documents containing NATO Restricted information shall, at a minimum, be transmitted by U.S. Postal Service First Class Mail within the U.S. and its territories.

(7) To ensure continuous control by U.S. personnel, transmission outside the U.S. and its territories shall be U.S. Postal Service First Class Mail using an APO/FPO address. Geographical addresses and international mail channels may be used for transmitting NATO RESTRICTED to or within NATO countries.

APR 17 2007

1. Reproduction. Accountable documents shall be reproduced only by the CNO Sub-Registry, and only if authority has been given by the Central U.S. Registry. Documents to be reproduced should be brought to the CNO Sub-Registry (DNS-34B), Room 1D469 for reproduction. The CNO Sub-Registry will provide the copy numbers assigned to the reproduced copies for Control Points and inform the Central U.S. Registry of reproduction of COSMIC or ATOMAL documents after receiving authority and their concurrence.

m. Dissemination of NATO Material and Exchange of Documents

(1) NATO documents to be mailed to other U.S. Commands shall be returned to the CNO Sub-Registry by the Control Officer or Alternate with proper notation on the route slip. CNO Sub-Registry shall mail the documents to the addressee through the proper channels. Exchanging or sending documents controlled by CNO Sub-Registry between Control Points in OPNAV to Sub-Registries, Control Points, or activities outside of OPNAV without sending them through the CNO Sub-Registry for coordination is forbidden.

(2) U.S. documents shall not be attached to or included with NATO documents being sent to other activities.

NATO material enclosures to U.S. letters or documents shall be brought to the CNO Sub-Registry for forwarding under "separate cover" through the proper NATO organization channels.

n. Release of Information to NATO Organizations. Except in cases where authority has been specifically assigned, requests to release classified documents to NATO Organizations shall be forwarded to the Navy International Programs Office (Navy IPO-01B), for disclosure authorization. After receipt of authorization, the documents should be forwarded to the proper U.S. document officer for release. Documents having unclassified information may be released by the originator of the document. Those documents shall be sent to the proper U.S. documents officer.

o. Transmission of NATO Material and Handling Procedures for Incoming Electronically Sent Messages

(1) The OPNAV Communications Officer (Deputy Navy Liaison, Pentagon Communications Center) is assigned as an Alternate Control Officer of the CNO Sub-Registry for messages only. The OPNAV Communications Officer is responsible for the enforcement of proper handling procedures for NATO material in the OPNAV Communications Office and shall control the reproduction of all messages bearing a NATO marking.

APR 17 2007

(2) During normal working hours, all copies of COSMIC and ATOMAL messages received shall be given to the CNO Sub-Registry. Other NATO messages shall be sent to the Control Point of the responsible activity.

(3) All NATO messages received by the Communications Office after normal working hours shall be sent to the Navy Department Duty Captain in the Navy Command Center (NCC) for action. The messages shall be handled only by persons having the proper authorization for access to NATO information. On completion of action, messages shall be returned to the Communications Office for delivery on the next working day. The destruction of NATO messages by NCC personnel is forbidden.

(4) NATO classified messages shall be handled only by those persons having proper authorization for access to NATO classified information.

(5) Accountability for COSMIC and ATOMAL messages shall be accomplished by the CNO Sub-Registry (DNS-34B) and the same control applied as to other accountable documents.

p. U.S. Electronically Transmitted Outgoing Messages

(1) Classified messages. Classified information to be released to NATO Organizations by message must be cleared for disclosure authorization before sending. All messages originated in the DON must be routed through NAVYIPO-01B. It is the originator's responsibility to make sure the message is cleared by NAVYIPO-01B before release is authorized. Messages shall be addressed to the proper U.S. representatives authorized to process NATO messages listed in the Standard Navy Distribution List (SNDL) Part 1 and shall include internal passing instructions indicating the ultimate addressee followed by the statement: "This message is authorized for release into NATO channels and authorization is granted to apply the NATO markings". Example of passing instructions of a message addressed to USDOCOSOUTH: "USDOCOSOUTH NOT ADDEE PASS ACTION (INFO) TO CINCSOUTH. THIS MESSAGE IS AUTHORIZED FOR RELEASE INTO NATO CHANNELS AND AUTHORIZATION IS GRANTED TO APPLY THE NATO MARKINGS".

(2) Unclassified messages. Messages containing unclassified information to be entered into NATO Organizations shall be delivered to the Communications Office for transmission. These messages shall be addressed to the U.S. documents office and will include internal passing instructions indicating the intended addressee followed by the authorization statement quoted in the preceding paragraph. Review by NAVYIPO-01B is not necessary.

APR 17 2007

(3) Communications "Service" messages. Communications Officers and/or Communications Watch Officers are assigned the authority to apply the NATO markings on service messages only. These service messages should not contain any intelligence information and must carry the same classifications and priority as the message being serviced. Review by NAVYIPO-00X is not necessary.

(4) For outgoing messages processed following paragraphs (1) through (3) above, NATO markings shall not be applied to copies sent to or kept by a U.S. agency.

q. Safeguarding and Storage. NATO documents shall be safeguarded and stored in containers required for the storage of U.S. documents of equal security classification. NATO documents may be stored in the same containers as non-NATO material provided they are separated by a file divider. No indication as to the subject matter shall appear on the outside of the container. NATO classified material shall not be retired to a U.S. depository, but shall be destroyed when it has served its purpose. Only the CUSR as the official U.S. repository has authority to permanently hold and/or retire NATO material. Knowledge of combinations will be restricted to the smallest number of persons. Combinations on containers with NATO documents have to be changed at intervals of not more than 12 months, whenever a change of personnel occurs or whenever a compromise has occurred or is suspected. In addition, if NATO material is secured in the same container with U. S. material, the combination will not be marked "NATO", but will bear U.S. markings with the caveat "(NATO) COSMIC/ATOMAL (if applicable) access required." If the container only secures NATO material, the envelope and the form containing the combination will bear NATO markings.

r. Destruction of NATO Material. ATOMAL and COSMIC documents shall be destroyed only by CNO Sub-Registry personnel. Other NATO documents issued to Control Points for retention may be destroyed by the Control Point, under security regulations for equal U.S. material, but not earlier than six months from date of receipt. Destruction reports of NATO material must be kept in accordance with paragraph 113(b) and (d) of reference (a); for COSMIC Top Secret, minimum of ten years and for NATO Secret, minimum of two years. Destruction reports for NATO must contain the CNO Sub-registry Document Control Number, Short Title, Copy Number(s), Date of Document, and be signed by two cleared and briefed people. A copy of the destruction reports for NATO Secret should be forwarded to the CNO Sub-Registry when documents have been destroyed by the Control Point. Destruction reports for NATO Secret must be maintained for a period of at least two years from date of signature on report. Reports of destruction

APR 17 2007

for NATO material must be separate for ATOMAL, COSMIC, and NATO SECRET and be separate from U.S. classified material. Emergency destruction plans shall include instructions for safeguarding NATO material. All NATO documents on hand should be reviewed at least every six months to determine if they have served their purpose. If it is determined that a document has served its purpose, it can be destroyed before the maximum retention date. This also applies to excessive copies of the same document.

s. Security Clearance Certificate for Access to NATO Classified Information during Travel

(1) To comply with NATO requirements, whenever an individual travels overseas to confer with officials of a foreign government or a NATO office, agency, command, or contractor, and the visit will involve access to NATO classified information, the courier certificate at page 3-36 of reference (a) shall be executed by an appropriate agency official. An authentication seal is desirable, if available.

(2) This certificate shall be sent in advance to assure timely receipt by the addressee. In exceptional circumstances, the information required by the certificate may be supplied by other means of communication but must be confirmed in writing. A copy of this certificate should not be given to the traveler although it is advisable to include security clearance status in official orders.

t. Annual Inspection of Control Points. Control Points must be inspected every 18 months and inspection reports kept for review by CNO Sub-Registry during the 18 month CUSR inspection cycle.

(1) Control Points located in the Washington, DC area shall be inspected by CNO Sub-Registry personnel on an annual inspection schedule arranged with individual Control Points.

(2) CNO Sub-Registry has no Control Points outside the Washington, DC area. Therefore, there are no requirements for inspections outside of the Metro-Washington, DC area.

(a) The inspection report shall be completed regardless of whether there is NATO material on hand or not. When a question does not apply to the control point, the words "not applicable" or "n/a" should be written in.

(b) A signed copy of the inspection report should be maintained by the CNO Sub-Registry (DNS-34B). Corrective action of any discrepancies should be included in the "remarks" section.

(c) The NATO Inspection checklist at

APR 17 2007

<https://secureweb.hqda.pentagon.mil/cusr> used in the annual inspection of Control Points shall be available to the CUSR members at inspection time.

u. Compromise and Other Security Violations

(1) When a NATO document is believed lost or compromised, a written report should be sent to the CNO Sub-Registry immediately by the Control Officer of the Control Point concerned, as provided in reference (b), Chapter 12. (Report symbol OPNAV 5510.6B applies.)

(2) All SIPRNET account holders will read the NATO briefing and sign the NATO briefing certificate as a prerequisite to assignment of SIPRNET account. This is done as an additional measure of protection of NATO material.

v. Emergency Action Procedures

(1) The following instructions govern emergency action procedures for the protection, removal, and destruction of NATO classified material during a fire, natural disaster, civil disturbance, or enemy action.

(2) Purpose. To prescribe procedures for safeguarding of all NATO classified material under the jurisdiction of this Sub-Registry in the event of any of the emergencies listed above.

(3) Implementation. For the CNO Sub-Registry and Control Points within OPNAV and SECNAV Offices in the Pentagon, emergency procedures will be implemented at the direction of the Director, Pentagon Force Protection Agency or GSA Building Manager via computer based emergency notification system (CENS) or "Big Voice" intercom announcements. In the event of the absence of the above, the senior individual present will implement these procedures. Occupants will be further alerted through the building alarm system. For those Control Points not physically located in the Pentagon, emergency procedures must be established per their command/building/facility requirements and NATO regulations unless they have been granted a waiver in writing of this requirement by the Central United States Registry.

(4) Procedures. Upon receipt of implementing instruction:

(a) NATO classified material will be returned to authorized security containers which will then be locked and left in place;

(b) Personnel will remain at duty positions pending receipt of further instructions;

APR 17 2007

(c) In the event of natural disaster, (i.e., storms, earthquake, or fire, etc.), necessitating evacuation of personnel, NATO classified material will be secured in authorized storage containers.

(5) Destruction. CNO Sub-Registry and Control Points physically located within the Pentagon are exempt from the requirements outlined in paragraph 114 of reference (a), regarding the emergency destruction of classified NATO material. Control Points not located in the Pentagon need to establish priorities of emergency/destruction which are consistent and relative by level of classification, i.e. Priority 1: TS, CTSA & CTS; Priority 2: US SECRET, NSA & NS; Priority 3: US CONFIDENTIAL, NCA & NC; Priority 4: FOR OFFICIAL USE ONLY, US UNCLASSIFIED requiring Operations Security protection, NATO RESTRICTED, and NATO UNCLASSIFIED. At no time should the emergency evacuation/destruction of NATO material prohibit that of US, of a higher or the same priority, especially COMSEC, Codeword, and Special Access material.

(6) Relocation. Relocation will generally be limited to the relocation of personnel and material required for operations in accordance with contingency plans.

(7) Safety. In the implementation of above procedures, personnel safety will be considered paramount. Above procedures will be implemented only when personal safety of individuals is not in jeopardy.

(8) Guards. The Pentagon Force Protection Agency (PFPA) is responsible for protection of the Pentagon, its occupants and government and private property. The OPNAV Security Manager (DNS-34), interfaces with PFPA and in consonance with guidelines, administers security enforcement procedures within OPNAV and the Secretariat through the Security Coordinators.

(9) Reports. Post reporting is required in the event of any emergency. Reporting will include all details surrounding the emergency including extent of compromise and possible compromise, as applicable. Reporting will be accomplished without delay, through command channels to CNO (N09N). The format contained in reference (b), paragraph 12-8 will be followed relative to compromise and possible compromise situations (Report symbol OPNAV 5510.6B applies).

(10) One copy of these procedures will be conspicuously posted within each area where security containers are used for the storage of classified NATO material.

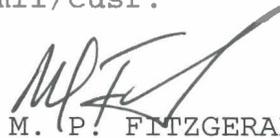
APR 17 2007

4. Action. All personnel assigned to the offices and commands on distribution for this instruction shall comply with references (a), (b), and this instruction.

5. Reports and Forms

a. The reports identified in paragraph 3c(8) are exempt from reports control by SECNAVINST 5214.2B.

b. The forms prescribed by this instruction may be procured from the CNO Sub-Registry, Room 1D469, Pentagon, or via <https://secureweb.hqda.pentagon.mil/cusr>.



M. P. FITZGERALD  
Vice Admiral, U.S. Navy  
Director, Navy Staff

Distribution:

Electronic only, via Department of the Navy Issuances website  
<http://doni.daps.dla.mil>



APR 17 2007

## Security Awareness Briefing Objectives

Because of the increased threat posed by terrorists and hostile intelligence operatives, it has become vitally important that we recognize that Pentagon employees are part of the first line of defense against those who wish to do us harm. With that in mind, it is critical that all employees receive basic security awareness training to enable them to understand and implement basic security measures on a routine basis:

1. **Badges.** Ensure that every individual entering the Pentagon building knows how to obtain and display the proper security badge. Ensure also that every individual knows that white badges are for government personnel, pink badges are for contractors, tan badges are for foreign personnel and blue badges with "PRESS" printed on them are for members of the news media. Additionally, ensure that all personnel know that lost badges must be immediately reported to the Pentagon Force Protection Agency (PFPA) Office at (703) 697-5555.
2. **Escorts.** Ensure that every individual escorting a visitor in the Pentagon building understands that they may not leave visitors unattended at any time. Additionally, every individual working in the Pentagon will know that they are required to report unattended visitors to PFPA.
3. **Classified Materials.** Ensure that every individual working in the Pentagon knows that classified material papers, as well as computers with classified information, may not be removed from the Pentagon without a proper courier authorization and without proper packaging and protection. Inside the Pentagon, no material may be carried outside office spaces unless it is also properly covered and safeguarded.
4. **Disposal.** Ensure that every individual working in the Pentagon knows that controlled documents may not be destroyed without proper authorization and then only in an authorized manner and at an authorized destruction facility.
5. **Classified Storage.** Ensure that every individual working in the Pentagon understands that all classified material must be stored in an approved safe or in an approved open storage office space.
6. **Telephones.** Ensure that every individual working in the Pentagon understands that classified information may only be discussed only on secure telephones.
7. **Faxes.** Ensure that every individual working in the Pentagon understands that faxes containing classified material may only be transmitted from a secure fax machine to a secure fax machine.
8. **Cellular Phones.** Ensure that every individual working in the Pentagon understands that all cellular phones must be disconnected from their batteries when entering SCIFs, and visitors to SCIFs must surrender their cellular phones to SCIF personnel who will maintain custody until the owner departs.
9. **Computers.** Ensure that every individual in the Pentagon understands that classified information may only be processed on approved secure computers, all approved computers and diskettes must be clearly marked with the appropriate security labels, and personally owned computers may never be used to process classified material.
10. **Photocopiers.** Ensure that every individual in the Pentagon understands that classified material must be properly marked and may only be copied on approved photocopiers and/or reproductive equipment.
11. **Discussion of Classified Subjects and Materials.** Ensure that every individual in the Pentagon understands that discussions of classified subjects or materials are only allowed in approved and secure areas. Discussions of classified subjects in the Pentagon hallways or dining areas, the Center Court area, the POAC, or in private vehicles during commutes to and from the Pentagon, is strictly prohibited.
12. **Procedure for Reporting Suspicious Persons and/or Circumstances.** Ensure that every individual in the Pentagon understands that all-suspicious persons and/or building emergencies (criminal activity, fire, medical) should be immediately reported to PFPA Communications Center at (703) 697-5555. (TDD 693-7008)
13. **Know who is the Security Manager/Security Coordinator.** Ensure that every individual in the Pentagon knows who their Security Manager is and how to reach them.
14. **I understand that I will not be granted access to any classified material, until this form is return to OPNAV Security within 10 days upon receiving this form.**

Print Name: \_\_\_\_\_ Sign: \_\_\_\_\_ Date: \_\_\_\_\_

APR 17 2007

## INSTRUCTIONS FOR COURIERS OF NATO CLASSIFIED DOCUMENTS

It has been found necessary to appoint you as an official courier to carry NATO classified material. Your courier authorization will accord the material you are carrying immunity from search and examination by Customs and Immigration officials of the countries whose borders you cross.

You are reminded of the following precautions which you will observe for the protection of the classified material that you will carry:

1. The package or bags containing the classified material must be covered by an official seal to prevent customs examination.
2. A list of all NATO classified documents you will carry must be inventoried and recorded by the appropriate office of your department, agency, or command prior to your departure.
3. Throughout the journey and while at destination, the classified material must never leave your possession unless deposited in a place of safety as provided for under the security arrangements of the diplomatic or military missions or commands of this country, national ministry or the host country, or with a NATO international agency.
4. NATO classified material must not be discussed in public places such as hotels or lounges.
5. NATO classified material must not be read in aircraft, trains, ships, or any other vehicles.
6. NATO classified material must not be left unattended in hotel rooms, staterooms on trains or ships, or stored in repositories, such as hotel safes. You may delegate your responsibility for direct surveillance of the classified material you are carrying only under the security arrangements of a United States diplomatic mission, United States military command, a host NATO government, or a NATO international agency.
7. Upon your return, the classified documents (or receipts for them if they are delivered into the custody of another authorized recipient) must be inventoried against the list prepared before departure. Should any NATO classified documents be acquired, the COSMIC control officer, or designated officer of your department, agency, or command will pick up accountability. Some of the measures necessary to sustain good security may be cumbersome, especially when at the end of a tiring day's work a journey to some other part of the city is necessary to deposit your papers in a place of safety. It is easy to persuade one's self that no harm will be done by keeping the papers overnight in the hotel or some equally insecure place. In reality, a person is presenting an easy target for the agents of foreign intelligence services by so doing and the records of the security services of NATO countries contain cases of loss or compromise of documents attributable to this dangerous practice. Should you encounter any security difficulties during your trip, please bring them to the attention of this office so that remedies may be worked out for the benefit of other NATO travelers.

\_\_\_\_\_  
Signature of appropriate briefing official

\_\_\_\_\_  
Date

I certify that I have read and understand the instructions set forth above which pertain to the handling of NATO classified documents in my custody while I am an official courier.

\_\_\_\_\_  
Signature

Enclosure (2)

SAMPLE

From: Chief of Naval Operations  
To: To Whom It May Concern

Subj: COURIER AUTHORIZATION

1. Mr. John Thomas Doe (full name) of Chief of Naval Operations (name of activity) is authorized to handcarry three sealed packages, 9" X 8" X 24" (describe package(s) being carried) from Chief of Naval Operations, Pentagon, Washington, DC (addresser) to U.S. Naval Postgraduate School, Monterey, CA (addressee name) on 14 June 1989 (date).
2. Flight #59 departs National Airport at 1100 and arrives at (insert flight information including transfer points) Los Angeles International Airport at 1400.
3. Mr. John Thomas Doe (name of courier) will carry a DOD Badge #12345 (type of I.D. w/photo). (If the courier is a civilian, include height, weight, date of birth and signature.)
4. This authorization expires 0900/07 June 1989 (Time/date not to exceed 7 days from date of issue.)
5. Confirmation of this authorization may be obtained by calling (703) 695-3667 or autovon 225-3667 or (703) 695-3121.
6. This package contains classified material and is not to be opened under any circumstances.

ALPHONSO W. MOORE  
Director, Security Programs/  
Command Security Manager

Copy to:  
DNS-34B

SAMPLE

Enclosure (3)