



UNITED STATES MARINE CORPS
COMMAND ELEMENT
II MARINE EXPEDITIONARY FORCE
PSC BOX 20080
CAMP LEJEUNE, NC 28542-0080

5510
G-1

APR 24 2019

POLICY LETTER 3-19

From: Commanding General, II Marine Expeditionary Force
To: Distribution list

Subj: NORTH ATLANTIC TREATY ORGANIZATION PROGRAM

Ref: (a) MCO 5510.18B
(b) II MEFO 5510.1C

Encl: (1) Reporting Compromises
(2) Levels and Processing of NATO Information
(3) II MEF NATO Inventory Form
(4) II MEF Brief/Rebrief/Debrief Certificate

1. Purpose. Per the references, to establish policy regarding the receipt, retention, storage, release, and sharing of North Atlantic Treaty Organization (NATO) information within the II Marine Expeditionary Force (II MEF). The enclosures are provided in support of program compliance.

2. Cancellation. II MEF Policy Letter 5-17.

3. Information. Upon request and when demonstrated that a requirement to receive and maintain NATO classified material, commands can be designated as NATO Control Points. If authorized, a NATO Control Point Officer (NCPO) and Alternate NCPO will be appointed in writing and will ensure compliance with the intent of this Policy.

4. Scope. Accountability and control of NATO material is maintained through a system of checks and balances, supported by a master tracker (inventory), signed records of receipt, validated inventories (at a minimum bi-annually; 31 January and 31 July), inspections, restrictions on reproduction and distribution, and completed destruction reports. These checks and balances ensure a complete record of receipt, reproduction, distribution, custody, and disposition.

a. The NATO Control Point Officer is the primary control point for all NATO material (up to NATO Secret) held by this headquarters (unless authorized separate correspondence by the Marine Corps, Sub-registry). Should a need arise to maintain other than the aforementioned (i.e. ATOMAL or COSMIC) a specific request in writing to higher headquarters is required.

b. Subordinate Element Missions

(1) Subordinate Commanders. Designate for appointment in writing a NCPO and Alternate, and issue written NATO internal control procedures for your commands if deemed applicable as stated in the reference and this Policy.

APR 24 2019

POLICY LETTER 3-19(2) Assistant Chief of Staff (AC/S), G-1

(a) Designate for appointment in writing a NCPO and Alternate for II MEF (Command Element).

(b) Provide the Marine Corps NATO Sub-registry Control Officer (CMC PS) with a current listing of names and specimen signatures for control point personnel who are authorized to receive NATO classified material using the "Control Point/User Office Signature List" DAAG Form 29.

(c) NCPO and Alternate. The II MEF Adjutant is assigned the collateral duty as the NCPO. The Classified Material Control Center Chief serves as the NCPO Alternate. Both the Primary and Alternate must have SIPR access. Manage the NATO Control Point program in accordance with (IAW) this Policy (see enclosure 2) and the reference(s). Both the NCPO and the Alternate are directly responsible to the AC/S G-1 for the day-to-day operations of the NATO Control Point. In addition, the NCPO will seek guidance from the II MEF Security Manager and higher headquarters (CMC PS) on all matters pertaining to NATO classified material. The NCPO is responsible for the following:

a. An inventory of NATO controlled classified material which consists not only of an inspection of documents on hand, but also a reconciliation of the account to ensure that all documents, whether on hand or assigned to a User Office are properly accounted for and tracked. Inventories will include a listing of documents by control number, title, originator, and copy number (at a minimum).

b. Inventories will be conducted bi-annually, and in conjunction with, the relevant quarterly CMCC inventories. Upon the change of a NCPO, there will also be a documented joint physical inventory of all (100 percent) NATO material. A copy will be forwarded to the NATO Sub-registry along with a revised DAAG form.

c. Ensure User Offices are designated in directorates or staff sections that hold NATO classified material (for 30 days or less only).

d. Ensure NATO classified material is not stored with other classified material, but rather in its own GSA approved security container.

e. Maintain a Standard Form (SF) 700 form, "Security Container Information" for all security containers and strong rooms used for storing NATO classified material throughout all II MEF. Combinations to security containers and vaults will be changed at least annually by properly cleared and authorized personnel.

f. Review the SF 701, "Activity Security Checklist" and SF 702, "Security Container Check Sheet" around the II MEF Command Element spaces in order to ensure proper use and retention. The completed forms will be retained for 30 days from last entry. Safes used for the storing of NATO classified material will have their own SF 702 forms. A single SF 701 form can be used in a space that has both non-NATO material and NATO classified material.

POLICY LETTER 3-19

- g. Prepare an emergency action plan (EAP)/emergency destruction plan as required, reviewing annually, to ensure the plan's feasibility.
- h. Maintain a continuous chain of receipts for all classified material controlled by the CMCC (to include NATO).
- i. Maintain a receipt system of all classified documents transferred to other commands.
- j. Ensure that only individuals with proper clearance, access, and "need-to-know" are granted access to NATO information.
- k. Ensure that receipt of improperly transmitted material is reported to the sender, and in compliance with enclosure (1) procedures as applicable.
- l. Maintain a turnover binder containing at a minimum, letters of appointment, access letters, User Office authorization letters (as applicable), inspection results, inventories, and destruction reports. These documents will be maintained for a minimum of 2 years.
- m. Submit timely and accurate reports of receipts, transfers, destruction, and other directed transactions to proper authority.
- n. Maintain control and accountability of all NATO classified (and unclassified) material issued on sub-custody from the Marine Corps Sub-registry. Ensure that if copies are made (as authorized) that proper accountability measures are followed.
- o. Maintain records reflecting the current status and location of NATO classified material received for sub-custody from the Marine Corps NATO Sub-registry.
- p. Brief and debrief personnel assigned to the control point as required by DODD 5100.55, or as detailed in enclosure (2).
- q. Maintain a current listing of personnel who are authorized access to NATO classified national security information (NSI) to include level of access.
- r. ICW the Security Manager ensure a copy of the "Briefing/Rebriefing/Debriefing Certificate" are maintained on file with a retention standard of 1 year after member has departed the Command (the official file for this purpose is the Original maintained by the Command Security Manager).
- s. Ensure NATO stickers establishing the authorization to process NATO information is affixed to all SIPR towers and laptops.
- t. Ensure external hard drives (HDD) storing any NATO documents are identified with NATO control numbers (internal to this Command). Users must report specific information of documents stored in their drives (i.e. subject, dates, etc...)

APR 24 2019

POLICY LETTER 3-19

u. Ensure that a NATO Material Log is maintained denoting when "moving" NATO documents. Verification of access must be made prior to transmitting/transporting.

v. Granting NATO Access. Upon request, verification that member has been briefed via applicable certificate and proof of need to know validated, ensure all personnel requiring access to NATO material are updated in the Joint Personnel Adjudication System (JPAS). Minimum expectation will be document stipulating need for access (i.e. Exercise Orders), duration of access, and minimum clearance level as detailed in JPAS (refer to enclosure (2)). Once access is no longer required ensure appropriate measures are taken to preclude access.

w. Ensure internal access rosters are generated and posted where NATO material is present/maintained (as applicable). Access list for approved cases will be forwarded to the NCPO.

(3) II MEF Principal/Special Staff Officers. You must inform the NCPO or Alternate of all NATO documents in your possession immediately and regardless of level. For all divisions that require temporary maintenance of NATO classified material a User Office designation will be authorized.

User Offices. A command which requires the use of NATO documents for a period of 30 days or less may be designated a NATO User Office. The NATO information point of contact within the User Office shall possess current clearance eligibility and shall maintain an access roster of personnel within the office to verify NATO access and Need-to-Know. User Office may only receive accountable NATO material from the Marine Corps Sub-registry or the Navy Control Point via receipt and must return that material when no longer needed. User Office reproduction or destruction of accountable NATO material is not permitted. A User Office's inventory of NATO classified material is managed by the Sub-registry or Control Point.

(4) Command Security Manager. The II MEF Command Security Manager is responsible for all matters pertaining to classified material (to include NATO). In addition, any compromise and/or breach of security will be reported to the II MEF Security Manager.

(a) Ensure all personnel requiring a security clearance receive a classified material brief, and also, the NATO brief using the "Briefing/Rebriefing/Debriefing Certificate (enclosure 4)."

(b) Upon request, provide a Briefing Certificate (copy) to the NCPO or Alternate for validation/verification of access granted (note: the original is maintained with the Command Security Office, accessible to the G-1 at any time).

(c) JPAS processing in support of access (brief to) will only be administered by the NCPO or Alternate.

(d) Ensure the Industrial Contractor:

1. Keeps the NCPO updated and informed of all contractor personnel that are required to have NATO access (with emphasis on those who change billet descriptions and are no longer authorized access).

APR 24 2019

POLICY LETTER 3-19

2. Maintain an official file copy of all current DD Form 254 "DoD Contract Security Classification Specifications" on all civilian contractors.

(5) Assistant Chief of Staff, G-6

(a) Ensure all applicable Automated Information Systems (AIS) guidelines and regulations associated with transmission of secured/guarded information comply with the NATO guidelines and users informed accordingly.

(b) Ensure Information Assurance Officer (NATO Information Security Officer equivalent) as required signs off on the DAAG Form 29 along with NCPO and Security Manager.

(c) Ensure II MEF Communications Security (COMSEC) Office (MCMO) coordinates with the NCPO each time the NATO COMSEC Information directive is required to be destroyed and a new one is received (semi-annually) in order to comply with this Policy relative to User Office status. The NCPO will destroy the directive and reassign a new NATO number.

c. Emergency Action Plan (EAP)

(1) USSAN 1-07 directs that each NATO Control Point develop its own EAP to take effect in the event of an emergency.

(2) The order to implement any of the EAPs will come from the Commander, or direct representatives (Executive Officer, Deputy, Chief of Staff (COS), or Assistant Chief of Staff (AC/S) via the NCPO). However, in situations that prevent contacting the above personnel, the senior U.S. military person present is authorized to implement the EAP/EDP when time is of the essence. Due to the immediate attention required by a fire, any U.S. service member is authorized to implement the Fire Plan. During implementation of any plan, Two-Person Integrity (TPI) shall be maintained IAW the references.

(a) Fire Plan. Custodial personnel or senior U.S. service member present will:

1. Sound the alarm, call the fire station (911), and notify the appropriate personnel (NCPO, Security Manager, command deck).

2. If possible, secure all NATO material in its storage container. Ensure to close and lock all storage containers.

3. Move to a safe area. Maintain and control access to the area. Record identification and contact information of all personnel entering or exiting the area.

4. Conduct a post-emergency inventory of NATO material and report any losses, destructions, or unauthorized exposures to the NCPO, Security Manager, and custodial personnel IAW the references.

(b) Safety of personnel should always be taken into consideration. Deviation from established plans is authorized when circumstances warrant. Under no circumstances will anyone subject themselves or others to possible death or injury to protect these materials from fire.

APR 24 2019

POLICY LETTER 3-19

d. Emergency Protection Plan. Custodian personnel or senior U.S. service member present will:

(1) Secure all NATO material not immediately required.

(2) Close and lock all storage containers, and take on scene responsibility for protecting NATO material.

(3) Take action to prevent damage to, and maintain the security of all NATO material in the section.

(4) Conduct a post-emergency inventory of NATO material and report any losses, destruction, or unauthorized exposures to the NCPO and Security Manager.

e. Emergency Removal Plan. Removal of NATO materials will only be conducted upon and under the direction of the NCPO.

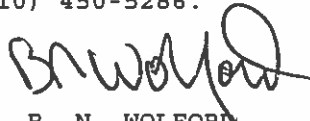
f. Emergency Destruction Plan. Destruction of NATO materials will only be conducted upon and under the direction of the NCPO. A positive record of accountability and accurate accounting of all classified materials destroyed as well as the facts surrounding the destruction must be kept and reported IAW the references by the most expeditious means available. Reports should indicate material destroyed, method and extent of destruction, and any NATO material presumed to be compromised, including serial numbers if possible.

4. Certification

a. This Policy applies to all personnel (e.g. Marines, Navy personnel assigned/attached to II MEF, government civilian employees, contractors, and consultants) employed by, and/or working in any element of II MEF.

b. Privacy Act. Any misuse or unauthorized disclosure of Personally Identifiable Information (PII) may result in both civil and criminal penalties. Any collection, use, maintenance, or dissemination of PII will be IAW the Privacy Act of 1974.

c. For questions regarding this letter, please contact the NCPO at (910) 451-8246/8266 or the Alternate at (910) 450-5286.


B. N. WOLFORD
Chief of Staff

Distribution: A,B

APR 24 2019

POLICY LETTER 3-19Reporting Compromises

1. All suspected or possible compromise of NATO classified NSI shall be reported immediately to the Command Security Manager and NCPO. The following timeline is applicable as derived from MCO 5510.18B. Refer to USSAN 1-07 for further details:

- ____ IMMEDIATELY: Command reporting incident shall conduct an investigation (determination will be made as to whether or not compromise occurred).
- ____ WITHIN 24 HOURS: Inform the Marine Corps Sub-registry and NCIS field office:

2. All investigations shall be forwarded to the Marine Corps Sub-registry:

COMMANDANT OF THE MARINE CORPS (PS)
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000
(703) 614-9464
(703) 692-4239

APR 24 2019

POLICY LETTER 3-19Levels and Processing of NATO Information

NATO Information is information that has been generated by or for NATO, or member nation national information that has been released into the NATO security system.

a. Levels and Protocols

LEVEL	UNAUTHORIZED DISCLOSURE	ACCOUNTING	STORAGE (NATO Control Point or Approved User Office Only)	DESTROY
* COSMIC Top Secret	Would cause exception-ally grave damage to NATO (COSMIC is applied to TS material to signify belonging to NATO)	Not Applicable/Not Authorized	Not Authorized	Not Authorized
NATO Secret	Would cause serious damage to NATO	Receipts, logs WILL be maintained on receipt, disposition, destruction and dispatch.	GSA Approved Safe / Separate from other Classified Material	Yes (Copy of destruction report to CMC (PS))
NATO Confidential	Would be damaging to NATO interests	Maintain Admin Control adequate to preclude unauthorized access. Specific accounting records are only required if specified by originator.	Same as NATO Secret	Same as NATO Secret
NATO Restricted	Would be disadvantageous to NATO interests - Maintained similar to FOUO, Official Use Only, Sensitive, but is UNCLAS - Unlike the aforementioned it is a Security Classification.	Same as NATO Confidential - May be maintained in a locked file cabinet as long as access is controlled.	Same as NATO Secret	Same as NATO Secret
NATO Unclassified	Access to info by non-NATO entities is permitted when such access would not be detrimental to NATO	Same as NATO Confidential	Same as NATO Secret	Same as NATO Secret

(*) Denotes not authorized currently for the II MEF CE

b. Protection. The protection of this information is controlled under NATO security regulations and the holder determines access within NATO, unless the originator specifies restrictions at the time of release to NATO.

c. Categories. All categories of NATO classified material are equivalent to the same classification of U.S. material and shall be afforded the same level of protection.

d. Access. Access and Investigative Requirements. Access to NATO information requires favorable eligibility and the Need-to-Know (not position, rank or level of clearance) at the same level as for access to U.S. classified NSI. As stipulated in DODD 5100.55, access to NATO classified NSI shall also require a supervisor's determination of the individual's Need-to-Know and possession of the requisite security clearance.

APR 24 2019

POLICY LETTER 3-19

Processing of NATO Information (Cont'd)

e. Briefing/Re-briefing/Debriefing. Personnel authorized access to NATO classified NSI shall receive the appropriate briefing, re-briefing, and debriefing as prescribed by DODD 5100.55 and MCO 5510.18B. The completion of this briefing, re-briefing, and debriefing must be recorded and this record retained for one (1) year following the individual's transfer or reassignment.

(1) Briefing. All personnel requiring access to NATO Classified Information based on a Need-to-Know shall receive a security briefing and a signed acknowledgment certificate. Receipt of the NATO briefing shall be verified prior to granting access to NATO classified NSI. The original statement shall be retained within the Control Point or security office of the authorizing command and access annotated in JPAS.

(2) ATOMAL Briefing. Personnel to whom ATOMAL access is to be granted, and those who require continued access, shall receive an initial briefing and annual re-briefing to remind them of their responsibilities and the special concerns for ATOMAL information.

(a) Access to ATOMAL information shall be authorized by the Marine Corps Sub-registry, or NATO ATOMAL Control Point.

(b) The individual must receive the ATOMAL security briefing and complete a statement acknowledging receipt of the briefing. The acknowledgement is available at:

<https://securecac.hqda.pentagon.mil/cusr/>. This access shall be annotated in JPAS.

(3) Need-to-Know. IAW reference DODD 5100.55, to facilitate potential access to NATO classified NSI, all personnel that require access to classified NSI and DO NOT have a Need-to-Know to access NATO Classified Information shall be briefed on their responsibilities for protection of NATO information.

(a) A written acknowledgement of the individual's receipt of the NATO briefing and responsibilities for safeguarding NATO classified NSI shall be maintained.

(b) Do not annotate the NATO briefing under this circumstance in JPAS.

(4) Re-briefing. Persons who require continued access to ATOMAL COSMIC, ATOMAL SECRET, and ATOMAL CONFIDENTIAL information must be re-briefed annually to remind them of their responsibilities and the special concerns for ATOMAL information. Record the annual re-briefing on the original briefing certificate. If the original briefing statement is not available, a new statement acknowledging receipt of the re-briefing shall be signed.

(5) Debriefing. All persons having access to NATO or ATOMAL information shall be debriefed when access is no longer required. A termination briefing shall remind personnel regarding responsibilities for continued safeguarding of whatever NATO and/or ATOMAL classified NSI to which

APR 24 2019

POLICY LETTER 3-19Processing of NATO Information (Cont'd)

they may have had access. The debriefing statement must be retained for one (1) year.

f. Control and Handling. The Marine Corps Sub-registry is responsible for the receipt, accounting, handling, and distribution of accountable information. NATO control points may assign local control numbers or use Marine Corps control numbers for tracking of a document during inventories and the bi-annual NATO inventory as required by DODD 5100.55.

g. Storage. NATO classified material shall be protected and stored IAW reference DODD 5100.55. NATO classified material, if filed in the same container as U.S. classified material, shall be filed separately. (Co-mingling of information/material is NOT allowed).

h. Reproduction and Extracts. Reproduction of NATO classified material, regardless of the classification, is prohibited without approval from the Marine Corps Sub-registry or originating Control Point. Marine Corps classified material containing extracted NATO classified NSI shall be marked, handled and declassified IAW references DOD Manual 5200.01 and DODD 5100.55.

i. Transportation and Transmission. The Marine Corps Sub-registry or control points are the only offices authorized to send NATO classified material directly to individuals and/or activities outside the Marine Corps.

(1) Authority to hand-carry any NATO classified material must be IAW DODD 5100.55.

(2) A NATO courier certificate must be used when hand-carrying NATO classified NSI. An example may be found at the CUSR NIPRNET website:

<https://securecac.hqda.pentagon.mil/cusr/>. The SIPRNET website is <http://classweb.hqda-s.army.smil.mil/cusr>

j. Electronic Mail (E-Mail). NATO classified NSI may be e-mailed within a local area network (LAN) or between LANs that are accredited to process NATO classified NSI IAW DODD 5100.55. It is the sender's responsibility to verify that the receiver is cleared for access to NATO classified NSI and has a Need-to-Know.

k. Destruction. All NATO Control Points shall annually review their NATO classified NSI to determine whether it may be destroyed. NATO material classified NATO Secret ATOMAL and above shall be destroyed only by the Marine Corps Sub-registry.

(1) NATO classified NSI shall be destroyed using the same methods as U.S. classified NSI and IAW DODD 5100.55.

(2) NATO Control Points shall be authorized to destroy NATO Secret and below information. All destruction certificates must be witnessed by two persons appropriately cleared to the level of information to be destroyed. Destruction certificates shall be forwarded to the Marine Corps Sub-registry.

APR 24 2019POLICY LETTER 3-19

Destruction certificates for CTS ATOMAL and NATO Secret ATOMAL shall be maintained at the control points for 10 years.

II MEF NATO Inventory Form

[illegible]

APR 24 2019

POLICY LETTER 3-19II MEF Brief/Rebrief/Debrief Certificate**SECTION A - GENERAL**

1. NAME: _____
2. DUTY POSITION: _____ 3. PHONE NUMBER: _____
4. ORGANIZATION: _____ 5. ADDRESS: _____

SECTION B - BRIEFING

6. I certify that I have (read and been granted access to) (been briefed) and fully understand the procedures for handling (COSMIC) (ATOMAL) (NATO SECRET) (NATO CONFIDENTIAL) material and am aware of my responsibilities for safeguarding such information, and that I am liable to prosecution under Sections 793 and 794 of Title 18, U.S.C., if either by intent or negligence I allow it to pass into unauthorized hands.

7. SIGNATURE OF INDIVIDUAL: _____ DATE: _____
8. SIGNATURE OF BRIEFER: _____ DATE: _____

SECTION C - ATOMAL REBRIEFING

9. I certify that I have been briefed and fully understand the procedures for handling ATOMAL material and am aware of my responsibility to safeguard such.

SIGNATURE DATE

SIGNATURE DATE

SECTION D - DEBRIEFING

10. I have been debriefed for (COSMIC) (ATOMAL) (NATO SECRET) (NATO CONFIDENTIAL) and I understand that I must not disclose any classified information which I have obtained in my assignment to this organization or in connection therewith. I also understand that I must not make any such classified information available to the public or to any person not lawfully entitled to that information. I further understand that any unauthorized disclosure of such classified information, whether public or private, intentional or unintentional, will subject me to prosecution under applicable laws.

- SIGNATURE OF INDIVIDUAL: _____ DATE: _____
- SIGNATURE OF CONTROL OFFICER: _____ DATE: _____