DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

IN REPLY REFER TO:
5510
ARS
APR 10 2015

Security Note 02-15

From: Director, Administration and Resource Management Division

Subj: POLICY FOR HANDLING AND SAFEGUARDING NORTH ATLANTIC TREATY ORGANIZATION (NATO) MATERIAL

Ref: (a) DoDM 5200.01
(b) USSAN 01-07
(c) MCO 5510.17 W/CH 1, 2

Encl: (1) NATO Security Briefing Forward
(2) NATO Briefing/Re-briefing/De-briefing Certificate
(3) NATO Briefing and De-briefing for Access to SIPRnet computers
(4) NATO Classified Material Control Form & Destruction Report
(5) DD Form 2881 label

1. Per the references, this Security Note is published to amplify the handling and safeguarding procedures of North Atlantic Treaty Organization (NATO) material.

2. Background. Per reference (b), the purpose of the NATO Sub-registry System is to implement the NATO Program within the USMC for receipt, retention, storage, release and sharing of classified NATO information. Security Programs and Information Management Branch (ARS), maintains the Headquarters Marine Corps (HQMC) NATO Control Point under the authority of the Marine Corps NATO Sub-registry. The HQMC Assistant Security Manager is the HQMC NATO Control Officer and is responsible for the oversight and management of the NATO Program within HQMC.

3. NATO Classification Levels. NATO has five classifications: COSMIC TOP SECRET, NATO SECRET, NATO CONFIDENTIAL, and NATO RESTRICTED. ATOMAL is a special caveat that may be found at any classification level and is used to identify NATO information that is in conjunction with U.S. RESTRICTED DATA (RD) or FORMERLY RESTRICTED DATA (FRD) pursuant to the Atomic Energy Act of 1954, as amended, provided it has been officially released to NATO. NATO also distinguishes unclassified information using the classification NATO UNCLASSIFIED.

4. Access. NATO Access shall be limited to those personnel who have a need-to-know for official purposes, hold a final U.S. security clearance at the equivalent level (e.g., Cosmic Top Secret requires Final U.S. Top Secret), have been briefed specifically for NATO Access, and acknowledge their understanding of NATO security requirements. A briefing and the need-

to-know for official purposes also applies for access to NATO Unclassified and NATO Restricted information.

a. Security Coordinators shall ensure personnel possess a final U.S. security clearance prior to requesting access. Interim Access is not authorized for access to NATO material. All requests for access will be submitted to the HQMC Security Manager for approval.

b. Access to Atomal information is administered by the HQMC NATO Control Point. Atomal Access requires personnel to have a need-to-know for official purposes, the appropriate final U.S. security clearance, and brief specific to the granting of Atomal Access.

c. Security Coordinators will maintain a current access roster, listing personnel who are authorized access to NATO material and the level of access to which they are authorized.

5. Briefing/Re-briefing/Debriefing. Per reference (a), personnel who are briefed on their responsibilities for protecting U.S. classified information, shall be briefed simultaneously on the requirements for protecting NATO classified information using enclosure (1). A written acknowledgement of the individual's receipt of the NATO briefing and responsibilities for safeguarding NATO classified information shall be maintained via enclosure (2). The NATO brief is not an automatic granting of access to NATO information but rather is designed to ensure the proper handling of NATO information in cases of inadvertent disclosure.

a. Security Coordinators must provide enclosure (2) to HQMC Security Manager when requesting access to NATO classified information. Receipt of the NATO briefing will be verified prior to granting access to NATO classified information.

b. Personnel requiring Atomal access and those who require continued access will receive an initial briefing and annual re-briefing by the HQMC NATO Control Point.

c. Personnel requiring a SIPRnet Account, will complete the NATO Briefing for Access to SIPRnet via enclosure (3).

d. Personnel no longer requiring access to NATO, Atomal or SIPRnet information shall be debriefed appropriately. This may be accomplished on the debriefing section of enclosures (2) and (3).

e. Security Coordinators will conduct briefings and debriefings as required and will retain for 2 years following the individual's transfer or reassignment.

6. Safeguarding. The HQMC NATO Control Point is responsible for the receipt, accounting, handling, and distribution of accountable NATO

information. HQMC NATO Control Point will assign local control numbers for tracking of the NATO material during dissemination, inventory, and the biannual NATO inventory.

a. HQMC NATO Control Point is the only office authorized to send NATO classified material directly to individuals and/or activities within or external of HQMC. NATO documents will be distributed to users on a day-to-day basis, and will be returned to the NATO Control Point by close of business each day. Release/Receipt of NATO material will always be accompanied by enclosure (4). NATO material must not be addressed to a specific person or title. All incoming and outgoing delivery of NATO material will be completed via the HQMC NATO Control Point located at:

3000 Marine Corps Pentagon
Room 2A288A
Washington, DC 20350-3000

b. Material received by a Staff Agency/Activity from any source other than the HQMC NATO Control Point must immediately be added to the Control Point NATO inventory.

c. NATO classified material will be stored in containers approved for the storage of equivalent U.S. material, ensuring there are no markings of any kind that would identify the contents of the material. NATO material may be stored in the same container but must be filed separately from U.S. material. Atomal information must be stored separately from non-Atomal information (no comingling of information is allowed). Storage container combinations must be changed under the following circumstances; annually, when an individual with the access combination departs, or anytime a suspected compromise occurs.

d. Staff Agencies/Activities will maintain an Access Roster that identify those persons authorized to access NATO material in the performance of their duties, signed by the Staff Agency/Activity Deputy Commandant/Director or By direction Authority. Access Roster will be posted on the interior wall of a designated space adjacent to the main entry point and will not be visible from the exterior. Staff Agencies/Activities will also maintain a roster of classified NATO holdings, located with the actual material.

7. Handling. The requirements, responsibilities and procedures to safely transmit, reproduce and mark NATO classified information are described below:

a. Reproduction of NATO material regardless of the classification is NOT authorized. The HQMC NATO Control Point may reproduce NATO material. Requests for additional copies should be made to the HQMC NATO Control Point.

b. Classified material containing NATO information will be marked, handled and declassified in accordance with the references. NATO classified

messages will be handled in the same manner as NATO material of the same classification, in accordance with the references. Prior to any disclosure, all NATO information must go through the HQMC NATO Control Point to ensure proper record and continuous receipts are maintained.

c. Marking of NATO material must be accomplished in accordance with the references. Training is available through the derivative classification training and further instructions can be provided by the HQMC NATO Control Point.

d. Authority to hand-carry any NATO classified material within the NCR, CONUS and OCONUS, must be approved by the HQMC NATO Control Point. A continuous chain of receipts is required to record the movement of all NATO material.

e. Destruction of NATO classified material is NOT authorized. NATO classified information will be destroyed only by the HQMC NATO Control Point. All destruction certificates will be afforded Two-Person Integrity (TPI) by appropriately cleared personnel, at the same level of the information to be destroyed. Enclosure (4) will be utilized to document destruction and will be forwarded to the Marine Corps Sub-registry. Destruction certificates will be maintained on file at the HQMC Control Point 5 years for NATO Secret and 10 years for Cosmic Top Secret and Atomal.

f. NATO Restricted is to be treated as U.S. For Official Use Only (FOUO) or Controlled Unclassified Information (CUI) with the exception of storage. NATO Restricted must be stored in a manner that would prevent unauthorized disclosure but is not held to the same requirements as NATO Secret or NATO Cosmic Top Secret.

g. NATO classified emails sent via SIPRnet must be properly marked and stored (when printed) under the same guidelines as other NATO classified documents. All classified equipment authorized to process classified information (i.e. desktops, laptops and servers) that may process NATO Secret information must be labeled, using enclosure (5). NATO Restricted is not authorized for transmission over the NIPRnet.

8. Compromise. Compromise includes disclosure or risk of disclosure to unauthorized individuals and physical loss or risk of loss of NATO material.

a. All suspected or possible compromises involving NATO classified information will be reported immediately to the HQMC Security Manager, NATO Control Point, and local NCIS field office (if required). The Marine Corps Sub-registry will be notified within 24 hours of the suspected compromise of NATO classified information.

b. To determine whether a compromise occurred, a Security Inquiry will be conducted in the same manner as U.S. classified, ensuring NATO

requirements are met (i.e., NATO brief, Final U.S. Clearance). All Security Inquiries will be forwarded to the Marine Corps Sub-registry.

9. Questions regarding this Security Note should be directed to the HQMC NATO Control Point at (703) 614-3609.

10. This note Supersedes enclosure (5) section (d), of the HQMC Information and Personnel Security Program Standard Operating Procedures of 06 August 2013.

M. M. OLIVER, JR.
By direction

NATO SECURITY BRIEFING FOREWORD

This sample security briefing contains the minimum elements of information that must be provided to individuals upon initial indoctrination for access to NATO classified information.

This briefing is intentionally general so it may be used by all U.S. Government agencies and contractors. Agencies and contractors are encouraged to expand upon this briefing to accommodate specific situations. There is no requirement to copy this format or literary style; however, the minimum elements contained herein shall be included. Detailed procedures are contained in United States National Security Authority for NATO (USSAN) Instruction 1-07, NATO's C-M(2002) 49 "Security within The North Atlantic Treaty Organization" and its Supporting Security Directives (AC/35-D/2000 through D/2005), and the National Industrial Security Program Operating Manual (NISPOM) DoD 5220.22-M.

NATO/ATOMAL SECURITY BRIEFING

INTRODUCTION

You will require access to NATO classified information in pursuance of your current duties. The security standards and procedures for handling and protecting NATO information are in some cases different than those for U.S. information. This briefing explains the basic security standards and procedures for safeguarding NATO information.

WHAT IS NATO?

NATO is an acronym for the North Atlantic Treaty Organization. Member nations have signed the North Atlantic Treaty and the NATO Security Agreement, which obligate them to comply with NATO rules. The following nations* are members of NATO:

Belgium	Hungary	Portugal	Turkey	Bulgaria	Slovenia
Canada	Italy	United Kingdom	Norway	Estonia	Albania
Luxemburg	Iceland	Czech Republic	Latvia	Croatia	Spain
Germany	Netherlands	United States	France	Lithuania	Greece
Poland	Denmark	Romania	Slovakia		

The Secretary of Defense is the United States National Security Authority for NATO. As such, he is responsible for ensuring that NATO security requirements are implemented throughout the Executive Branch of the United States Government.

WHAT IS 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. The protection of this information is controlled under the NATO security regulations, and access within NATO is determined by the holder, unless restrictions are specified by the originator at the time of release to NATO.

Material received by an agency direct from another NATO member nation may contain either NATO information generated by a NATO element or national information generated by a NATO member nation. If it has been marked "NATO"

by the originating nation, it must be assumed to contain information released to NATO, and it is controlled under the NATO Security Program. If the material has a national classification marking and is not marked "NATO" by the originator, DO NOT apply a NATO marking unless you are informed in writing by the originator that the material is intended for NATO and is to be protected under the NATO Security Program. Moreover, the material or the information therein shall not be released into the NATO system without the prior written consent of the originator.

"RELEASABLE TO NATO" statements on U.S. material indicate that the information contained therein has been authorized under applicable disclosure policies for release to NATO and may be discussed within the NATO community. ONLY the copies that are being released to NATO shall be marked with a NATO marking. They are to be dispatched and controlled in the NATO registry system or in accordance with guidance provided by the supporting sub registry or control point. The remaining copies shall continue to be controlled as U.S. information. There must be a record, however, that the information has been authorized for release to NATO.

CLASSIFICATION MARKINGS AND CATEGORIES OF NATO INFORMATION

NATO has four levels of classified information: COSMIC TOP SECRET, NATO SECRET, NATO CONFIDENTIAL, and NATO RESTRICTED.

Certain NATO information is further classified in a specific category as ATOMAL which can be either RESTRICTED DATA (RD) or FORMERLY RESTRICRED DATA (FRD). NATO also distinguishes official, unclassified information. The markings and categories of NATO information are described below.

COSMIC TOP SECRET (CTS) - This security classification is applied to information the unauthorized disclosure of which would cause exceptionally grave damage to NATO. (NOTE: The marking "COSMIC" is applied to TOP SECRET material to signify that it is the property of NATO. The term "NATO TOP SECRET" is not used.)

NATO SECRET (NS) - This security classification is applied to information the unauthorized disclosure of which would cause serious damage to NATO.

NATO CONFIDENTIAL (NC) - This security classification is applied to information the unauthorized disclosure of which would be damaging to the interests of NATO.

NATO RESTRICTED (NR) - This security classification is applied to information the unauthorized disclosure of which would be disadvantageous to the interests of NATO. (NOTE: Although the security safeguards for NATO RESTRICTED material are similar to FOR OFFICIAL USE ONLY information, "NATO RESTRICTED" is a security classification and MUST be sent via classified means.)

ATOMAL - ATOMAL information can be either U.S. Restricted Data or Formerly Restricted Data that is classified pursuant to the Atomic Energy Act of 1954, as amended, or United Kingdom ATOMIC information that has been officially released to NATO. ATOMAL information is marked either COSMIC TOP SECRET ATOMAL (CTSA), NATO SECRET ATOMAL (NSA), or NATO CONFIDENTIAL ATOMAL (NCA).

NATO UNCLASSIFIED (NU) - This marking is applied to official information that is the property of NATO, but does not meet the criteria for classification. Access to the information by non-NATO entities is permitted when such access would not be detrimental to NATO.

In this regard, it is similar to U.S. Government official information that must be reviewed prior to public release. (As of mid-2002, NATO has required its classified information to be portion-marked, i.e. with a classification marking applied to each paragraph heading, etc.)

ACCESS AUTHORIZATION

NATO Classified Information. Your security official will inform you of your level of access to NATO classified material and whether you are authorized access to ATOMAL information (see below). Additionally, your agency should maintain a list indicating the levels of access for each assigned individual who is authorized access to NATO information for you to verify NATO access authorizations for other employees. As with U.S. information, access is NOT based on duty position, rank, or level of clearance. Access is based on need-to-know, the proper level of U.S. clearance, and an access briefing for a specific level and type of NATO/ATOMAL information. Remember, IT IS YOUR RESPONSIBILITY to ensure that an individual is authorized access to a particular type and level of classified NATO or/and ATOMAL information BEFORE you provide access. This responsibility applies to all modes of transmission, e.g., oral, written, visual and electronic. If in doubt, seek assistance from your security officer or NATO sub registry or control point. NATO information is provided to non-NATO nationals and entities only with the approval of the originator of the information. That approval is gained through the appropriate NATO committee.

ATOMAL Information. An employee of the Department of Defense or its contractors may be granted access to ATOMAL information only if the employee has a need-to-know to perform his or her job and has been appropriately cleared and briefed for access to Restricted Data. An employee of NASA may be granted access to ATOMAL information concerning aeronautical and space activities, if the individual is cleared for access to Restricted Data. All other individuals, and NASA employees requiring access to ATOMAL information other than that covering aeronautical and space matters, shall have a "Q" clearance issued by the Department of Energy. Interim clearances shall not be accepted as the basis for access to ATOMAL information.

THE REGISTRY SYSTEM

A Central Registry has been established by each NATO member nation to ensure proper control and accountability of NATO classified documents. The Central United States Registry (CUSR) is located in Arlington, Virginia.
As an official representative of the U.S. Security Authority for NATO, the CUSR oversees the administration of the U.S. registry system. The CUSR establishes all U.S. sub-registries to execute the accountability and security management of NATO and ATOMAL material at various U.S. locations throughout the world. Based on location and volume of material, control points may be established to assist in these operations.

ACCOUNTING FOR NATO CLASSIFIED MATERIAL

COSMIC TOP SECRET, NATO SECRET, and all ATOMAL. Receipts and logs shall be maintained on the receipt, disposition, destruction, and dispatch of COSMIC

TOP SECRET, NATO SECRET, and all ATOMAL material. In addition, each individual is required to execute a disclosure record upon acquiring access to each item of CTS/CTSA material, or ATOMAL with special limitation restrictions.

NATO CONFIDENTIAL and NATO RESTRICTED. You are required to maintain administrative control of NATO CONFIDENTIAL and NATO RESTRICTED material adequate to preclude unauthorized access. Specific accounting records are not necessary unless they are required by the originator.

MARKING AND ACCOUNTING FOR U.S. DOCUMENTS CONTAINING NATO CLASSIFIED INFORMATION

A newly generated U.S. classified document that contains NATO classified information shall bear a U.S. classification marking that reflects the highest level of NATO or U.S. classified information it contains. Declassification and downgrading instructions shall indicate that the NATO information is exempt from downgrading or declassification without the prior consent of NATO; the reason to be cited is"foreign government information." The statement "THIS DOCUMENT CONTAINS NATO CLASSIFIED INFORMATION" will be affixed to the front cover or first page, if there is no cover. Portions that contain NATO classified information shall be marked to identify the information (e.g., NS). The document shall be accounted for, safeguarded and controlled as specified for NATO documents of the same classification.

If a record is required for the NATO classification information, a U.S. document containing the NATO information will be logged, accounted for and handled in the same manner as required for the NATO information. However, NATO reference numbers are not required.
A record shall be maintained of source NATO documents, as required for derivatively classified U.S. documents. Existing U.S. documents that do not meet this requirement shall be marked and handled according to these procedures when they are removed from the files for use.

AIS storage media shall be handled as described in C-M (2002)49 and its Supporting Directives and the USSAN 1-07, Para. 7.11, 1-2).

SAFEGUARDING NATO MATERIAL

General. The physical security requirements for material marked NATO CONFIDENTIAL and above are the same as for U.S. material of the same level of classification. NATO RESTRICTED material may be stored in a locked filing cabinet, book case, desk or other such container or in a room or building that is locked during non-duty hours, provided access to the room or building is controlled so that only authorized personnel can gain access to the information. All personnel with access to a security container that is used to store NATO information must be briefed and authorized access to the level and type of NATO information that is stored in that container.

Segregation. You are required to ensure that NATO and non-NATO material are filed separately. ATOMAL material must be filed separately from non-ATOMAL material. This may be accomplished by using a separate security container or, to conserve storage space, by using separate drawers or file dividers in the same security container holding U.S. classified material. Additionally, you are required to segregate ATOMAL control records from non-ATOMAL control records.

Combinations. Combinations to security containers containing NATO classified material must be changed at least annually, upon departure of an individual with access to the combination, or if the combination has been or is suspected of having been compromised.

Transmission. The national or international transmission of CTS and CTSA material shall be through the registry system using a cleared government courier service; for example, diplomatic pouch or military courier service. The national and international_transmission of NS, NSA, NC, and NCA shall be by cleared courier, or by appropriately cleared and briefed employees who possess courier identification and authorization, or by U.S. registered mail using the same provisions as prescribed for U.S. classified material. Receipts are required for CTS, NS and all ATOMAL material. NC may also be sent by U.S. First Class mail between U.S. Government activities within the United States. In urgent situations, the United States Postal Service Express Mail may be used to transmit material NS and below within the United States, its Territories, and the District of Columbia. However, there are restrictions on the use of Express Mail; guidance should be sought from your security officer or sub registry or control point. NR material may be sent by U.S. First Class mail within the United States and to an APO/FPO or NATO address through the U.S. or NATO member nation postal service.

Automated Information Systems (AIS). Systems must be accredited specifically to handle NATO classified information. Organizations with AIS systems accredited for handling NATO classified information must issue instructions for processing, handling and accounting for NATO classified information. Be sure you receive a copy of those instructions and apply them.

Destruction. The destruction of CTS, CTSA, NS, NSA, and NCA material will be accomplished only by registry system personnel using a destruction certificate and a method approved for the destruction of U.S. material of the same level of classification. NATO RESTRICTED and NATO CONFIDENTIAL shall be destroyed by any means authorized for U.S. CONFIDENTIAL material.

Reproduction. COSMIC documents shall be reproduced by the Central US Registry and COSMIC Sub-registries which must report the number of copies made to the CUSR. Reproduction of ATOMAL (CTSA, NSA and NCA) shall be made only by the CUSR, ATOMAL Sub-registries and ATOMAL Control Points. Reproduction of NATO Secret and below may be produced by the addressee under strict need-to-know principle and provided that the originator has not restricted reproduction. Reproduced copies shall be accounted for and safeguarded in the same manner as the original.

SECURITY VIOLATIONS AND POSSIBLE LOSS/COMPROMISE OF NATO CLASSIFIED MATERIAL

General. NATO guidelines are very similar to those used for U.S. material. However, the servicing sub registry or control point must be informed of the incident, in addition to the responsible security or counterintelligence officials.

Procedures. If you find NATO material unsecured and unattended notify your security officer or registry system official immediately. Stay with the material and wait for the security officer or registry official to arrive. Do not disturb the area or material. Do not allow anyone else to disturb the area or allow unauthorized personnel to have access to the material.

If it is necessary that you leave the area before your security officer or registry system official can assume custody, place the material in a security container and lock the container. If the container is already locked, and you are not authorized access, or there is no container, take the material directly to an appropriately cleared security or registry system official, explain the circumstances, and obtain a receipt for the material.

Espionage, Sabotage, Terrorism, and Deliberate Compromise. Information concerning a deliberate compromise of NATO/ATOMAL material, attempted or actual espionage directed against NATO/ATOMAL information, or actual or planned terrorist or sabotage activity against facilities or users of NATO classified material shall be reported promptly to your security officer or to your agency's counterintelligence officer or the Federal Bureau of Investigation. The following are typical reportable situations:

1. Attempts by unauthorized persons to obtain classified information concerning NATO or U.S. facilities, activities, personnel, or material through questioning, elicitation, bribery, threats, or coercion, either by direct or indirect contacts or correspondence.

2. Attempts by unauthorized persons to obtain classified information through photographing, wiretapping, eavesdropping, observation, or by any other means.

3. Attempts by persons with known, suspected, or possible foreign intelligence backgrounds, associations, or activities to establish a friendship or a social or business relationship, or to place you under obligation through special treatment, favors, gifts, money, or other means.

3. Information concerning terrorist plans and activities posing a direct threat to U.S. or NATO facilities, activities, personnel or material.

4. Known or suspected acts or plots to harm or destroy U.S. or NATO property by sabotage.

Anyone with access to NATO classified information could be a potential target. If you become aware of activities such as those as described above, or someone approaches you directly to engage in such activities, remember the following:

1. STAY CALM. You are not at fault because they chose to target you.

2. BE NONCOMMITTAL. Be ambiguous as to whether or not you will provide them with material or information.

3. REPORT IT PROMPTLY. Even if it seems purely coincidental or insignificant, a small detail may be the key to identifying and countering espionage or sabotage or a terrorist act. Do not discuss the incident with friends, family, co-workers, etc., unless directed to by your security officer or counterintelligence representative.

4. IT IS NEVER TOO LATE! If you have provided material or information to an unauthorized recipient, REPORT IT.

FOREIGN TRAVEL

Your personal travel will not be limited based solely on the fact that you have access to NATO classified information. There are, however, risks involved in travel to certain countries. Check with your security officer for advice and assistance. If you choose to travel to high-risk countries, you are required to coordinate with your leave/travel order granting authority and security office and obtain a travel security briefing. Upon your return, you should report any incident that may have been an attempt to collect sensitive information.

WHERE DO I GO FOR MORE HELP?

If problems or specific questions arise concerning NATO classified information, your security officer and sub registry/control point can assist you. Further information is also available to users in .mil and .gov domains on the Central U.S. Registry website.

NIPRNET website is https://secureweb.hqda.pentagon.mil/cusr

BRIEFING/REBRIEFING/DEBRIEFING 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 AND DATE SIGNATURE AND 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: _____

Last Revised [illegible]

APPENDIX A: NATO BRIEFING and DEBRIEFING FOR ACCESS TO SIPRNET COMPUTERS

SECTION 1 – GENERAL INFORMATION

NAME: _____

(LAST, FIRST, MI)

DUTY POSITION: _____ **PHONE NUMBER:** _____

ORGANIZATION: _____

E-MAIL ADDRESS: _____

SECTION II - BRIEFING

I understand that I am authorized use of SIPRNet computers but I am not authorized to print or otherwise handle NATO classified material without prior authorization. I also understand that violation of this will subject me to prosecution under applicable laws and regulations.

SIGNATURE OF INDIVIDUAL: _____
DATE: _____

SIGNATURE OF SECURITY MANAGER: _____
DATE: _____

SECTION III – DEBRIFING

I have been debriefed from this organization and no longer require use of SIPRNet computers. I certify that I have not printed or handled any NATO classified material without prior authorization. I understand that I must not disclose any other classified information that 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 SECURITY MANAGER: _____
DATE: _____

NATO CLASSIFIED MATERIAL CONTROL FORM & DESTRUCTION REPORT

(A SEPARATE SHEET AND CONTROL NUMBER SHOULD BE ISSUED FOR EACH INDIVIDUAL DOCUMENT OR COPY THEREOF)

CONTROL NUMBER:	CLASSIFICATION OF THIS SHEET, ONLY:	CLASSIFICATION OF ATTACHED MATERIAL:
	UNCLASSIFIED	

ORIGINATOR:	DATE of DOCUMENT:	NUMBER OF COPIES RECEIVED:
TO:	DATE DOCUMENT RECEIVED:	COPY NUMBER:

SUBJECT or TITLE (WARNING: ENTRY OF CLASSIFIED SUBJECT OR TITLE WILL REQUIRE CLASSIFICATION OF THIS FORM AND ALL TITLES):	ENCLOSURES RECEIVED:

RECORD OF CUSTODY

TO (PRINTED NAME)	RANK	INITIALS	DATE OUT	SIGNATURE	RETURN DATE
		I've been briefed and understand my responsibilities in the protection of this material_____			Rcvd by CP:
		I've been briefed and understand my responsibilities in the protection of this material_____			Rcvd by CP:
		I've been briefed and understand my responsibilities in the protection of this material_____			Rcvd by CP:
		I've been briefed and understand my responsibilities in the protection of this material_____			Rcvd by CP:
		I've been briefed and understand my responsibilities in the protection of this material_____			Rcvd by CP:
		I've been briefed and understand my responsibilities in the protection of this material_____			Rcvd by CP:
		I've been briefed and understand my responsibilities in the protection of this material_____			Rcvd by CP:

Note: When the above lines are filled, generate a new form with identical header information and attach to original form, keeping both forms together for the life of the material and associated documentation.

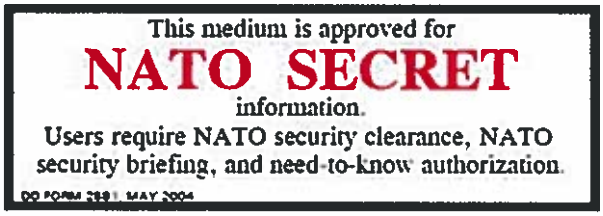
REMARKS :

DESTRUCTION REPORT: The classified material described above has been destroyed in accordance with regulations established by the U.S. Security Authority for NATO Affairs (USSAN) 1-69, 21 April 1982, subject: U.S. Implementation of NATO Security Procedures. This form may be used to provide activities with a record of destruction of classified material. Also, copies may be utilized for reports to activities originating material, where such reports are necessary.

OFFICER or INDIVIDUAL AUTHORIZING DESTRUCTION *(Signature, Printed name, Rate, Grade, Title)*	Date of Destruction:	TOTAL # of PAGES:

WITNESSING OFFICIAL *(Signature)*	WITNESSING OFFICIAL *(Signature)*
WITNESSING OFFICIAL *(Printed name, grade, position)*	WITNESSING OFFICIAL *(Printed name, grade, position)*

NOTE: Reproduction of NATO material regardless of the classification is **NOT** authorized. Requests for additional copies must be completed through the HQMC NATO Control Point.


This medium is approved for
NATO SECRET
information.
Users require NATO security clearance, NATO
security briefing, and need-to-know authorization.