

U.S. Department of Transportation

DOT 1642.2/MAO 280-4

Maritime Administration

February 25, 2014

Subject: NORTH ATLANTIC TREAT ORGANIZATION (NATO) PROGRAM

Section 1. Purpose:

This Order establishes uniform policies and procedures for effective and efficient management and control of NATO material. It implements all applicable laws, Executive Orders, and regulations pertaining to NATO within the U.S. Department of Transportation (DOT).

Section 2. Background:

The Department of Defense (DOD), the Executive Agent for NATO issued United States Security Authority for North Atlantic Treaty Organization Affairs (USSAN) Instruction 1-07, Implementation of North Atlantic Treaty Organization Security Requirements, which applies to all Executive Branch agencies. This Order implements the policy and procedures set forth in USSAN Instruction 1-07.

Section 3. Scope:

This Order applies to all DOT Secretarial Offices and Operating Administrations (OAs) that receive, store, process, generate, discuss, or otherwise handle NATO material or have the potential of handling NATO material.

Section 4. References:

- a. Executive Order 13526 Classified National Security Information
- b. 32 CFR Part 2001 Classified National Security Information (CSNI)
- c. NATO's C-M (2002) 49 "Security within the North Atlantic Treaty Organization"
- d. USSAN Instruction 1-07 Implementation of North Atlantic Treaty Organization Security Requirements
- e. DoDD 5100.55 United States Security Authority for North Atlantic Treaty Organization Affairs (USSAN)
- f. Department of Transportation Order 1640.4E Classified National Security Information

## Section 5. Definitions:

5.01 The Central United States Registry (CUSR) is the Department of Defense Registry for management of NATO information. The CUSR is the only organization authorized to permanently store NATO information. The CUSR grants accreditations of networks and approves command Sub-Registries.

5.02 The Sub-Registry is a subordinate depository under the administrative control and management of the CUSR and serves as the single point responsible for the overall management of the DOT's NATO Program. The Sub-Registry function is performed in the Office of Management and Administrative Service (MAR 390) by the MARAD Security Officer.

5.03 Control Point is a subordinate depository under the administrative control and management of the Sub-Registry and serves as a focal point for management of NATO information and material in the respective activities. There are two Control Points under the DOT's Sub-Registry — one Control Point is organized under the Office of Emergency Preparedness (MAR 620) and the other Control Point is organized under the Director, Office of Intelligence, Security, and Emergency Response (OST S-60).

## Section 6. Policy:

### 6.01 General:

1. NATO information and material will be protected at the same level as U.S. Classified National Security Information but at an enhanced security level that provides compartmentalization.
2. Users of this Order shall refer concurrently to NATO regulations for guidance. In the event of a conflict between this Order and NATO security policy, NATO security policy takes precedence. Users must report conflicts to the Maritime Administration Security Officer (SO), MAR 390 at phone number 202-366-2808.

### 6.02 Access: Individuals will be granted access to NATO information and material once:

1. The individual completes initial NATO specific training to ensure a complete understanding of NATO requirements;
2. The individual is indoctrinated into NATO by signing the briefing/debriefing acknowledgement form (Appendix 1) and if;
3. The individual has a need to know, position requirement, justification, and appropriate security clearance.

6.03 Delivery: NATO information and material is transferred to the DOT via multi-delivery methods and it is departmental policy that only verified personnel that are indoctrinated in the NATO program will receive NATO information and material.

1. NATO delivery via hardcopy will be processed and received by the Control Point or the Sub-Registry and the following will be accomplished:
  - a. A receipt log will be established—DA Form 3964 will be used to record the receipt of the NATO document and material (Appendix 2).
  - b. If the document or material is received by a member of the Control Point activity, the Control Point will notify the Sub-Registry of receipt of the NATO document or material.
2. NATO delivery via soft copy on a verified, approved, and accredited computer system will be processed as follows:
  - a. NATO (soft copy) information will be processed on verified and accredited computer systems and only by indoctrinated personnel.
  - b. Individuals must establish a receipt log upon printing soft copy to hard copy—DA Form 3964 will be used for this process (Appendix 2) and the policy above for hard copy processing will be followed.
  - c. Non-indoctrinated personnel, who have access to specialized computer systems where NATO information is available will be briefed on the NATO program and required to sign an acknowledgement form (Appendix 1).

6.04 Handling and Protection: It is DOT policy to ensure that all NATO material is properly protected as required by applicable laws and regulations. These protection techniques include maintaining uniform procedures for handling, classification, declassification, destruction, marking, transmission, and processing.

1. Handling of NATO material will be accomplished only by personnel authorized for and indoctrinated into the NATO program.
2. NATO (actions) documents will be processed only on NATO accredited systems. The accreditation coverage must extend to the security classification level of the document being processed. For example, if the document being processed is NATO Secret the accreditation must be at least a Secret level.
3. Distribution/transmission of NATO material will be transferred to only verified personnel that are indoctrinated in the NATO program. The classified document accountability record—DA Form 3964 will be used to record the movement of the NATO document (Appendix 2).

- a. Hand carrying NATO material is unauthorized without approved courier orders.
  - b. System to system processing is the preferred method for NATO material distribution/transmission.
4. Reproduction of NATO material will only be processed on NATO approved copying or multi-functional machines that are extended to the security classification level of the document being reproduced. For example, if the document being reproduced is NATO Secret, then copying or multi-functional machines must be at least a Secret level.
5. Destruction of NATO material is accomplished under normal destruction Classified National Security Information standards as specified in DOT Order 1640.4E with the following additional requirements:
  - a. A classified document accountability record—DA Form 3964 must be used to record destruction of registry worthy documents (Appendix 2).
  - b. Maintain a copy of the destruction certificate (DA Form 3964) for 5 years.
6. Security incidents involving NATO information or material that may contribute to a possible loss, compromise, or unauthorized disclosure of classified information will be handled in the manner as specified in DOT Order 1640.4E with the following additions:
  - a. The Central Registry will be notified immediately when initiating an inquiry or investigation that may contribute to a possible loss, compromise, or unauthorized disclosure of classified information.
  - b. Maintain a copy of the Security Incident Report for 3 years.
7. Emergency Action Plans (EAP) for NATO material are based primarily on a LOW threat level consideration; therefore, this EAP is centered on natural disaster emergencies such as fire, flood, tornado, and earthquake. There are three courses of action to be considered in protecting NATO classified material:
  - a. Securing Material
    - (1) This is the routine procedure followed in storing the material after normal use and prior to departure from the area. Normal storage requires storage in an approved General Service Administration security container when not in use.
    - (2) Only grant access to cleared personnel as verified by the control official.
    - (3) Use only approved Automatic Information Systems devices for processing (e.g., copying, printing, and presenting).
    - (4) Use approved methods for destroying.

(5) Hand carrying of NATO material (outside the compound) is prohibited without approval of the Sub-Registry Security Officer.

(6) All conference and group discussion involving NATO material in the DOT compound must be approved by Sub-Registry Security Officer.

b. Evacuation of Material (and equipment)

(1) Cannot be considered as a viable solution for responding to emergency evacuation, due to the storage method (approved security container)—extreme weight and lack of transportation resources.

(2) Destruction of classified material is the only acceptable method for dealing with long term evacuations.

c. Destruction of Material: Any of the methods approved for routine destruction of classified national security information or material may be used for destruction under the provision of this EAP (32 CFR standards). There are two types of destruction—precautionary and emergency.

(1) Precautionary destruction is the destruction of classified material that is not essential to current operations. This destruction is utilized to reduce the size of the classified holdings so that complete destruction can be accomplished more rapidly if so ordered later.

(2) Emergency destruction is the complete destruction of all classified material. If destruction is impossible be sure that all classified material is properly secured in approved containers.

Section 7. Responsibilities:

7.01 The Assistant Secretary for Administration has designated the Maritime Administrator to serve as Executive Agent for management of NATO material in DOT.

7.02 The Maritime Administrator will:

1. Issue departmental policy for effective compliance with, and implementation of this Order, thereby ensuring DOT conformance with Federal regulations, laws, and policies concerning the protection of NATO material.
2. Represent the Secretary of Transportation at NATO committee meetings and provide DOT representation, as appropriate on NATO subcommittees and working groups that have responsibility for developing national policies governing the protection of NATO materials.

7.03 The Maritime Associate Administrator for Administration will:

1. Serve as the Program Manager for the NATO Program in DOT.

2. Provide support to DOT as the subject matter expert on NATO Security.
3. Administer and manage DOT's NATO Sub-Registry under the guidance of the Central United States Registry, and prepare written instructions within the framework of the established guidelines for management of the NATO program.
4. Provide guidance to DOT component organizations to implement and maintain the NATO program, ensuring it complies with all Government-wide security policies for the protection of NATO material.
5. Represent DOT on all applicable NATO committees not attended by the Maritime Administrator and provide DOT representation, as appropriate on NATO subcommittees and working groups that have responsibility for developing national policies governing the protection of NATO materials. Additionally, when outside groups request participation of OAs and Secretarial Offices on matters involving NATO, the MARAD Security Officer must be consulted.
6. Provide oversight of the OA responsibilities under this Order through the conduct of site visit/assessments and spot inspections as appropriate to ensure compliance with policies for the proper disposition of NATO material.
7. Manage the submission of all required annual reports for Central Registry to ensure compliance with NATO requirements.
8. Provide annual NATO training to all personnel who are read into the programs and maintain a copy of completion acknowledgement.

7.04 The Maritime Associate Administrator for National Security will:

1. Appoint a primary and alternate Control Point Officer to manage the MARAD NATO program. The Control Point is authorized to maintain NATO Confidential material permanently; however, only temporary storage of NATO Secret material for 24 hours or less is authorized.
2. Coordinate the development/creation of all derivative NATO documents with the Sub-Registry.
3. Conduct an annual self-inspection in the month of October and provide the results to the Sub-Registry.

7.05 The Director, Office of Security will work closely with all DOT organizations to assist in effectively implementing the requirements of this Order.

7.06 The Director, Office of Intelligence, Security, and Emergency Response will:

1. Coordinate with the MARAD Security Officer to ensure all counterintelligence information, relating to the protection of DOT's NATO program from espionage, sabotage, and subversion is carefully monitored.

2. Appoint a primary and alternate Control Point Officer to manage the OST NATO program. The Control Point is authorized to maintain NATO Confidential material permanently; however, only temporary storage of NATO Secret material for 24 hours or less is authorized.
3. Coordinate the development/creation of all derivative NATO documents with the Sub-Registry.
4. Conduct annual self-inspection in the month of October and provide the results to the Sub-Registry.

7.07 The Departmental Director, Office of Human Resource Management will provide oversight of annotating NATO functional requirements in position description.

7.08 The Departmental Chief Information Officer will coordinate with the MARAD Chief Information Officer (Sub-Registry Information Assurance Officer) to ensure all systems that process NATO material are properly certified and accredited and readily available for review upon request.

7.09 Secretarial Officers and Heads of OAs will provide leadership and support necessary to ensure compliance with the requirements of this Order within their respective organizations.

7.10 The Sub-Registry will have a primary and alternate Control Officer and Information Assurance Officer appointed in writing (Appendix 3). The appointed Control Officer will:

1. Ensure Control Points are in compliance with this Order and primary and alternate Control Officers are appointed as required (Appendix 4).
2. Ensure personnel requesting access to NATO material have the appropriate security clearance before granting access, also a need to know, a justification, and the requirement is recorded on the individual's position description.
3. Maintain NATO folders on each individual indoctrinated into the NATO program and ensure that each folder has the read-on acknowledgement forms, annual training acknowledgement, and other program related documents as appropriate.
4. Conduct NATO access read-on briefings before access is granted and ensure an acknowledgement briefing form (Appendix 1) is maintained in the folder.
5. Ensure all individuals with NATO access complete annual NATO specific training and sign appropriate training acknowledgement forms.
6. Debrief all personnel when access to NATO material is no longer required (Appendix 1), or prior to departing the organization, or when U.S. clearance is revoked and/or suspended.
7. Maintain a roster of all personnel read-on to the NATO Program.
8. Conduct on site visit/assessments and spot inspections as appropriate to ensure compliance with policies for the proper disposition of NATO material.

9. Conduct an annual inventory of all registry required documents and submit required annual report for the Central United States Registry no later than March 15 of each year.
10. Ensure transferring NATO documents are recorded on the classified document accountability record—Department of the Army (DA) Form 3964 (Appendix 2). The DA Form 3964 will be used to record reproduction authorization, destruction certification and serve as receipt/tracer action.
11. Serve as a focal point for receiving and storing NATO material and recording initial registry item on the classified document accountability record—DA Form 3964 (Appendix 2).
12. Pass/forward individual's NATO access authorization to external organizations as appropriate.

7.11 The Control Point will have a primary and alternate Control Officer appointed in writing (Appendix 4). The appointed Control Officer serves as the program representative and will:

1. Ensure that the Control Point operates as an extension of the Sub-Registry only maintaining minimum documents for continuous operation at NATO Confidential and below level.
2. Ensure the Control Point maintains the operational capability to provide temporary storage of NATO Secret for 24 hours or less.
3. Serves as a focal point for receiving NATO material and recording initial registry item on the classified document accountability record—DA Form 3964 (Appendix 2).
4. Maintain a roster of all personnel read-on to NATO Program.
5. Coordinates with the Sub-Registry to read-on or debrief assigned personnel.
6. Coordinates with the Sub-Registry to pass/forward an individual's NATO access authorization to external organizations.

7.12 Employees and contractors will comply with this Order as a minimum standard to maintain continuous access to NATO material and will:

1. Protect NATO material from individuals who do not have authorized access to that information, including securing it in approved equipment or facilities whenever it is not under the direct control of an authorized individual.
2. Ensure individuals are properly indoctrinated (read-on) into the NATO program prior to granting access to NATO material.
3. Sign the briefing/debriefing acknowledgement form (Appendix 1) before any involvement in the NATO program.

4. Ensure that all changes in position descriptions related to the access requirement for NATO or removal of NATO access is reported to the Office of Human Resources and the Sub-Registry.
5. Complete annual NATO specific training and sign appropriate training acknowledgement forms.
6. Prior to departing DOT, each employee and contractor will out-process with the Sub-Registry and sign the debriefing acknowledgement form (Appendix 1).
7. Ensure compliance with NATO handling procedures for classification marking, classification (including derivative/downgrade classification), destruction, transmitting, copying, and storing. The Sub-registry and Control Point will assist as appropriate.

A handwritten signature in black ink that reads "Paul N. Jaenichen". The signature is written in a cursive style with a large, looping initial "P".

Paul N. Jaenichen  
Acting Maritime Administrator

Central U.S. Registry  
9301 Chapek Rd  
BLDG #1458, Rm#2NW3604  
Ft. Belvoir, VA 22060  
<https://secureweb.hqda.pentagon.mil/cusr>  
<http://classweb.hqda-s.army.smil.mil/cusr>

**SUBREGISTRY SIGNATURE LIST**

ACCREDITATION EXPIRATION DATE:  
FOR CUSR USE ONLY  
DATE: \_\_\_\_\_

<b>Higher HQ Commander/Director:</b>	<b>SUBREGISTRY ORGANIZATION:</b>	<b>Office symbol:</b>
<b>MAILING ADDRESS:</b>	<b>MAILING ADDRESS:</b>	<b>Office Phone</b> <b>Commercial:</b> <b>DSN:</b>
		<b>Fax</b> <b>Commercial:</b> <b>DSN:</b>

<b>Primary Control Officer's email Address:</b>	<b>CLASSIFIED &amp; UNCLASSIFIED:</b> Unclassified: Classified:
<b>Alternate Control Officer's email Address:</b>	Unclassified: Classified:
<b>Primary IA Officer's email Address:</b>	Unclassified: Classified:
<b>Alternate IA Officer's email Address:</b>	Unclassified: Classified:

**Defense Courier Service Address:**  
(for CTS and ATOMAL SR & CP only)

(CHECK ONLY ONE BOX)

\_\_\_\_ CTS ATOMAL SR    \_\_\_\_ Cosmic SR    \_\_\_\_ NS ATOMAL SR    \_\_\_\_ NATO Secret SR

**System Accreditation:** Establish Date: \_\_\_\_\_ Expiration Date: \_\_\_\_\_  
Network Type: \_\_\_\_\_

Individual Access (Enter Only One Abbreviation Below)

CTSA - Cosmic Top Secret ATOMAL	CTS - Cosmic Top Secret	NSA - NATO Secret ATOMAL	NS- NATO Secret
------------------------------------	-------------------------	-----------------------------	-----------------

Name of Control Officer and Alternates	Grade	Access	Signature	Office Phone Number
<b>Primary:</b>				
<b>Alternate(s):</b>				
<b>Name of IA Officer and Alternates</b> (NATO INFOSEC Officer equivalent)				
<b>Primary:</b>				
<b>Alternate:</b>				
<b>Authorizing Official (Typed)</b>	<b>Signature</b>	<b>Date</b>	<b>Phone Number</b>	

**SECURITY MANAGER**

<b>Primary:</b>			
<b>Alternate(s):</b>			
<b>Agency:</b>	<b>SMO Code:</b>	<b>Fax Number:</b>	

Central U.S. Registry  
9301 Chapek Rd  
BLDG #1458, Rm#2NW3604  
Ft. Belvoir, VA 22060  
<https://secureweb.hqda.pentagon.mil/cusr>  
<http://classweb.hqda-s.army.smil.mil/cusr>

**CONTROL POINT SIGNATURE LIST**

ACCREDITATION EXPIRATION DATE FOR CUSR USE ONLY
DATE: _____

<b>Parent Sub-Registry Name /POC</b>	<b>CONTROL POINT ORGANIZATION :</b>	<b>Office symbol:</b>
<b>Sub-Registry MAILING ADDRESS:</b>	<b>MAILING ADDRESS:</b>	<b>Office Phone</b> <b>Commercial:</b> <b>DSN:</b>
	<small>(DO NOT ABBREVIATE)</small>	<b>Fax</b> <b>Commercial:</b> <b>DSN:</b>

<b>CLASSIFIED &amp; UNCLASSIFIED:</b>	
<b>Primary Control Officer's email Address:</b>	Unclassified: Classified:
<b>Alternate Control Officer's email Address:</b>	Unclassified: Classified:
<b>Primary IA Officer's email Address:</b>	Unclassified: Classified:
<b>Alternate IA Officer's email Address:</b>	Unclassified: Classified:

**Defense Courier Service Address:**  
(for CTS and ATOMAL SR & CP only)

(CHECK ONLY ONE BOX)

CTS ATOMAL CP    
  Cosmic CP    
  NS ATOMAL CP    
  NATO Secret CP

**System Accreditation:** Establish Date: \_\_\_\_\_ Expiration Date: \_\_\_\_\_  
Network Type: \_\_\_\_\_

**Individual Access (Enter Only One Abbreviation Below)**

CTSA - Cosmic Top Secret ATOMAL	CTS - Cosmic Top Secret	NSA - NATO Secret ATOMAL	NS- NATO Secret
------------------------------------	-------------------------	-----------------------------	-----------------

Name of Control Officer and Alternates	Grade	Access	Signature	Office Phone Number
<b>Primary:</b>				
<b>Alternate(s):</b>				
<b>Name of IA Officer and Alternates</b> (NATO INFOSEC Officer equivalent)				
<b>Primary:</b>				
<b>Alternate:</b>				
<b>Authorizing Official (Typed)</b>	<b>Signature</b>		<b>Date</b>	<b>Phone Number</b>

**SECURITY MANAGER**

<b>Primary:</b>		
<b>Alternate(s):</b>		
<b>Agency:</b>	<b>SMO Code:</b>	<b>Fax Number:</b>

**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) (been briefed) and fully understand the procedures for handling (COSMIC) (ATOMAL) (NATO SECRET) (NATO CONFIDENTIAL) material and am aware of my responsibility 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 rebriefed and fully understand the procedures for handling ATOMAL material and am aware of my responsibility to safeguard such information.	
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: _____
_____	

CLASSIFIED DOCUMENT ACCOUNTABILITY RECORD						DATE	
For use of this form, see AR 380-5; the proponent agency is the Office, Assistant Chief of Staff for Intelligence.							
SECTION A - GENERAL							
TO:				FROM:			
DATE RECEIVED		ACTION OFFICE(S)		SUSPENSE DATE(S)		REGISTER OR CONTROL NO.	
CONTROL LOG OR FILE NO.	CLASSIFI-CATION	NUMBER OF COPIES	DESCRIPTION (Type, File Ref., Unclassified Subject or Short Title and Number of Indorsements/Incls)			DATE OF DOCUMENT	ORIGINATOR
SECTION B - ROUTING							
TO	COPY NO.	DATE	I ACKNOWLEDGE RECEIPT OF THE MATERIAL DESCRIBED HEREON				
			PRINTED NAME		SIGNATURE		
1.							
2.							
3.							
4.							
5.							
SECTION C - DESTRUCTION CERTIFICATE (Check appropriate block)							
MATERIAL DESCRIBED HEREON HAS BEEN:						PAGE OR COPY NO.	
<input type="checkbox"/> DESTROYED <input type="checkbox"/> TORN IN HALF AND PLACED IN A CLASSIFIED WASTE CONTAINER (AR 380-5)							
OFFICE SYMBOL	DATE	PRINTED NAME OF CUSTODIAN OR REP			SIGNATURE		
DESTRUCTION RECORD NO.	DATE	PRINTED NAME OF CERTIFYING/DESTR. OFF.			SIGNATURE		
PAGE OR COPY NUMBER	DATE	PRINTED NAME OF WITNESSING OFFICIAL			SIGNATURE		
SECTION D - REPRODUCTION AUTHORITY							
NUMBER OR COPIES TO BE REPRODUCED		AUTHORIZED BY			DATE		
SECTION E - RECEIPT/TRACER ACTION (Check appropriate block)							
<input type="checkbox"/> RECEIPT OF DOCUMENT(S) ACKNOWLEDGED			<input type="checkbox"/> DOCUMENT(S) HAVE NOT BEEN RECEIVED				
<input type="checkbox"/> TRACER ACTION: SIGNED RECEIPT FOR MATERIAL DESCRIBED ABOVE HAS NOT BEEN RECEIVED.							
DATE	PRINTED NAME, GRADE OR TITLE				SIGNATURE		
COMMENTS							