Department of the Army Headquarters, United States Army Training and Doctrine Command Fort Eustis, Virginia 23604-5700

22 August 2016

Administration-General

INFORMATION SECURITY PROGRAM

FOR THE COMMANDER:

OFFICIAL:

KEVIN W. MANGUM Lieutenant General, U.S. Army Deputy Commanding General/ Chief of Staff

RICHARD A. DAVIS

Senior Executive

Deputy Chief of Staff, G-6

History. This publication is a new U.S. Army Training and Doctrine Command (TRADOC) memorandum.

Summary. This memorandum establishes policies and procedures for the information security program for Headquarters (HQ), TRADOC organizations located at Fort Eustis, Virginia.

Applicability. This memorandum applies to all military and Department of the Army (DA) civilian personnel within HQ TRADOC organizations, Army Capabilities Integration Center (ARCIC), and the U.S. Army Center for Initial Military Training (USACIMT).

Proponent and exception authority. The proponent of this memorandum is the Office of the TRADOC Deputy Chief of Staff (DCS), G-2. The proponent has the authority to approve exceptions or waivers to this memorandum that are consistent with controlling laws and regulations. Activities may request a waiver to this memorandum by providing justification that includes a full analysis of the issue and a formal review by the TRADOC Staff Judge Advocate. All waiver requests will be endorsed by the senior leader of the requesting activity and forwarded to the policy proponent.

Army Management Control Process. This memorandum does not contain management control provisions.

Supplementation. Supplementation of this memorandum and establishment of command and local forms is prohibited without prior approval from TRADOC DCS, G-2, 950 Jefferson Avenue, Fort Eustis, VA 23604-5740.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to TRADOC DCS, G-2, 950 Jefferson Avenue, Fort Eustis, VA 23604-5740.

Distribution A. This publication is available in electronic media only and is published on the TRADOC homepage at http://www.tradoc.army.mil/tpubs/.

Summary of Change

TRADOC Memorandum 380-XX Information Security Program

This new publication, dated 22 August 2016 –

- o Prescribes policies and procedures for the information security program for headquarters United States Army Training and Doctrine Command organizations located at Fort Eustis, Virginia.
- o Applies to headquarters United States Army Training and Doctrine Command military personnel, government civilian employees and contractors at Fort Eustis, Virginia.

Contents

	Page
Chapter 1 Introduction	5
1-1. Purpose	
1-2. References	
1-3. Explanation of abbreviations and terms	5
1-4. Responsibilities	
Chapter 2 Responsibilities	5
2-1. Commanding General, United States (U.S.) Army Training and Doctrine Command	
(TRADOC)	5
2-2. TRADOC Deputy Chief of Staff (DCS), G-2	5
2-3. TRADOC Command Security Manager	5
2-4. TRADOC DCS, G-2 Security	5
2-5. TRADOC Activity Security Manager	5
2-6. TRADOC Controlled Unclassified Information (CUI) Officer	6
2-7. TRADOC Management	6
2-8. TRADOC Personnel	6
Chapter 3 Background and Protection	6
3-1. Background	6
3-2. Protection	7
Appendix A References	7
Appendix B Original versus Derivative Classification	9
Appendix C Classification Guides	11
Appendix D Declassification Procedures	13
Appendix E Marking Documents	
Appendix F Controlled Unclassified Information (CUI)	15
Appendix G Distribution Statements	17
Appendix H Control Measures	18
Appendix I Emergency Planning	23
Appendix J Classified Discussion	26
Appendix K Removal of Equipment	26
Appendix L Classified Visits	27
Appendix M Classified Venues	30
Appendix N Information Processing Equipment	32
Appendix O Receipt of Classified Material	
Appendix P Accountability	34
Appendix Q Reproduction	36
Appendix R Disposition and Destruction	37
Appendix S Waivers	38
Appendix T Inspections	38
Appendix U Storage	39
Appendix V Physical Security Standards	
Appendix W Transmission	
Appendix X Handcarrying Classified Material	
Appendix Y Unauthorized Disclosure	
Appendix Z Security Education, Training, and Awareness (SETA)	
Glossary	

Figure List	
Figure I-1. Emergency Plan Example	24
Figure L-1. Secure Internet protocol router network (SIPRNET) and AV Classified Open	
Storage Area Acknowledgement	29
Figure M-1. Security Checklist for Classified Conferences/Meetings	32
Figure X-1. Courier Briefing	46
Figure X-2. Courier Acknowledgement	49
Figure X-3. CONUS Courier Authorization Orders	51
Figure Z-1. North Atlantic Treaty Organization (NATO) Briefing	56
Figure Z-2. NATO Acknowledgement	63

Chapter 1 Introduction

1-1. Purpose

This memorandum establishes and standardizes the processes, requirements, and procedures relating the Headquarters (HQ), United States (U.S.) Army Training and Doctrine Command (TRADOC) information security program.

1-2. References

Required and related publications are listed in Appendix A.

1-3. Explanation of abbreviations and terms

Abbreviations and special terms used in this memorandum are explained in the Glossary.

1-4. Responsibilities

Responsibilities are listed in Chapter 2.

Chapter 2 Responsibilities

2-1. Commanding General, United States (U.S.) Army Training and Doctrine Command (TRADOC)

Security is a command function. The Commanding General, TRADOC, has overall management, functioning, and effectiveness for security programs within TRADOC. The Commanding General, TRADOC, may delegate the authority to execute security requirements but not the responsibility to do so.

2-2. TRADOC Deputy Chief of Staff (DCS), G-2

The TRADOC DCS, G-2 is the TRADOC Senior Intelligence Officer responsible for the overall command intelligence and sensitive compartmented information (SCI) programs.

2-3. TRADOC Command Security Manager

The Director of Security, HQ TRADOC DCS, G-2, is appointed as the TRADOC Command Security Manager. The TRADOC Command Security Manager is the principal advisor for the TRADOC information security program and is responsible to the Commanding General, TRADOC, for management and implementation of the program.

2-4. TRADOC DCS, G-2 Security

The Office of the TRADOC DCS, G-2 Security is responsible for the overall management of the TRADOC information security program.

2-5. TRADOC Activity Security Manager

Each HQ TRADOC staff element, Army Capabilities Integration Center (ARCIC), and U.S. Army Center for Initial Military Training (USACIMT), will appoint, in writing, a primary and alternate activity security manager who are responsible for the management and implementation of their respective organization's information security program.

2-6. TRADOC Controlled Unclassified Information (CUI) Officer

Each HQ TRADOC staff element, ARCIC, and USACIMT, will appoint, in writing, a primary and alternate CUI Officer who are responsible for the management and implementation of their respective organization's CUI program.

2-7. TRADOC Management

Directors, managers, and supervisors have a key role in the effective implementation of TRADOC security programs. Directors, managers, and supervisors set the tone for compliance by subordinate personnel with the requirements to properly safeguard, classify, and declassify information relating to national security. Directors, managers, and supervisors will:

- a. Ensure subordinate personnel who require access to classified information are properly cleared and given access only to that information for which they have a need-to-know.
 - b. Ensure subordinate personnel are trained in, understand, and follow security requirements.
- c. Oversee subordinate personnel in the execution of procedures necessary to allow the continuous safeguarding and control of classified and sensitive information.
- d. Lead by example. Directors, managers, and supervisors shall follow Department of Defense (DOD) and Department of the Army (DA) policies and procedures to properly protect classified and sensitive information, and classify/declassify information, as appropriate.
- e. Ensure subordinate personnel whose security clearance eligibility requires an update or upgrade complete and submit Electronic Questionnaires for Investigations Processing (e-QIP) documentation to the Personnel Security Investigation Center of Excellence within 5 calendar days of receiving the initial request to update/upgrade the security clearance.

2-8. TRADOC Personnel

All TRADOC personnel have a personal, individual, and official responsibility to safeguard information related to national security, and protect government property.

- a. Security regulations do not guarantee protection and cannot be written to cover all situations. Basic security principles, common sense, and a logical interpretation of regulations must be applied by all personnel.
- b. TRADOC personnel will immediately report, through their supervisor to HQ TRADOC DCS, G-2 Security, violations that could lead to the unauthorized disclosure of classified and sensitive information.

Chapter 3 Background and Protection

3-1. Background

a. Recent events in the news have highlighted the ramifications of poor security and protection of classified national defense information and CUI. Technological advances in media storage coupled with a determined individual's desire to cause harm (for either perceived good or

bad intentions) have resulted in unimaginably large volumes of information being stolen and compromised in mere seconds.

b. The ultimate release of this information has caused irreparable damage to our national security efforts as well as political and economic trusts the Army has shared with some of its closest Allies. Insider threat personnel have made their mark on the security of classified and unclassified information systems.

3-2. Protection

- a. The protection of classified national defense information and CUI is paramount to the safety of the lives of U.S. military personnel, civilians, contractors, family members, as well as those coalition forces that fight at our sides.
- b. All personnel having access to classified and/or CUI have an obligation to protect this information by following those steps outlined in this memorandum as well as those in supporting manuals, directives, and regulations.
- c. In the interest of national security, it is vital TRADOC continually protects personnel who live, work, and visit its facilities and the classified and CUI material they work with, from natural and manmade threats and disasters.

Appendix A References

Section I Required Publications

DOD Manual 5200.01, Volumes 1-4 DOD Information Security Program

AR 380-5 & TRADOC Supplement 1 to AR 380-5 DA Information Security Program

Section II Related Publications

Executive Order 13526 Classified National Security Information

Information Security Oversight Office Directive No. 1 Classified National Security Information

DOD Instruction 5230.24 Distribution Statements on Technical Documents

AR 25-2

Information Assurance

AR 25-30

The Army Publishing Program

AR 380-10

Foreign Disclosure and Contacts with Foreign Representatives

AR 380-40

Policy for Safeguarding and Controlling Communications Security Material

AR 380-67

Personnel Security Program

AR 525-13

Anti-Terrorism Force Protection: Security of Personnel, Information, and Critical Resources

AR 25-400-2

The Army Records Information Management System (ARIMS)

U.S. Security Authority for North Atlantic Treaty Organization (NATO) Instruction 1-07 Implementation of NATO Security Requirements

Section III

Referenced Forms

DA Form 3161, Request for Issue or Turn-In

DA Form 3964, Classified Document Accountability Record

DD Form 254, Contract Security Classification Specification

DD Form 2501, Courier Authorization Card

Department of Energy (DOE) Form 5631.20, Request for Visit or Access Approval

Standard Form (SF) 312, Classified Information Nondisclosure Agreement

SF 700, Security Container Information

SF 701, Activity Security Checklist

SF 702, Security Container Check Sheet

SF 706, Top Secret (label)

SF 707, Secret (label)

SF 708, Confidential (label)

SF 710, Unclassified (label)

SF 711, Data Descriptor (label)

SF 712, Classified SCI (label)

Appendix B Original versus Derivative Classification

B-1. Original Classification

- a. Original classification is the initial decision by an original classification authority (OCA) that an item of information could reasonably be expected to cause identifiable or describable damage to the national security if subjected to unauthorized disclosure and requires protection in the interest of national security.
- b. These decisions can only be made by persons designated in writing, who have received training in the exercise of this authority, and who have program support responsibility or cognizance over the information. At HQ TRADOC, the following positions are designated as having OCA:
- (1) Commanding General, TRADOC Top Secret OCA approved through Headquarters, Department of the Army (HQDA) DCS, G-2 and by the Under Secretary for Defense (Intelligence).
 - (2) Director, ARCIC Secret OCA approved by HQDA DCS, G-2.
- c. The OCA must determine information under their purview meets the requirements of Executive Order 13526, and there is a reasonable possibility the information can be provided protection from unauthorized disclosure. Once a decision is made to classify, information will be classified at one of three levels:
- (1) <u>Top Secret</u> Shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the OCA is able to identify or describe.
- (2) <u>Secret</u> Shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the OCA is able to identify or describe.
- (3) <u>Confidential</u> Shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the OCA is able to identify or describe.

- d. Information shall be classified only to protect national security. Classification may be applied only to information that is owned by, produced by or for, or is under the control of the U.S. Government.
- e. Information may be considered for classification only if its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to national security and it concerns one of the categories below:
 - (1) Military plans, weapons systems, or operations.
 - (2) Foreign government information.
- (3) Intelligence activities (including covert action), intelligence sources or methods, or cryptology.
 - (4) Foreign relations or foreign activities of the U.S., including confidential sources.
 - (5) Scientific, technological, or economic matters relating to the national security.
 - (6) U.S. Government programs for safeguarding nuclear materials or facilities.
- (7) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security.
 - (8) The development, production, or use of weapons of mass destruction.
- f. Classification challenges will be brought to the attention of the respective activity security manager and HQ TRADOC DCS, G-2 Security for discussion/resolution in accordance with Enclosure 4, Volume 1, DOD Manual 5200.01.
- g. The OCAs are required to receive initial and annual OCA training in accordance with DOD Manual 5200.01. The HQ command group and ARCIC activity security managers are responsible for ensuring their respective OCA receives OCA training, and the OCA certifies in writing of having received such training.
- h. Contact the HQ TRADOC Foreign Disclosure Officer prior to releasing any classified information to foreign governments or international organizations.

B-2. Derivative Classification

- a. Derivative classification incorporates, paraphrases, restates, or generates in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. It also includes the classification of information based on classification guidance.
 - b. Persons who apply derivative classification markings shall:
- (1) Be identified by name, position, and organization in a manner that is immediately apparent for each derivative classification action.

- (2) Observe and respect original classification decisions;
- (3) Use only authorized sources for classification guidance;
- (4) Use caution when paraphrasing or restating information extracted from a classified source document as the classification level may change; and
- (5) Take appropriate and reasonable steps to resolve doubts or conflicts about the classification, level of classification, and duration.
- c. Derivative classifiers will complete derivative classification training at least once every 2 years.
- d. Derivative classifiers will consult Enclosure 4, Volume 1, DOD Manual 5200.01 for further derivative policy guidance.

Appendix C Classification Guides

C-1. Security Classification Guide (SCG)

- a. SCGs are prepared to facilitate the proper and uniform derivative classification of information. Each guide shall be approved in writing by the OCA and at the highest level of classification prescribed in the guide.
- b. Each approved SCG and its changes will be sent to the following agencies along with a DD Form 2024 (DOD Security Classification Guide Data Elements):
 - (1) One copy to HQ TRADOC DCS, G-2 Security.
- (2) HQ TRADOC DCS, G-2 Security will, in turn, provide to HQDA DCS, G-2 information security program manager.
- (3) One copy to Department of Defense, Office of Security Review, 1155 Defense Pentagon, Washington, DC 20301-1155.
- (4) One copy, in paper document (hard copy) and/or automated format (soft copy) will be sent to Army Declassification Activity, Room 102, Casey Building, 7701 Telegraph Road, Alexandria, VA 22315-3860. Email questions on how to send guides electronically to: usarmy.belvoir.hqda-oaa-ahs.mbx.rmda-records-declassification@mail.mil.
- (5) One copy to the Administrator, Defense Technical Information Center, ATTN: DTIC-OA (Security Classification Guides), 8725 John J. Kingman Road, Fort Belvoir, VA 22060-6218. Each guide furnished to Defense Technical Information Center shall bear the appropriate distribution statement required by DOD Instruction 5230.24. For information on e-mail or electronic submission, contact TR@dtic.mil.

Note: Do not distribute SCGs covering Top Secret, SCI, SAP information, or guides deemed by the SCG's approval authority to be too sensitive for automatic secondary distribution. Contact the HQ TRADOC DCS, G-2 Security for further guidance.

C-2. SCG Requirements

- a. SCGs will, at a minimum, include the following information:
- (1) Identify specific items/elements of information to be protected and the classification level to be assigned.
 - (2) Provide declassification instructions for each item/element, to include any exemptions.
- (3) Provide a concise reason for classification for each item, element, or category of information and cite the applicable classification category(ies).
- (4) State the declassification instructions for each item or element of classified information.
 - (5) Identify any special handling caveats, warning notices, or instructions.
- (6) Identify by name or personal identifier and position title, the OCA along with the date of the approval.
- (7) Provide a point of contact, address, and telephone number for any questions, challenges, or suggestions, and include a statement encouraging personnel to informally question the classification of information before formally challenging.
- b. The OCA will review and update, as needed, SCGs once every 5 years, and submit changes to agencies outlined in Para C-1.b. If no changes are required, the OCA will submit to Defense Technical Information Center and copy furnish HQ TRADOC DCS, G-2 Security a new DD Form 2024 with the date of the next required review and annotate the record copy of the guide with this fact and the date of the review.
 - c. Guides will be cancelled if:
 - (1) All classified information within the guide specifies has been declassified; or
- (2) A new SCG incorporates the classified information covered by the old guide, and there is reasonable likelihood that any information not incorporated by the new guide shall be the subject of derivative classification.
- (3) The OCA, or successor organization, shall maintain a record copy of any canceled guide.

Appendix D

Declassification Procedures

D-1. Declassification

Declassification is the authorized change in the status of information from classified information to unclassified information.

- a. Information will be declassified as soon as it no longer meets the standards for classification. Information shall remain classified only as long as it is in the best interest of national security to keep it protected, and continued classification is in accordance with DOD Manual 5200.01.
- b. Declassified information shall not be released to the public until a public release review has been conducted.
- c. Holders of classified information marked with a date or event on the "declassify on" line, shall, prior to downgrading or declassifying the information, confirm with the OCA the information has not extended the classification period. Classified information shall continue to be safeguarded until the OCA has not extended the classification period.
- d. A declassification review of original classified, permanent historical value information will be conducted annually, normally at the end of each FY and in conjunction with the annual SF 311 (Agency Security Classification Management Program Data) review.

D-2. Automatic Declassification

Automatic declassification is the declassification of information based solely upon the occurrence of a specific date or event as determined by the OCA or the expiration of a maximum time frame for duration of classification. Refer to Enclosure 5, Volume 1, DOD Manual 5200.01, for additional declassification requirements.

Appendix E Marking Documents

E-1. Marking

Marking is the principal means of informing holders of classified and sensitive information of its classification/sensitivity level and protection requirements. Marking serves the following purposes:

- a. Alerts holders to the presence of classified and sensitive information.
- b. Identifies the exact information needing protection.
- c. Indicates the level of classification/sensitivity assigned to the information.
- d. Provides guidance on downgrading and declassification.
- e. Gives information on the source(s) and reason(s) for classification of information.

f. Warns holders of special access, control, dissemination, or safeguarding requirements.

E-2. Marking Elements

All classified information will include the following marking elements:

- a. The overall classification of the document, referred to as the "banner line" and the most restrictive control markings applicable to the overall document.
- b. Identification of the specific classified information in the document and its level of classification referred to as "portion marks". Every portion (e.g., subject, title, paragraphs, sections, tabs, attachments, classified signature blocks, bullets, tables, pictures) in every classified document shall be marked to show the highest level of classification that it contains.
- c. Component, office of origin, and date of origin and will be shown on the first page, title page, or front cover.
- d. Identification of the basis for classification of the information contained in the document and of the OCA or derivative classifier, referred to as the "classification authority block". The "classification authority block" will normally appear on the face of each classified U.S. Government document and will indicate the authority for the classification determination and the duration of classification.
- e. Declassification instructions and any downgrading instructions that apply. "Declassify On" line will be included on the face of each classified U.S. Government document except those containing Restricted Data or Formerly Restricted Data.
- f. Identification of special access, dissemination control, and handling or safeguarding requirements that apply.

E-3. Marking Media

- a. Classified material other than paper (and comparable electronic) documents require the same information above and either marked on it or made available to holders by other means of notification.
- b. When classified or sensitive information is contained in information technology (IT) equipment, hardware, or media or on film, tape, or other audio/visual (AV) media, the marking provisions of Volume 2, DOD Manual 5200.01 will be met in a way that is compatible with the type of material. This is to ensure holders and users are clearly warned of the presence of classified/sensitive information. These types of materials will be marked with the following labels:
 - (1) SF 706 Top Secret label for IT media.
 - (2) SF 707 Secret label for IT media.
 - (3) SF 708 Confidential label for IT media.

- (4) SF 710 Unclassified label for IT media.
- (5) SF 711 Data descriptor label for IT media.
- (6) SF 712 Classified SCI label.
- c. Classified information contained on fixed or removable magnetic storage media will be stored in a General Services Administration (GSA)-approved security container or used in an approved open storage of classified material area. Refer to Volume 2, DOD Manual 5200.01, for additional marking requirements and guidance regarding removable IT storage media.
- d. Refer to Volume 2, DOD Manual 5200.01, for the complete and latest classified marking requirements with examples.

Appendix F

Controlled Unclassified Information (CUI)

F-1. CUI

In addition to classified information, certain types of unclassified information also require application of access and distribution controls and protective measures for a variety of reasons. Such information is referred to as CUI.

- a. The originator of the information is responsible for determining at origination whether the information qualifies for CUI status, and if so, for applying the appropriate CUI markings.
- b. All DOD unclassified information must be reviewed and approved for release (to include posting to public accessible websites) by the TRADOC Operations Security and Public Affairs Officers.
- c. Any TRADOC administrative publication must have the originator's review and written approval prior to publishing. Proponent will maintain written approval within publication records.
- d. Contact the HQ TRADOC Foreign Disclosure Officer prior to releasing CUI to foreign governments or international organizations.
- e. Pay particular attention to export control regulations and access restrictions on exportcontrolled CUI information that may be protected by law, Executive order, regulation, or contract.

F-2. Types of CUI

There are several types of information that are considered CUI to include:

- a. For Official Use Only (FOUO).
- b. Law Enforcement Sensitive.

- c. DOD Unclassified Controlled Nuclear Information.
- d. Limited Distribution.
- e. Department of State Sensitive But Unclassified.
- f. Certain Foreign Government information (Restricted or In Confidence).

F-3. For Official Use Only (FOUO)

- a. FOUO is a dissemination control applied by DOD to unclassified information when disclosure to the public of that particular record, or portion thereof, would reasonably be expected to cause a foreseeable harm to an interest protected by one or more Freedom of Information Act Exemptions 2 through 9 below. The Freedom of Information Act specifies nine exemptions:
 - (1) Exemption 1. Information that is classified to protect national security.
- (2) Exemption 2. Information related solely to the internal personnel rules and practices of an agency.
 - (3) Exemption 3. Information that is prohibited from disclosure by another federal law.
- (4) Exemption 4. Trade secrets or commercial or financial information that is confidential or privileged.
 - (5) Exemption 5. Privileged communications within or between agencies, including:
 - (a) Deliberative Process Privilege.
 - (b) Attorney-Work Product Privilege.
 - (c) Attorney-Client Privilege.
- (6) Exemption 6. Information that, if disclosed, would invade another individual's personal privacy.
 - (7) Exemption 7. Information compiled for law enforcement purposes that:
 - (a) Could reasonably be expected to interfere with enforcement proceedings.
 - (b) Would deprive a person of a right to a fair trial or an impartial adjudication.
- (c) Could reasonably be expected to constitute an unwarranted invasion of personal privacy.
 - (d) Could reasonably be expected to disclose the identity of a confidential source.

- (e) Would disclose techniques and procedures for law enforcement investigations or prosecutions.
 - (f) Could reasonably be expected to endanger the life or physical safety of any individual.
 - (8) Exemption 8. Information that concerns the supervision of financial institutions.
 - (9) Exemption 9. Geological information concerning wells.
 - b. FOUO information and material shall include:
 - (1) The identity of the originating agency or office.
- (2) The marking FOR OFFICIAL USE ONLY at the bottom of the outside of the front cover, the title page, the first page, and the outside the back cover (if there is one).
- (3) The marking FOR OFFICIAL USE ONLY at the bottom of internal pages containing FOUO material.
- (4) The marking FOUO within subject lines, titles, and each section, part, paragraph, or similar portion of an FOUO document to show that they contain information requiring protection.
 - (5) Exemption and distribution statements on FOUO documents as applicable.
- c. No person may have access to FOUO information unless that person has been determined to have a valid need to know. Reasonable steps shall be taken to minimize the risk of access by unauthorized personnel.
- d. After working hours, FOUO information may be stored in unlocked containers, desks, or cabinets when there is 24-hour access personnel present; otherwise, secure FOUO information in locked desks, file cabinets, bookcases, locked rooms, etc.
- e. Transmit FOUO materials via first class mail, parcel post, or via fourth class mail for bulk shipments. Utilize secure (encrypted), electronic means whenever practical.
 - f. Refer to Volume 4, DOD Manual 5200.01, for complete CUI guidance.

Appendix G Distribution Statements

G-1. Distribution Statements

Distribution statements are intended to facilitate control, secondary distribution, and release of documents without the need to repeatedly obtain approval or authorization from the controlling DOD office.

G-2. Distribution Statements Requirements

- a. Distribution statements will be placed on classified and unclassified scientific and technical documents created under the DOD scientific and technical information program.
- b. Distribution statements are to be applied to all newly created technical documents generated by DOD-funded research, development, test, and evaluation programs and to newly created technical documents and other technical information (e.g., test plans, computer software) that can be used or adapted for use in development, manufacture, or operation of any military or space equipment or related technology.
- c. Distribution statements are also required on all TRADOC publications in accordance with AR 25-30.
- d. TRADOC organizations generating or responsible for technical documents and/or publications shall determine if one or more of the reasons for controlled dissemination apply and mark the documents appropriately before initial distribution.
 - e. Consult DOD Instruction 5230.24 for the latest distribution statements and requirements.

Appendix H Control Measures

H-1. Safeguarding

All personnel are responsible for safeguarding U.S. Government information for which they have access. This responsibility includes ensuring they do not permit access to CUI or classified information by unauthorized personnel. An unauthorized person is any person who does not have a need to know and who is not cleared or granted access to information at that level.

H-2. Access Requirements

- a. Prior to having access to classified information, all newly assigned personnel shall view, at a minimum, the HQDA DCS, G-2 initial online security training (and annual refresher training thereafter) located within the Army Learning Management System (ALMS) and any other organization-specific security training provided by their respective activity security manager.
 - b. Activity security managers will:
- (1) Verify the individual's security clearance eligibility utilizing the DOD security system of record, currently the Joint Personnel Adjudication System (JPAS), to ensure eligibility meets or exceeds the access requirement.
- (2) Ensure each civilian position sensitivity level posted within the DOD security system of record, currently the JPAS, is accurate.
- (3) Ensure the Table of Distribution and Allowances military security clearance requirement is correct. If the Table of Distribution and Allowances security clearance eligibility

requirement is lower than the military occupational specialty held by the military individual, activity security managers will ensure the eligibility remains current based off of the individual's military occupational specialty.

- (4) Coordinate with the supervisor and civilian/military personnel representative for any position sensitivity or security clearance requirement changes.
- (5) Ensure a SF 312 (Classified Information Nondisclosure Agreement) has been executed and JPAS annotated accordingly prior to the individual having access to classified information.
- (6) Forward the executed original SFs 312 to the respective military/civilian personnel office for upload into the individual's personnel electronic records management system, and verify the SF 312 has been successfully uploaded and is legible.
- (7) Take JPAS "ownership" of all permanent party military and civil service personnel and consultants specifically working for or within their respective organization.
- (8) Take a JPAS "servicing" relationship for Reserve and National Guard military personnel and contractors working for or within their respective organization.
- (9) Post the U.S. and NATO accesses as well as the IT access within JPAS once eligibility and access requirements are met.
- c. If an individual's security clearance eligibility does not meet position requirements or is outdated, a SF 86 (Questionnaire for National Security Positions) via electronic Questionnaires for Investigations Processing (e-QIP) will be initiated to either upgrade or update the security clearance eligibility, whichever is required.
- d. Personnel will be notified at least 60 days in advance of their security clearance eligibility update requirement to start gathering the required data. The Information Protection Office, 633 Air Base Wing, Fort Eustis, will be notified the first week of each month of those personnel whose U.S. accesses will require updating for that specific month.
- e. Prior to granting any interim security clearance eligibility/access, completion of local records checks is required.
- f. Personnel security investigations are not authorized if an individual (excluding a General Officer) is retiring or separating from government service within 12 months.

H-3. Care During Working Hours

a. Classified material removed from storage will be kept under constant surveillance and control by authorized personnel. Classified document cover sheets, SF 703, 704, and 705 (Top Secret, Secret, and Confidential Cover Sheets, respectively) will be placed on classified documents or files not in secured storage.

- b. SF 702 (Security Container Check Sheet).
- (1) A SF 702 will be displayed on each GSA-approved security container, approved open storage area, and active secret Internet protocol router network (SIPRNET) lock box. Organizations having such storage will record the date and time of each instance when a container/area/box is opened and closed and the initials of the individual(s) doing so.
- (2) At the end of each business day, a person will double check the container/area/box to make sure it is properly secured. This person will record the time the container/area/box was checked and initial the form.
- (3) Security containers/areas/boxes not opened during the workday will also be checked at the end of the work day and the action recorded on the SF 702.
- (4) The SF 702 will be retained at least 24 hours following the last entry unless there has been an incident reported during the period. Retain the SF 702 for 60 days, at a minimum, after the incident report has been finalized.
- (5) Reversible OPEN-CLOSED or OPEN-LOCKED signs will be utilized on each security container and open storage area.
- (6) If connectivity to a specific SIPRNET lock box is inactive, an end-of-day check is not required for that specific box; however, a notice will be placed on the outside of the SIPRNET lock box stating that the SIPRNET is inactive along with the inactive date and the responsible party's initials.
- (7) Each TRADOC organization having the responsibility for a conference and/or team room will complete at the end of each work day a security check of each conference and team room utilizing a SF 701 (Activity Security Checklist). The organization is also responsible for completing the SF 702 for any active SIPRNET lock box and AV open storage area located within the conference/team room.
- (8) Building 950 access control/front desk personnel will complete end-of-day security checks for all SIPRNET rooms in Building 950, Fort Eustis, as well as Room 1901B. The SF 702 will be utilized for such checks.
- (9) The following organizations have the responsibility for completing end of day checks utilizing the SF 702 for SIPRNET rooms located within Building 661, Fort Eustis:

<u>Organization</u>	SIPRNET Rooms
Office of the TRADOC DCS, G-6	162 and 400
Office of the TRADOC DCS, G-8	255
Office of the TRADOC DCS, G-1/4	361

(10) The USACIMT Operations will complete end-of-day checks for all SIPRNET rooms in Building 210, Fort Eustis. The SF 702 will be utilized for such checks.

(11) The Operational Environment Training Support Center will complete end-of-day checks for all SIPRNET rooms in Building 601, Fort Eustis. The SF 702 will be utilized for such checks.

c. SF 700 (Security Container Information).

- (1) Activity security managers will utilize and maintain the SF 700 for each security container, approved open storage area, and SIPRNET lock box within their respective organization. The SF 700 provides the location of the container/area/box, and the names, home addresses, and home or cell phone numbers of the individuals having access to the container/area/box.
- (2) The completed Part 1, SF 700, will be placed in a sealed opaque envelope to protect personally identifiable information (PII). This envelope will then be posted on the inside of the locking drawer/door.
- (3) The completed Parts 2 and 2A, SF 700, will be marked with the highest classification authorized for each security container, approved open storage area, and SIPRNET lock box. Part 2A will be detached and inserted in the Part 2, SF 700, envelope, and the envelope shall be sealed.
- (4) The classification authority block shall state on the back of each Part 2, SF 700, "Derived From: 32 CFR 2001.80(d)(3)" and "Declassify: Upon Change of Combination."
- (5) Part 2, SF 700, will then be secured in a separate security container approved for the storage of classified information and treated as information having a classification equal to the highest classification level of the classified information that is accessed in the security container/open storage area/SIPRNET lock box. If there is not a second security container, the SF 700 will be maintained by the Office of the DCS, G-2 Security.

d. SF 701 (Activity Security Checklist)

- (1) Activity security managers will utilize and maintain the SF 701 for each area containing at least one SIPRNET box. The first item on the Activity Security checklist will be "Security containers have been locked and checked." Security containers include GSA-approved safes and all SIPRNET boxes in the area.
- (2) The SF 701 will log the inspection of the security containers along with other end-of-day checks in the area. The SF 701 must be kept on record for a minimum of one year.
- e. Unattended, Open Security Containers/Open Storage Area/SIPRNET Box.
- (1) A person discovering an unattended security container, open storage area, or active SIPRNET box will keep the container/area/box under guard/surveillance and notify one of the persons listed on Part 1, SF 700 and the respective activity security manager. If one of the individuals cannot be contacted, the HQ TRADOC Emergency Operations Center will be notified.

- (2) The individual contacted will report to the location, and check the contents for visible indications or evidence of tampering, theft, or compromise. If there is evidence of tampering, theft, or compromise, the respective activity security manager will determine the nature of the tampering and whether the security lock is operating properly.
- (3) The activity security manager will change the combination and lock the container/area/box. If the combination cannot be changed immediately, the container/area/box will be locked and placed under guard until the combination can be changed, or the classified contents will be transferred to another container or secure area.
- (4) A preliminary inquiry is required for all security incidents. Refer to Appendix Y and Volume 3, DOD Manual 5200.01, for further details.

H-4. After-Duty-Hours Unannounced Inspection

- a. After-duty-hours security checks may be conducted for the purpose of detecting improperly secured classified information.
- b. Each military member and civilian employee will be provided in advance, written notification of after-hours inspections conducted by HQ TRADOC DCS, G-2 security personnel.
 - c. After-hours inspections will include, but is not limited to:
 - (1) Offices and cubicles.
 - (2) Desks.
 - (3) Trash receptacles.
 - (4) Copier areas.
 - (5) Shredder areas.
 - (6) Conference and team rooms.
 - (7) Common areas.
- d. Any unauthorized items found by HQ TRADOC DCS, G-2 security personnel during inspections may be turned over to Fort Eustis law enforcement officials. The TRADOC Command Provost Marshal and the TRADOC HQ Office of the Staff Judge Advocate may also be notified upon discovery of such items. As needed, the HQ TRADOC DCS, G-2 will consult with the TRADOC HQ Office of the Staff Judge Advocate prior to performing unannounced inspections to ensure the inspections will not violate an employee's rights or violate terms of a labor contract.

Appendix I Emergency Planning

I-1. Emergency Planning

- a. To minimize the risk of compromise, an emergency plan will be developed to protect, remove, and/or destroy classified material in case of fire, flood, earthquake, other natural disasters, civil disturbance, terrorist activities, or enemy action.
- b. The activity security manager will post the emergency plan in, on, or near each security container and approved open storage area within their respective organization. To serve a group of containers, one plan will be posted in the vicinity of the containers.
- c. Activity security managers will ensure emergency plans are approved, posted accordingly, and reviewed by security custodians at least annually.

I-2. Emergency Plan Example

An example of an emergency plan is at Figure I-1.

U.S. ARMY TRAINING AND DOCTRINE COMMAND (TRADOC) EMERGENCY EVACUATION AND DESTRUCTION PLAN

- 1. REFERENCES. Volume 3, DOD Manual 5200.01, DOD Information Security Program, and AR 380-5, Department of the Army Information Security Program.
- 2. PURPOSE. To prescribe procedures and assign responsibility for the emergency evacuation or destruction of classified material within (INSERT ORGANIZATION), U.S. Army TRADOC, in the case of fire, natural disaster, civil disturbance, terrorist attack, or imminent hostilities, to minimize the risk of its compromise.
- 3. APPLICABILITY. This plan applies to (INSERT ORGANIZATION).
- 4. SCOPE. This plan prescribes procedures for the emergency evacuation or destruction of classified material within (INSERT ORGANIZATION), defines responsibility of personnel for executing this plan, and provides authority and guidance for implementation.

5. RESPONSIBILITIES.

- a. The Commanding General, TRADOC, or his designated representative, is the implementing authority for this plan.
- b. (INSERT ORGANIZATION) Directors or designated representatives are responsible for implementing Paragraph 6.b.(4) below.
- c. All personnel listed on the SF 700 (Security Container Information) are responsible for the implementation of this plan.

6. PROCEDURES.

- a. The responsible recipient will review all classified material for proper disposition, retention, destruction, classification/markings, or transfer.
- b. Fire. To ensure risk of injury or loss of life is minimized, the following actions will be taken in regard to classified material:
- (1) For safety reasons, if there is little reaction time, leave classified material in place, even if you have a valid courier card and are authorized to transport the classified documents.
 - (2) Secure classified containers unless there is no time to do so.
 - (3) If possible, remove and safeguard any classified document accountability records.
- (4) Designate and train authorized personnel to position themselves at selected locations around the affected area for the prevention of unauthorized removal of classified material.

Figure I-1. Emergency Plan Example

c. Natural Disasters.

- (1) Tornadoes. If time permits, secure all classified material within classified containers, and remove and safeguard any classified document accountability records.
- (2) Flooding. Move classified material and equipment to a location to ensure protection. Disconnect all electrical equipment from electrical outlets, and place the equipment above floor level by placing on desktops, cabinets, tables, etc.
- d. Civil Disturbances. Secure classified material in appropriate security containers and post knowledgeable individuals at each entrance to control access. If the seriousness of the situation warrants, the Commanding General, TRADOC, or his designee will request Security Forces, Fort Eustis, to provide security.
- e. Terrorist Activities/Imminent Hostilities. Unless otherwise directed or when emergency removal is impractical due to the volume of classified material, (INSERT ORGANIZATION) personnel will ensure classified material is secured in authorized security containers, and all outside entrances into the area are secured. Total destruction will occur only at the direction of the Commanding General, TRADOC, his designated representative, or the TRADOC Command Security Manager.
- f. In situations not specifically anticipated by this plan or when circumstances warrant it, the senior individual present in an office containing classified material may deviate from procedures in this plan. Any deviation will be within basic security principles and guidelines.
- g. When emergency evacuation or destruction procedures are complete, reconcile all accountable records, conduct a 100 percent inventory of accountable classified documents and material, and report immediately to the TRADOC Command Security Manager any discrepancies.
- h. A copy of this plan will be posted in/on/near each security container and approved secure open storage areas and near a group of security containers.
- 7. IMPLEMENTATION. Implement the provisions of this plan on the order of the Commanding General, TRADOC, his designated representative, or the TRADOC Command Security Manager.
- 8. COORDINATING INSTRUCTIONS. Questions regarding this plan should be referred to the (INSERT ORGANIZATION) security manager, (INSERT PHONE NUMBER), or HQ TRADOC DCS, G-2 Security.

Figure I-1. Emergency Plan Example, continued

Appendix J Classified Discussion

J-1. Classified Discussions

- a. Classified discussions are not permitted in personal residences, in public, in public transportation conveyances (airplane, taxi, etc.), or in any area outside approved spaces on a U.S. Government or cleared contractor facility. Written requests for exception to policy will be forwarded to the TRADOC Command Security Manager.
- b. Classified discussions will only be discussed in closed offices, team rooms, conference rooms, and open storage areas located throughout TRADOC facilities. Steps will be taken to ensure individuals that are uncleared or do not have a need to know do not hear classified discussions.

J-2. Telephone Equipment Requirements

- a. In telephone conversations, classified information will only be discussed over secure communication equipment.
- b. All non-secure telephones will have a DD Form 2056 (Telephone Monitoring Notification Decal) affixed, advising the user that the telephone is subject to monitoring at all times and use constitutes consent to monitoring.
- c. All secure telephones will have a DD Form 2056 affixed minus the top portion, "Do Not Discuss Classified Information."

Appendix K Removal of Equipment

K-1. Equipment Inspection

- a. Security containers and IT equipment used to store or process CUI and/or classified information will be inspected by cleared personnel before removing from protected areas, TRADOC facilities, and/or before unauthorized persons are allowed unescorted access to them.
- b. This inspection ensures no CUI or classified information remains within or on the equipment. Items to be inspected include security containers, reproduction equipment, facsimile machines, printers, IT equipment, destruction equipment, and other equipment used for safeguarding or processing CUI and/or classified information.
- c. Desks, cabinets, and other furniture items located in protected areas where CUI or classified material is routinely accessed will be inspected to ensure the items are free of CUI or classified material before removing from protected area.
- d. A written record of the inspection will be completed and retained by the respective activity security manager for 2 years.

K-2. Exceptions

Where equipment cannot be properly sanitized or an appropriately knowledgeable escort provided, cleared maintenance technicians shall be used. Equipment parts will be replaced and destroyed when CUI or classified information cannot be removed from the equipment. Markings and labels will be removed from sanitized equipment and media after inspection and prior to removal from protected area.

Appendix L Classified Visits

L-1. Classified Visits Within DOD

- a. TRADOC personnel visiting other Army commands, other U.S. Government agencies, and/or U.S. Government contractor facilities will provide advance notification of any pending visit that is anticipated to involve access to classified information.
- b. The JPAS will be utilized to verify/provide an individual's security access level. Activity security managers will submit classified visit requests for respective personnel via JPAS.
- c. The activity security manager of the DOD individual visiting a TRADOC organization is responsible for submitting a classified visit request to the appropriate TRADOC-designated JPAS security management office. The responsible activity security manager will verify the visit request and coordinate with the respective host to validate the requirement and need to know.
- d. The activity security manager and/or host will also provide advance written notification of pending visitor(s) to the Front Desk, Building 950/661, Fort Eustis, for badge issuance purposes.
- e. TRADOC personnel will ensure individuals visiting TRADOC activities who require access to classified information have the appropriate security access level and need to know prior to granting classified material access.
- f. Visit requests can be approved, denied, or rescheduled at the option of the command/agency/company being visited.

L-2. Classified Visits Outside DOD

Activity security managers of personnel outside DOD will forward written classified visit requests to the TRADOC respective activity security manager and will include:

- a. Visitor's full name, date and place of birth, social security number, and rank or grade.
- b. Visitor's security clearance and any special access authorizations required for the visit. Security clearance information will include security clearance level, date clearance granted, type of investigation completed, and investigation completion date.

- c. A signature (digital accepted) from their activity security manager or official other than the visitor who is in a position to verify the person's security clearance.
 - d. The TRADOC host point of contact and phone number.
- e. The purpose of the visit in sufficient detail to establish an assessment of need to know and necessity of the visit.
- f. The date and duration of the proposed visit. Intermittent visits on the same visit request are authorized for up to one year, when stated on the request and approved by the TRADOC organization to be visited.

L-3. Department of Energy (DOE) Classified Visits

- a. TRADOC individuals visiting a DOE facility will coordinate with their respective activity security manager for completion of the DOE Form 5631.20.
- b. The activity security manager will forward the DOE Form 5631.20 to HQ TRADOC DCS, G-2 Security for approval signature from the TRADOC DCS, G-2, the TRADOC Deputy G-2, or the TRADOC Command Security manager.

L-4. TRADOC In-House Contractors

- a. TRADOC activities may maintain a current classified visit certification on file for all contractor personnel having access to government classified material; however, the contractor Facility Security Officer (FSO) is under no obligation to provide such certification if the FSO has implemented and populated contractor personnel security data and access levels within JPAS.
- b. Contractor classified visit requests are valid until contract end date or a date specified within the classified visit request, whichever date occurs first.

L-5. TRADOC secret Internet protocol router network (SIPRNET) and audio/visual (AV) Classified Open Storage Areas

- a. Outside visitors and in-house contractors requiring access to the TRADOC SIPRNET and AV classified open storage areas will have their respective activity security manager forward a visit request to the TRADOC security management office code W3YTAASRAV.
- b. In-house AV contractors will read and sign the SIPRNET and AV classified open storage area acknowledgement (Figure L-1) prior to gaining access to any TRADOC SIPRNET and AV classified open storage area, and provide the executed acknowledgement to the HQ TRADOC Facilities Management Office (FMO).

- c. The HQ TRADOC FMO will:
 - (1) Verify need to know;
 - (2) Maintain in-house contractor AV acknowledgements;
 - (2) Grant access on an as needed basis; and
- (3) Provide the Front Desk, Bldg 950/661 a copy of each SIPRNET/AV visit request (minus PII information).
- d. The HQ TRADOC FMO is also responsible for updating/changing the SIPRNET and AV classified open storage area combination locks and updating the SFs 700 accordingly. Copies of current SF 700 authorization lists and classified open storage area approvals will be maintained inside each SIPRNET/AV open storage area as well as the Front Desk, Buildings 950 and 661.

HQ TRADOC

SIPRNET and Video Teleconference (VTC)/Audio Visual (AV) Classified Open Storage Area Acknowledgement

(Print Name)	is authorized to access the following HQ TRADOC
SIPRNET and/or VTC/AV classified	open storage area(s):
(Insert Appropriate SIPRNET and/or	VTC/AV open storage areas)
•	ow acknowledgement and return it to the HQ TRADOC or receiving combination locks, alarm pin, and hard keys.
(Facilities Management Office Signat	,
HQ TRADOC classified open storage	received the classified SECRET combinations to the above e areas and have been issued a pin for the areas' alarm ombinations and pins are secured in a GSA-approved safe.
I have been trained on how to operate combination locks.	e the areas' alarm system and X-09 electro-magnetic

Figure L-1. Secure Internet protocol router network (SIPRNET) and AV Classified Open Storage Area Acknowledgement

Prior to entering a classified open storage area, I will sign for a key at the HQ TRADOC

Building 950/661 Front Desk, and return it to same when finished.

I will notify the HQ TRADOC Building 950/661 Front Desk at 501-5007/7154, respectively, each time I arm or disarm a classified open storage area.

I am responsible for completing the SF 702 (Security Container Check Sheet) provided on the outside of each classified open storage area's door upon opening and security the area.

I am responsible for securing the classified open storage areas (activating the alarm and locking the X-09 and key locks) each time I exit the area.

If I am unable to secure the alarm correctly, I will notify the HQ TRADOC Building 950/661 Front Desk immediately so that they may notify the installation military police to prevent them from responding and charging the command unnecessarily.

I will notify the HQ TRADOC Facilities Management Office when I depart, no longer require access, or no longer require an alarm pin for the classified open storage areas.

I will notify the HQ TRADOC Facilities Ma	C	HQ TRADOC DCS, G-2
Security if a possible compromise has occur	red.	
Signature	Date	_

Figure L-1. SIPRNET and AV Classified Open Storage Area Acknowledgement, continued

Appendix M Classified Venues

M-1. Classified Venues

- a. Meetings, conferences, classes, seminars, symposia, and similar activities at which classified information is to be presented or discussed are considered classified meetings.
- b. The classified portions of these meetings present special vulnerabilities to unauthorized disclosure and will be limited to persons possessing an appropriate security clearance and access and the need to know for the specific information involved.
- c. Security requirements contained within this memorandum, AR 380-5, and DOD Manual 5200.01 apply, without exception, to classified meetings.

M-2. Venue Requirements

The TRADOC organization responsible for a classified meeting/conference held within TRADOC facilities will:

a. Verify security clearance access utilizing JPAS and need to know.

- b. Ensure written classified visit requests for personnel outside DOD are in accordance with this memorandum and DOD Manual 5200.01.
- c. Ensure all personnel attending the meeting/conference are wearing the appropriate badge issued by the Front Desk, Building 950/661, Fort Eustis.
- d. Complete the classified checklist (Figure M-1) provided within each conference and team room outside of classified open storage areas, Sensitive Compartmented Information Facilities (SCIF), and the Special Access Program (SAP) facility. This checklist will assist each host with their security responsibilities before, during, and after a classified meeting.
- e. Provide the completed classified conference room checklist to their respective activity security manager to maintain for 60 days thereafter. The checklist will provide insight to the responsible organization and its activity security manager should a security incident arise during/after the meeting/conference.
- f. Refer to Enclosure 2, Volume 3, DOD Manual 5200.01, for additional classified meetings/conference security requirements.

M-3. Security Checklist for Classified Conferences/Meetings

a. The organization hosting a TRADOC classified conference/meeting within TRADOC facilities is responsible for all security requirements before/during/after the classified conference/meeting. The host will complete the security checklist at Figure M-1 by initialing each security requirement to reflect completion or entering "N/A" for those security requirements that did not apply. The completed security checklist will be provided to the activity security manager at the end of the conference/meeting.

HQ TRADOC Security Checklist for Classified Conferences/Meetings

Host Organization:	Date:			
Individual Responsible:	Room #:			
(Print Name)				
1 Determine highest level of classification to include	e special access, i.e., NATO/critical			
nuclear weapons design information.				
2 Determine storage capabilities before, during, and				
3 Ensure all entry/exit doors and first floor area wind	Ensure all entry/exit doors and first floor area window blinds are closed.			
4 Ensure area is checked prior to conference/meeting	g for unauthorized items, i.e.,			
recording devices.				
5 Ensure marquee or a sign posted outside the classif				
security classification level. Clear marquee/sign upon confer				
6 Contact activity security manager to open SIPRNE				
7 Ensure IT equipment used to process or project cla	ssified information is approved for			
the classified level provided/discussed.				
8 Verify via JPAS security clearance access of all att				
classification level and any special access requirements, and	verify need-to-know prior to			
conference/meeting.				
9 Establish method to identify cleared attendees for e	•			
10 Ensure cellular phones, radios, tape or digital recor	•			
tronic device that can transmit or record, are not allowed wit				
11 At the beginning of conference/meeting, announce	<u> </u>			
attendees and provide security procedural guidelines to atten				
12 Ensure classified material provided is appropriately				
13 Ensure any notes taken during classified discussion	is are safeguarded, marked, and			
transmitted appropriately.	lunch maniada			
14 Protect classified materials during any breaks and 1				
15 After conference/meeting, ensure area is checked f16 Ensure SIPRNET lock box is secured and SF 702 i				
17 Ensure audio visual room within conference room				
17 Elisule audio visual foolii within conference foolii	is secured.			
Figure M-1. Security Checklist for Classified	Conferences/Meetings			
·	5			

Appendix N Information Processing Equipment

N-1. Information Processing Equipment

a. There is a variety of non-communications security equipment used to process classified information, including copiers, facsimile machines, computers, notebooks, and other IT equipment and peripherals, typewriters, hand-held personal data managers, etc.

b. Any TRADOC equipment used to process classified information that may retain all or part of the classified information shall be identified and include the overall level of classified information processed and any retention capabilities.

N-2. Equipment Certification/Accreditation

- a. Digital copiers, printers, scanners, faxes, and similar information system devices employ embedded hard drives or other media that may retain residual CUI or classified information. These devices will be included as part of the certification and accreditation process. Classified retention equipment, i.e., drum, printer cartridge, used outside of an open storage area will be safeguarded and maintained in a GSA-approved security container when not in use.
- b. Cleared and technically qualified personnel will inspect and sanitize the equipment before the equipment is removed for service/turn-in.
- c. Replaced equipment parts shall be destroyed when removed or placed, as an alternative, within an open storage area approved for the storage of classified information at that classification level.

N-3. Equipment Approval

Each activity security manager will post notice on or near IT equipment approved for classified use within their respective organization. The activity security manager will also post notice on or near IT equipment that is not approved for classified use.

N-4. Information Technology (IT) Access Requirements for Foreign Nationals Access to IT equipment by foreign nationals will be in accordance with AR 25-2.

Appendix O Receipt of Classified Material

O-1. Mail Room – Incoming Accountable Mail

- a. The Classified Mail Room, Mail and Distribution Center, 1321A Lee Boulevard, Fort Eustis, will accomplish the handling and processing of accountable mail (insured, certified, and registered mail articles) and classified distribution.
- b. Incoming accountable mail and classified correspondence will be handled and processed as follows:
- (1) Only authorized personnel with the appropriate security clearance will sign for accountable/classified material.
- (2) Each piece of accountable/classified mail received will be inspected for damage prior to acceptance.
- (3) Accountable/classified material receipts (normally a DA Form 3964, Classified Document Accountability Record) will be checked to ensure the material listed on the receipt has

been received. The recipient will sign and forward the receipt acknowledgement to the originator. The activity security manager will retain a copy of the receipt for 2 years.

- (4) Accountable/classified materials will be properly secured when not in use.
- (5) TRADOC personnel authorized to receive accountable/classified material will safeguard all incoming mail marked "POSTMASTER: RETURN SERVICE REQUESTED" until such mail is opened and inspected for classified material.
- (6) Personnel who inadvertently receive classified mail will immediately contact their respective activity security manager.

O-2. Mail Room – Outgoing Accountable Mail

- a. Outgoing accountable mail and classified material will be handled and processed as follows:
- (1) Outgoing accountable/classified material will be stored in a GSA-approved storage container or certified open storage area until such material is handcarried to the Classified Mail Room, Mail and Distribution Center, 1321A Lee Boulevard, Fort Eustis, for final processing.
- (2) Only authorized personnel with the appropriate security clearance and DD Form 2501 (Courier Authorization Card) will hand-carry accountable/classified material to the Classified Mail Room, Mail and Distribution Center, 1321A Lee Boulevard, Fort Eustis.
- (3) A DA Form 3964 (original plus two copies) will accompany the material along with two pre-addressed address labels.
- (4) The activity security manager will maintain for 2 years the executed DA Form 3964 from the recipient. A copy of the executed DA Form 3964 will be provided to the Classified Mail Room, Mail and Distribution Center, 1321A Lee Boulevard, Fort Eustis.
- b. Activity security managers will ensure current signature authority cards for those personnel designated to receive/drop-off accountable/classified material are provided to the Classified Mail Room, Mail and Distribution Center, 1321A Lee Boulevard, Fort Eustis, in a timely manner.
 - c. The DD Form 2501 may be issued for 2 years to cleared, authorized classified couriers.

Appendix P Accountability

P-1. Collateral Top Secret, Secret, and Confidential Information/Material

a. Collateral Top Secret, Secret, and Confidential information/material originated, received, distributed, or routed within HQ TRADOC will be protected by measures outlined in this memorandum and its references.

- b. Within TRADOC, collateral Top Secret, Secret, and Confidential information will be kept to a minimum and retained for only as long as the information/material is needed.
- c. Except for controlled/accountable collateral classified material, such material may be transferred within HQ TRADOC organizations without utilizing a DA Form 3964.
- d. A DA Form 3964 will be utilized for collateral Top Secret, Secret, and Confidential information/material forwarded outside HQ TRADOC, to include local agencies and contractors. This same form will be utilized when transmitting such information over secure facsimile devices.
 - e. The executed DA Form 3964 returned by the recipient will be maintained for 2 years.

P-2. North Atlantic Treaty Organization (NATO) and Foreign Government Material

NATO classified information shall be controlled and safeguarded in accordance with U.S. Security Authority for NATO Instruction 1-07. Safeguard foreign government information in accordance with Enclosure 2, Volume 3, DOD Manual 5200.01. Contact HQ TRADOC DCS, G-2 Security for further guidance.

P-3. Working Papers

Working papers are documents and materials created during development and preparation of a finished product and are not intended or expected to be disseminated. Working papers will be:

- a. Dated when created.
- b. Marked with the highest classification of any information contained therein.
- c. Safeguarded as required for the assigned classification.
- d. Conspicuously marked as WORKING PAPERS on the cover and/or first page of the document or material.
 - e. Destroyed appropriately and when no longer needed.
- f. If retained for more than 180 days, filed permanently, emailed within or outside TRADOC, or released outside of TRADOC, mark and control as if the document/material is a final product. Consult Enclosure 2, Volume 2, DOD Manual 5200.01, for exceptions.

Appendix Q Reproduction

Q-1. Reproduction

- a. Documents and other material containing classified information will be reproduced only when necessary for the accomplishment of TRADOC's mission or for compliance with applicable statutes or directives.
- b. Reproduction equipment and its process involve substantial risk; therefore, the reproduction of classified material will be limited to that which is mission essential, and countermeasures will be taken to negate or minimize any risk.
- c. All copies of classified documents are subject to the same safeguards and controls prescribed for the document from which the reproduction is made. Reproduced material will be clearly identified as classified at the applicable level.
- d. Waste products generated during reproduction will be properly safeguarded to the level of classification contained within until such time it can be destroyed in an approved manner at the appropriate classification level.
- e. Personnel who operate this equipment will be made aware of the risks involved with the specific equipment and the procedures concerning the protection, control, accountability, and destruction of reproduced classified information/material.
- f. Foreign government information will not be reproduced and will be controlled pursuant to guidance and authority granted by the originating government.

Q-2. Reproduction Equipment Approval

- a. Requests for approval for equipment to reproduce classified information will be forwarded through HQ TRADOC DCS, G-2 Security and to the TRADOC Command Security Manager for approval. Written approval with procedures signed by the TRADOC Command Security Manager will be posted on/near the reproduction equipment authorized to reproduce classified material.
- b. Reproduction equipment which leaves latent images in the equipment or on other material will not be authorized to reproduce classified material unless:
 - (1) The equipment is in an approved open storage area;
 - (2) The equipment is protected as classified material; and
 - (3) The material on which the image resides is destroyed as classified waste.

Q-3. Controlled Reproduction

Except for the controlled initial distribution of information processed or received electronically, or that containing communications security or SCI which are governed by separate policies, reproduction of classified accountable information, i.e., NATO Secret, will be strictly controlled. Contact HQ TRADOC DCS, G-2 Security for guidance.

Appendix R Disposition and Destruction

R-1. Disposition and Destruction

- a. Classified and CUI documents and materials will be retained only if they are required for effective and efficient TRADOC operations or if retention is required by law or regulation.
- b. Annually, TRADOC organizations shall review their classified holdings and destroy classified information no longer required/needed for TRADOC operations. Activity security managers will document and maintain the number of inches/feet destroyed each fiscal year and at each classification level, i.e., Confidential, Secret, and Top Secret.
- c. Classified materials which are no longer required will be disposed of in accordance with the provisions of the Federal Records Act as implemented by AR 25-30. Special care will be exercised in the placing of classified information in files designated as "permanent." Volume 1, DOD Manual 5200.01, provides guidelines for permanent retention of classified material.

R-2. Destruction Equipment

- a. Classified documents and materials will be destroyed by pulverizing, cross-cut shredding utilizing approved Class 1 high security cross-cut shredders, or mutilation to preclude recognition or reconstruction of the classified information.
- b. Activity security managers will post notice on each shredder to warn the user as to whether or not the shredder is authorized to shred classified information. The SFs 707 and 710, Secret and Unclassified labels, respectively, may be used for this purpose.
- c. Strip shredders that do not have a half-inch cross cut feature do not sufficiently destroy the information and are not authorized for use to destroy classified information.
- d. Activity security managers will coordinate with the Fort Eustis Recycle Center, 1209 Taylor Avenue, Fort Eustis, to schedule the use of the shredders and degaussers for destroying CUI and classified information and IT equipment as needed.

R-3. Destruction Records

a. Records of destruction are required for NATO Secret and Foreign Government documents and material. A DA Form 3964 may be used for this purpose. Records of destruction will be maintained for 5 years from the date of destruction. Contact HQ TRADOC DCS, G-2 Security for destruction and retention standards for NATO classified materials.

- b. Records of destruction are required for Top Secret documents and material.
- c. Records of destruction are not required for Secret material.
- d. Records of destruction are not necessary for Confidential materials unless required by the originator.

Appendix S Waivers

S-1. Waivers

- a. Waivers to the information security program requirements outlined within this memorandum are granted only on a case-by-case basis where there is a unique or unusual situation/factor requiring deviation from this memorandum and its references. Request for waivers will be submitted through the TRADOC Command Security Manager and addressed to the Commanding General, TRADOC for approval.
- b. Deviations will be based on the consideration of risk management factors, i.e., criticality, sensitivity, information value, analysis of the known and anticipated threat, vulnerabilities to exploitation, and countermeasure benefits versus cost (monetary and to national security).

S-2. Waiver Revalidation Requirements

Waivers must be revalidated no less than ever 5 years and will require re-justification of the unique or unusual circumstances.

Appendix T Inspections

T-1. Self Inspections

Activity security managers will conduct self-inspections within his/her area of responsibility involving classified and CUI materials. Such inspections are to evaluate and assess the effectiveness and efficiency of the TRADOC information security program. Written security self-inspection results will be maintained until the next comparable inspection.

T-2. Fort Eustis Security Inspections

The Information Protection Office, 633 Air Base Wing, Fort Eustis, will conduct information security program inspections of HQ TRADOC organizations located at Fort Eustis. Written notification of such inspection will be forwarded to the organization at least 60 days prior to the inspection. Activity security managers will forward a copy of the inspection results to HQ TRADOC DCS, G-2 Security.

T-3. TRADOC Security Assistance Visits

Activity security managers may contact HQ TRADOC DCS, G-2 Security at any time to have a security assistance visit conducted within their respective organization. Available security

assistance visits include personnel, information, industrial, and communications security programs, NATO security program, and the foreign disclosure program.

Appendix U Storage

U-1. Storage

Classified information that is not under the personal control and observation of an authorized person is to be guarded or stored in a secured, GSA-approved security container or approved secure open storage room, pursuant to the level of classification and DOD Manual 5200.01.

U-2. Top Secret Storage

Top Secret information will be stored as follows:

- a. GSA-approved security container with one of the following supplemental controls:
- b. An employee cleared to at least the Secret level shall inspect the security container once every 2 hours.
- c. The location that houses the security container is protected by an Intrusion Detection System (IDS) meeting the requirements contained within Volume 3, DOD Manual 5200.01, with personnel responding to the alarm within 15 minutes.
- d. In a GSA-approved security container with an electro-magnetic lock (e.g., X-09) and within an area having security-in-depth.
- e. In an open storage area constructed in accordance with Volume 3, DOD Manual 5200.01 and equipped with an IDS with personnel responding to an alarm within 15 minutes of the alarm annunciation if the area has been determined to have security-in-depth or within 5 minutes of alarm annunciation without security-in-depth.
 - **f.** In a vault as specified in DOD Manual 5200.01.

U-3. Secret Storage

Secret information will be stored either:

- a. In the same manner as Top Secret information;
- b. In a GSA-approved security container or vault without supplemental controls; or
- c. In approved classified open storage areas meeting the requirements outlined in Volume 3, DOD Manual 5200.01, having security-in-depth, and either:
- (1) An employee cleared to at least the Secret level shall inspect the open storage area once every 4 hours; or

(2) An IDS meeting Volume 3, DOD Manual 5200.01, requirements with personnel responding to the alarm within 30 minutes.

U-4. Confidential Storage

Confidential information will be stored in the same manner as Top Secret or Secret information except that supplemental controls are not required.

U-5. Specialized Security Equipment

Specialized Security Equipment includes:

- a. GSA-approved two, four, and five drawer security containers will be used to store classified information and materials.
- b. GSA-approved map and plan file security containers may be utilized for storage of odd-sized items such as computer media, maps, charts, and classified equipment.

U-6. Unauthorized Storage

Unrelated unclassified documents or equipment, i.e., cash, keys, jewelry, personal protection equipment, will not be stored in security containers in which classified material is stored.

U-7. Residential Storage

Classified information will not be stored in a personal residence, on or off Fort Eustis. Classified information will not be stored in any location outside an approved U.S. Government location or cleared contractor facility. Exceptions follow:

- a. In extreme and exceptional situations, the Commanding General, TRADOC, may approve an exception for the storage of Secret and below classified material for a General Officer whose residence is on Fort Eustis. Requests for exception to policy will be submitted through the TRADOC Command Security Manager, and addressed to the Commanding General, TRADOC.
- b. The Secretary of the Army is the only DA official that can authorize the removal of Top Secret materials from designated work areas for temporary storage outside a U.S. Government or cleared contractor facility, to include the storage at a personal residence on a U.S. Government facility.

U-8. Equipment Designations

- a. There will be no external markings revealing the level of classified information authorized to be or actually stored in a given container or approved open storage area, or indicating the priority assigned to the container for emergency evacuation and destruction.
- b. Each security container will have the label GENERAL SERVICES ADMINISTRATION APPROVED SECURITY CONTAINER affixed to the front of the container, usually on the control or the top drawer.
- c. For identification/inventory purposes, each GSA-approved security container will bear an external, assigned number. Activity security managers having a GSA-approved security container are responsible for assigning such identification numbers and maintaining a current inventory of each.

- d. The assigned number, the SF 702, and the OPEN-CLOSED or OPEN-LOCKED signs, and the emergency evacuation/destruction plan are the only items permitted on the exterior of the security container and approved classified open storage area door.
 - e. The tops of the security containers will be kept clear.
- f. All security containers not authorized for classified storage will have the notation NOT AUTHORIZED FOR STORAGE OF CLASSIFIED INFORMATION affixed to the front of the security container.

U-9. Security Combinations

- a. Security combinations to security containers and approved classified open storage areas will be changed only by authorized individuals, trained security personnel, or a GSA-certified locksmith.
 - b. Combinations will be changed:
- (1) When the security container or approved classified open storage area door is placed in service.
 - (2) Whenever an individual knowing the combination no longer requires access.
 - (3) When compromise of the combination is suspected.
 - (4) At least annually.
- (5) When the container or approved classified open storage room door is taken out of service or is no longer used to store classified information, the combination shall be reset to the manufacturer standard combination 50-25-50 and a notice placed on the container/door confirming the manufacturer standard combination. Activity security managers will turn in any unused Sargent and Greenleaf SIPRNET padlocks with combination to HQ TRADOC DCS, G-2 Security.
 - c. Only a minimum number of authorized persons shall have knowledge of the combinations.
- d. New combinations will be tested several times before locking the security container/classified open storage area door to avoid the expense of a lock-out.

U-10. Repair of Damaged Security Containers

- a. Neutralization of lock-outs or repair of any damage that affects the integrity of a security container/approved classified open storage area will be accomplished only by authorized persons who have been the subject of a trustworthiness determination or are continuously escorted while so engaged.
- b. Unapproved modification or repair of security containers and approved classified open storage area doors is considered a violation of the container or door's integrity, and the GSA label will be removed. These safes/secure areas will not be used to protect classified information.

U-11. Maintenance and Operating Inspections

- a. Activity security managers will periodically inspect security containers and approved classified open storage area room doors and locks to ensure each are in good working order. Activity security managers will also schedule periodic maintenance for security containers and approved classified open storage area room doors and locks within their respective organization to detect and correct any problems in their early stages and define symptoms of developing problems. HQ TRADOC Facilities Management is responsible for scheduling periodic maintenance of SIPRNET and AV/VTC classified open storage area doors and locks.
- b. It is important to never use force to try to correct the problem. Critically needed materials will not be stored in containers showing any of the following symptoms, since they cannot be depended upon to open again:
 - (1) A dial that is unusually loose or difficult to turn.
 - (2) Any jiggling movement in the dial ring.
 - (3) Difficulty in dialing the combination or opening the container.
 - (4) Drawers rubbing against container walls.
- (5) Problems with opening/closing drawers, because the tracks or cradles need lubricant, material is jammed in behind the drawer, or the internal locking mechanism is tripped.
- (6) The control drawer handle or latch will not return to the locking position when the drawer is shut.
 - (7) The locking bolts move roughly, slip, or drag.

U-12. Turn-In or Transfer of Security Equipment

- a. In addition to having combinations reset before turn-in, security equipment will be inspected before turn-in or transfer by the activity security manager to ensure classified material is not left in the container.
- b. Each security container drawer will be removed and the interior inspected to ensure all papers and other materials are removed and the container is completely empty. The electromagnetic combination lock, i.e., X-09, will be removed or the combination will be changed back to the manufacturer combination 50-25-50 prior to the turn-in of the security container. Results of the inspection and combination lock will be recorded on a memorandum for record (MFR) and maintained for 2 years.
- c. Additionally, the activity security manager will contact the Environmental Element Office, Civil Engineer Division, 733d Mission Support Group, Fort Eustis, at (757) 878-7373, to inspect the security container for asbestos prior to turn-in.

- d. A copy of the above MFR, a copy of the Environmental Element Office asbestos report, and a completed DA Form 3161 (Request for Issue or Turn-In) will accompany the security container upon turn in to the Fort Eustis property book office, Building 1608, Fort Eustis.
- e. Contact the Civil Engineer Division service work order desk at (757) 878-5225 to transport the security container to the property book office.
- f. Shredders, other classified material destruction devices, copiers and facsimiles used for the reproduction and transmission of classified information, and furniture located within approved classified open storage areas rooms will be thoroughly inspected by the activity security manager prior to turn-in or transfer to ensure no CUI or classified material remains.

Appendix V

Physical Security Standards

V-1. Physical Security Standards

Detailed physical security standards for areas requiring the open storage of classified information are contained in the Appendix to Enclosure 3, Volume 3, DOD Manual 5200.01, to include:

- a. Construction standards.
- b. IDS standards.
- c. Access control requirements.

V-2. Classified Open Storage Standards

- a. Classified open storage areas will only be approved when storage in other approved security containers is not feasible due to the size, shape, or volume of material stored.
- b. A classified open storage physical security and structural inspections request will be forwarded to the Information Protection Office, 633 Air Base Wing, Fort Eustis. In turn, the Information Protection Office will contact the Security Forces Squadron physical security officer and the appropriate civil engineer department to conduct physical security and structural inspections of the proposed area.
- c. Upon completion of the physical security and structural inspections, a written request with justification for classified open storage approval will be forwarded to HQ TRADOC DCS, G-2 Security with the following documentation:
 - (1) Results of the completed physical security and structural inspections.
 - (2) Schematic drawing of the proposed open storage area.
- (3) Written security control and operating procedures for the proposed classified open storage area.

- d. The TRADOC Command Security Manager will provide written open storage approvals to those areas meeting regulatory requirements. Certifications are valid for 5 years or until structural modifications are made to the area, whichever comes first. The open storage approval will immediately terminate if structural modifications are made that degrade security.
- e. Activity security managers will coordinate with HQ TRADOC DCS, G-2 Security, the HQ TRADOC DCS, G-34, and the 633 Air Base Wing Information Protection Office on new construction and upgrades to existing facilities involving classified open storage areas or classified meeting sites to ensure all applicable security requirements are incorporated into the initial planning.
- f. Requests for deviations to classified open storage construction requirements will be forwarded through the TRADOC Command Security Manager and addressed to the Commanding General, TRADOC, for approval. Requests will include justification and proposed compensatory systems, controls, and procedures to properly protect classified information.

Appendix W Transmission

W-1. Transmission

- a. There are a variety of authorized, cost-effective transmission means for each level of classified information with minimal risk accessible within TRADOC facilities. A complete list of authorized ways to transmit/transport Top Secret, Secret, and Confidential materials are provided within Enclosure 4, Volume 3, DOD Manual 5200.01.
- b. Authorized persons transmitting or transporting classified information are responsible for ensuring the intended recipient is authorized access, have a need to know, and have the capability to store classified information.
 - c. Communications security material will be transmitted in accordance with AR 380-40.
- d. Computer and other IT systems used for transmitting classified information shall be approved and accredited through the DOD Information Assurance Certification and Accreditation Process.
- e. Complete guidelines for transferring classified information are contained within Enclosure 4, Volume 3, DOD Manual 5200.01.

W-2. Transmission of NATO Information

NATO Unclassified may be transmitted and stored via the non-secure Internet protocol router network utilizing encryption capability. The SIPRNET, Joint Worldwide Intelligence Communications System, U.S. Battlefield Information Collection and Exploitation Systems, and Combined Enterprise Regional Information Exchange System-International Security Assistance Force are the only authorized networks approved to transmit and store NATO Secret, NATO Confidential, and NATO Restricted information. Approval to process, transmit, and store NATO materials within the SIPRNET requires local accreditation approval from the Designated

Approval Authority, 7th Signal Command. Contact the HQ TRADOC DCS, G-2 Security for additional NATO requirements and information.

W-3 Transmission of Classified Information to Foreign Governments

Classified information originating in, or provided to or by the DOD may be disseminated to a foreign government or an international organization of governments, or any element thereof in accordance with AR 380-10. Prior to releasing any classified information to a foreign government, coordinate with the HQ TRADOC DCS, G-2 Foreign Disclosure Office.

Appendix X Handcarrying Classified Material

X-1. Handcarrying Classified Material

- a. Appropriately cleared personnel may be authorized to escort or handcarry classified material between locations when other means of transmission or transportation cannot be used.
- b. Handcarrying of classified material will be limited to situations of absolute necessity and will be carried out to make sure it does not pose an unacceptable risk to the information. Two-way handcarrying (carrying the material to and from the destination) is not authorized unless specific justification is provided.

X-2. Authorization to Handcarry Classified Information

- a. Handcarrying will be authorized when:
- (1) The information is not available at the destination and is required by operational necessity or a contractual requirement.
- (2) The information cannot be sent by secure electronic means, i.e., Secret-Army Knowledge Online, SIPRNET, secure facsimile transmission.
 - (3) The handcarry has been authorized and approved in writing.
- (4) The handcarry is accomplished aboard a U.S. carrier if at all possible, and the information will remain in the custody and physical control of the U.S. escort at all times.
- (5) Arrangements have been made in advance for secure storage during overnight stops and similar periods. The material will not be kept in hotels, personal residences, vehicles, or any other unapproved storage location.
- (6) A receipt for the material, for all classification levels, is obtained from an appropriate official at the destination, and a copy of the receipt is returned to the respective activity security manager.

X-3. DD Form 2501 (Courier Authorization Card)

- a. DD Form 2501 (Courier Authorization Card) will be used to identify appropriately cleared TRADOC military and civilian personnel who are authorized to handcarry classified material within the continental U.S. (CONUS), except when utilizing commercial aircraft. The activity security manager will issue a DD Form 2501 when:
 - (1) An individual has a recurrent need to handcarry classified information.
- (2) The individual has received a courier briefing (Figure X-1) and has provided a written acknowledgement of their understanding of the briefing (Figure X-2).
 - (3) The DD Form 2501 is completed and signed by the activity security manager.
- b. The DD Form 2501 may be issued for up to 2 years. The requirement to handcarry classified information will be revalidated prior to issuing a new courier authorization card.
- c. Contractor employees who are required to handcarry classified information will coordinate with their company's FSO for issuance of a DD Form 2501. Contractor employees will also notify the respective TRADOC activity security manager of the courier requirement.

Courier Authorization Briefing To Handcarry/Escort Classified Material (Sample)

1. General Instructions.

- a. As a designated courier of classified material, you are authorized to handcarry or escort material. Upon receipt of the classified material, you become, as defined in DOD Manual 5200.01, DOD Information Security Program, and AR 380-5, DA Information Security Program, the custodian of that information.
- b. All military personnel and DA civilian employees are subject to Title 18, U.S. Code, which deals with unauthorized release of national security information. However, as a courier, you are solely and legally responsible for protection of the information in your possession. This responsibility lasts from the time you receive it until it is properly delivered to the station, agency, unit, or activity listed as the official address.
- c. The intent of this briefing is to help you become familiar with your responsibilities as a courier, duties as a custodian, and the security and administrative procedures governing the safeguards and protection of classified information. You must be familiar with the provisions of Volume 3, DOD Manual 5200.01 (DOD Information Security Program: Protection of Classification Information) and AR 380-5 (DA Information Security Program) relating to couriering classified information with special emphasis on the areas listed below.

d. Access.

Figure X-1. Courier Briefing

- (1) You will be given delivery instructions for the material when it is released to you. Follow those specific instructions given and seek assistance from your activity security manager if you are unable to do so.
- (2) Dissemination of classified material is restricted to those persons who are properly cleared and have an official need for the information. No person has a right or is entitled to access of classified information solely by virtue of rank or position.
- (3) To help prevent unauthorized access and possible compromise of material entrusted to you, it must be retained in your personal possession or properly guarded at all times. You will not read, study, display, or use classified material while in public places or conveyances.

e. Storage.

- (1) Whenever classified information is not under your personal control, it will be guarded or stored in a GSA-approved security container. You will not leave classified material unattended in locked vehicles, car trunks, commercial storage lockers, or in commercial airlines passenger storage compartments and while aboard trains or buses.
- (2) You will not store the material in detachable storage compartments such as trailers, luggage racks, or aircraft travel pods. You will not pack classified items in regular checked baggage.
- (3) Retention of classified material in hotel/motel rooms or personal residences is specifically prohibited. Hotel safes and safety deposit boxes do not provide adequate storage for classified material.
- (4) Advance arrangements for proper overnight storage at a U.S. Government facility or, if in the U.S., a cleared contractor's facility are required prior to departure. Arrangements are the responsibility of the activity authorizing the transmission of classified material.

f. Preparation.

- (1) Whenever you transport classified information, it must be enclosed in two opaque sealed envelopes, similar wrappings, or two opaque sealed containers such as boxes or other heavy wrappings without any metal bindings/clips.
- (2) A locked briefcase or zippered pouch with an integral key-operated lock may be used for hand-carrying classified material outside an activity; however, it will not serve as an outer wrapping or container. The inner envelope or container shall be addressed to an official government activity (as if for mailing), stamped with the highest classification and placed inside the second envelope or container.
- (3) The outer covering will be sealed and addressed for mailing (in event of emergency) to the government activity. Proper preparation is the responsibility of the activity authorizing transmission. Do not accept improperly prepared material for transmission.

Figure X-1. Courier Briefing, continued

(4) If the classified material is to be retained by the official government activity you are visiting, a DA Form 3964 (Classified Document Accountability Record) will be completed, and a copy will be returned to your activity security manager.

g. Handcarrying.

- (1) The courier authorization and a picture ID should ordinarily permit you to pass through airport passenger control points within the U.S. without the need for subjecting the classified material to inspection.
- (2) If the screening official is not satisfied with your identification, authorization statement, or envelope, ask to speak with the senior official in a closed area. If the senior official demands to see the actual contents of the package, it may be opened in his/her presence in an area out of sight of the public. Ensure:
- (a) Precautions are taken to show officials only as much of the contents as satisfies them that the package does not contain any other item.
- (b) The senior official provides evidence of opening and inspection of the package by sealing and signing it when closed and confirming on the shipping documents or courier orders that the package has been opened. The addressee and activity security manager will be informed in writing of the opening of the material.
- (c) Classified material is inventoried, a copy of the inventory shall be retained at the courier's office/duty location, and you shall carry a copy of the inventory.
- (d) You have extra materials, i.e., opaque wrapping, appropriate tape, address labels, to repackage the classified information as necessary.
- (e) You return all classified material in a sealed package or, for any classified material that is not returned, produce a receipt signed by the activity security manager of the addressee organization. Return the receipt, normally a DA Form 3964, to your activity security manager.

h. Escorting.

- (1) When escorting classified material that is sealed in a container and too bulky to handcarry or is exempt from screening, prior coordination is required with the Federal Aviation Authority (FAA) and the airline involved.
- (2) This coordination is the responsibility of your organization's approving authority. You will report to the airline ticket counter prior to starting your boarding process. If satisfied, the official will provide an escort to the screening station and exempt the container from physical or other type inspection.
- (3) The actual loading and unloading of bulky material will be under the supervision of a representative of the airline; however, you or other appropriately cleared persons shall accompany the material and keep it under constant surveillance during the loading and unloading process.

- (4) Appropriately cleared personnel will be available to assist in surveillance at any intermediate stop when the plane loads and the cargo compartments are to be opened. Coordination for assistance in surveillance is the responsibility of the activity authorizing the transmission of the material.
- 2. Our primary concern is the protection and safeguarding of classified material from unauthorized access and possible compromise. Security regulations cannot guarantee the protection of classified information nor can they be written to cover all conceivable situations. They must be augmented by basic security principles and a common sense approach to protect official national security information.
- 3. You are reminded any classified instructions you receive must also be protected. Do not discuss verbal instructions with anyone not having a need to know, i.e., do not talk about where you were, what you did, or what you saw.
- 4. If you have questions at any time concerning the security and protection of classified and sensitive material entrusted to you, contact your activity security manager or HQ TRADOC DCS, G-2 Security.

Figure X-1. Courier Briefing, continued

HQ TRADOC Courier Certificate (Sample)	
As a designated courier of classified material, I,	
Designated Courier	
Date	
Activity Security Manager	

Figure X-2. Courier Acknowledgement

X-4. Continental U.S. (CONUS) Courier Authorization Orders

- a. Courier authorization orders with itinerary (Figure X-3) will be provided by the activity security manager for the handcarrying or escorting of classified material within CONUS utilizing commercial aircraft when:
- (1) The respective activity security manager has received a written justification for the need to handcarry or escort classified information.
- (2) The individual has received a courier briefing and has provided a written acknowledgement having read and understood such briefing.
 - (3) The individual is in possession of a DOD identification card.
- (4) Advance coordination with appropriate authorities has been made, i.e., overnight storage when appropriate, Federal Aviation Administration, Transportation Security Administration, transhipping activities for shipment of bulky materials.
- (5) Arrangements will be made in advance with customs, police, and/or immigration officials to facilitate movement through security. Activity security managers will ensure personnel understand the requirements contained within Paragraph 11, Enclosure 4, Volume 3, DOD Manual 5200.01, if, during transport, a senior official demands to see the contents of the package containing the classified information.
- b. For operations security purposes, courier authorization orders will <u>not</u> stipulate the courier is handcarrying classified material, only that the courier is authorized to handcarry certain items, e.g., laptop computer with CDROM/3.5 media drives, computer power and connectivity accessories, media storage devices, paper documentation, maps.
 - c. Blanket courier authorizations are not authorized.

HQ TRADOC CONUS Courier Authorization (Sample)

(Insert Letterhead)

(Office Symbol) (Date)

MEMORANDUM FOR (Insert Courier's Name, Organization, and Full Address)

SUBJECT: (U) CONUS Courier Authorization

1. (FOUO) The following (Insert Organization Name) individual is authorized to handcarry (Insert item(s) to be handcarried, i.e., laptop computer with CDROM/3.5 media drives, computer

power and connectivity accessories, media storage devices, documentation, maps) to/from (Insert Destination) for the period (Insert Departure and Arrival Dates):

<u>Name</u>	Rank/Grade and DoD CAC DID# (Last 4)		<u>Identification Type</u>	
(Insert Name)	(Insert Rank/Grade)	(Insert last 4 DID# digits)	(Insert the type of ID)	

- 2. (U) The complete itinerary is enclosed.
- 3. (U) The destination point of contact is (Insert Destination Point of Contact Name, Phone Number, and Email Address).
- 4. (U) The TRADOC point of contact is the undersigned, (Insert Phone Number, and Email Address).

Encl

(Insert Activity Security Manager Signature Block)

FOR OFFICIAL USE ONLY

HQ TRADOC CONUS COURIER AUTHORIZATION ITINERARY (SAMPLE) (Insert Dates)

<u>DATE</u>	<u>DEPART</u>	<u>ARRIVE</u>	<u>AIRLINES</u>	<u>FLIGHT</u>	<u>TIME</u>
(Insert All Dates, Departures, Arrives, Airlines, Flight Numbers, and Times - Example Below)					
13 Aug 16	Fort Eustis, VA				1600
13 Aug 16		Norfolk, VA			1730
13 Aug 16	Norfolk, VA		Delta Airlines	879 1925	
13 Aug 16		Atlanta, GA			2111
13 Aug 16	Atlanta, GA		Delta Airlines	9382155	
13 Aug 16		Nashville, TN			2200
14 Aug 16	Nashville, TN		Delta Airlines	4571	1950
14 Aug 16		Atlanta, GA			2158
14 Aug 16	Atlanta, GA		Delta Airlines	4564	2253
15 Aug 16		Norfolk, VA			0027
15 Aug 16	Norfolk, VA				0100
15 Aug 16		Fort Eustis, V	A		0230

FOR OFFICIAL USE ONLY

Figure X-3. CONUS Courier Authorization Orders

X-5. Outside CONUS Courier Authorization Orders

TRADOC personnel required to handcarry classified information outside the U.S. will request the Oustide CONUS courier order through their respective activity security manager, through HQ TRADOC DCS, G-2 Security, and to the TRADOC Command Security Manager for approval.

Appendix Y Unauthorized Disclosure

Y-1. Unauthorized Disclosure

- a. The compromise of classified information can cause damage to our national security. Loss of classified material is just as serious. When one or both of these occur, immediate action is required to minimize any damage and eliminate any conditions that might cause further compromises.
- b. Prompt and effective investigation of the situation and prompt reporting of results are critical to minimize/eliminate further compromises. In cases where compromise has been ruled out and there is no adverse effect on national security, a common sense approach to the early resolution of an incident at the lowest appropriate level is encouraged.
- c. Anyone finding classified material out of proper control will take custody of and safeguard the material and immediately notify their respective activity security manager or HQ TRADOC DCS, G-2 Security.
- d. Any person who becomes aware of the possible loss or compromise of classified information will immediately report it to their respective activity security manager and HQ TRADOC DCS, G-2 Security or, if after duty hours, the HQ TRADOC Operations Center.
- e. At a minimum, a security preliminary inquiry will be conducted for any security incident involving classified information, to include data spillage. Refer to Enclosure 6, Volume 3, DOD Manual 5200.01, for complete security incident requirements.

Y-2. Preliminary Inquiry/Investigation Officer

- a. A person not involved directly or indirectly with the incident will be appointed to conduct the preliminary inquiry or investigation. An activity security manager will not be appointed as the preliminary inquiry or investigative officer but will assist the appointed officer as necessary. The appointed individual will:
 - (1) Have the appropriate security clearance;
 - (2) Have the ability and available resources to conduct an effective inquiry/investigation;
- (3) Conduct the inquiry/investigation according to the guidelines outlined in Enclosure 6, Volume 3, DOD Manual 5200.01; and

(4) Complete a report of security incident, inquiry, or investigation as shown in Appendix 1 to Enclosure 6, Volume 3, DOD Manual 5200.01.

Y-3. Preliminary Inquiry/Investigation

- a. The appointing authority will forward to HQ TRADOC DCS, G-2 Security:
- (1) The completed preliminary inquiry or investigation with written concurrence/non-concurrence.
 - (2) The findings and recommendations of the inquiry/investigation.
 - (3) Proposed corrective actions.
 - b. The activity security manager will:
- (1) Ensure the security incident inquiry or investigation is promptly and properly completed;
 - (2) Notify the OCA when a possible compromise or greater has occurred;
- (3) Provide preliminary inquiry/investigation results to HQ TRADOC DCS, G-2 Security within 10 working days from the date of discovery (extensions may be granted);
 - (4) Ensure corrective actions are implemented.
- (5) Maintain a copy of the entire preliminary inquiry or investigation for a minimum of 2 years.

Y-4. Data Spills

- a. Classified data spills occur when classified data is introduced either onto an unclassified information system or to an information system with a lower level of classification, or to a system not accredited to process data of that restrictive category.
- b. Although it is possible that no unauthorized disclosure occurred, classified data spills are considered and handled as a possible compromise of classified information involving information systems, networks, and computer equipment until the inquiry determines whether an unauthorized disclosure did or did not occur.
- c. Activity security managers are responsible for ensuring the policy requirements for addressing an unauthorized disclosure, as specified in this memorandum and within Enclosure 6, Volume 3, DOD Manual 5200.01, are met.
- d. Activity security managers will work closely with the IT and HQ TRADOC DCS, G-6 information assurance staff who have responsibility for the operation of the networks and systems as well as the technical knowledge needed to address the spill.

e. Activity security managers and preliminary inquiry/investigation officers will familiarize themselves with Enclosure 7, Volume 3, DOD Manual 5200.01, for incidents involving data spillage.

Y-5. Personally identifiable information (PII) Unauthorized Disclosure

Activity security managers will notify the HQ TRADOC DCS, G-6 PII Officer within 1 hour of discovering a PII unauthorized disclosure.

Y-6. Unauthorized Disclosure – Other Requirements

- a. In cases where a person has had unauthorized access to classified information, the individual concerned will receive a debriefing from the respective activity security manager, and sign the SF 312, Classified Information Nondisclosure Agreement, security debriefing acknowledgement.
- b. If classified information appears in the public media, personnel will not make any statement or comment that would confirm the accuracy or verify the classified status of the information and will immediately report it to HQ TRADOC DCS, G-2 Security.
- c. The TRADOC Command Security Manager will be immediately notified of any unauthorized absences, suicides, incapacitation, or revocation of a security clearance where military or civilian personnel have had access to classified information.
- d. Any incident in which the deliberate compromise of classified information or involvement of foreign intelligence agencies is suspected will be reported to the TRADOC Command Security Manager and the 902nd Military Intelligence Group Resident Office, Fort Eustis.

Appendix Z Security Education, Training, and Awareness (SETA)

Z-1. SETA Responsibilities

- a. Each activity security manager is responsible for providing SETA training throughout their respective organization. SETA is aimed at promoting quality performance of security responsibilities by personnel to:
- (1) Provide the necessary knowledge and information to enable quality performance of security functions.
- (2) Promote an understanding of information security program policies and requirements and their importance to the national security.
 - (3) Instill and maintain continuing awareness of security requirements.
 - (4) Assist in promoting a high degree of motivation to support TRADOC goals.

(5) Utilize periodic briefings, training sessions, formal presentations, video tapes, computer-generated security training, and published articles when providing SETA.

Z-2. Initial Security Orientation

- a. Initial security orientations will be provided to all personnel who could be expected to play a role in the information security program and/or have an IT account, i.e., electronic mail.
 - b. Newly assigned personnel will complete within 7 days of their arrival:
- (1) Mandated ALMS online security training. Activity security managers may also provide a supplemental briefing specifically tailored to their organization; however, the organizational briefing will not substitute for the online security training.
 - (2) CUI training in accordance with Volume 4, DOD Manual 5200.01.
 - (3) NATO training.
- (a) The individual will read the NATO security briefing and sign an acknowledgment statement (Figures Z-1 and Z-2, respectively) to the fact that he/she has received such briefing and understand his/her responsibilities for handling NATO information.
- (b) Activity security managers will maintain the acknowledgement statements and annotate JPAS accordingly.
- (c) Activity security managers will also provide a NATO briefing to their respective contract personnel and maintain acknowledgement statements if the DD Form 254 (DOD Contract Security Classification Specification) requires the contractor to have NATO access.
 - (4) Antiterrorism/Force Protection (AT/FP) Level 1 training.

U.S. ARMY TRADOC NORTH ATLANTIC TREATY ORGANIZATION (NATO) SECURITY BRIEFING

FOREWORD

This 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 U.S. National Security Authority for NATO 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 DoD 5220.22-M.

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	Spain	Norway	Estonia	Albania
Czech Republic	Luxembourg	United Kingdom	Iceland	Latvia	Croatia
Germany	Netherlands	U.S.	France	Lithuania	
Greece	Poland	Denmark	Romania	Slovakia	

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

Figure Z-1. North Atlantic Treaty Organization (NATO) Briefing

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.

NOTE: U.S. Army Training and Doctrine Command (TRADOC) NATO Control Points and User Agencies are authorized access to NATO Secret and below only. Access to COSMIC and ATOMAL information is not authorized.

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.

Figure Z-1. North Atlantic Treaty Organization (NATO) Briefing, continued

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 those of FOR OFFICIAL USE ONLY, OFFICIAL USE ONLY, or SENSITIVE, BUT UNCLASSIFIED information, "NATO RESTRICTED" is a security classification.)

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).

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. 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 subregistry 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.

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 U.S. 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.

Figure Z-1. North Atlantic Treaty Organization (NATO) Briefing, continued

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 <u>all ATOMAL</u> 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, its Supporting Directives, and U.S. National Security Authority for NATO Instruction 1-07, Section 7, Page 31)

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.

Figure Z-1. North Atlantic Treaty Organization (NATO) Briefing, continued

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 U.S.

In urgent situations, the U.S. Postal Service Express Mail may be used to transmit material NS and below within the U.S., 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 U.S. 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. NATO accredited SIPRNET, Joint Worldwide Intelligence Communication System (JWICS), U.S. BICES, and CENTRIX-ISAF are the only authorized networks approved to transmit and store NATO SECRET, NATO CONFIDENTIAL, and NATO RESTRICTED information.

Destruction. The destruction of CTS, CTSA, NS, and NSA 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 CONFIDENTIAL, NATO RESTRICTED and NATO UNCLASSIFIED shall be destroyed by any means authorized for U.S. CONFIDENTIAL material.

Reproduction. COSMIC documents shall be reproduced by the Central U.S. Registry and COSMIC Sub-registries which must report the number of copies made to the CUSR. Reproduction of ATOMAL (CTSA, and NSA) 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.

Figure Z-1. North Atlantic Treaty Organization (NATO) Briefing, continued

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, immediately contact your security officer or registry system official. 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.
- 4. Information concerning terrorist plans and activities posing a direct threat to U.S. or NATO facilities, activities, personnel or material.
- 5. 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:
- a. STAY CALM. You are not at fault because they chose to target you.
- b. BE NONCOMMITTAL. Be ambiguous as to whether or not you will provide them with material or information.

Figure Z-1. North Atlantic Treaty Organization (NATO) Briefing, continued

- c. 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.
- d. 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 information, your security officer or the HQ U.S. Army TRADOC NATO Secret Sub-Registry Officer can assist you.

Figure Z-1. North Atlantic Treaty Organization (NATO) Briefing, continued

HQ TRADOC NORTH ATLANTIC TREATY ORGANIZATION (NATO) BRIEFING ACKNOWLEDGEMENT

Section A.

I certify that I have read the NATO briefing and fully understand the procedures for handling NATO SECRET and below material and my responsibility for safeguarding such information. 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.

I understand U.S. Army Training and Doctrine Command (TRADOC) organizations are not authorized to maintain NATO materials above NATO SECRET. I understand that I am not authorized to maintain nor have access to NATO information unless my position requires such access and the need-to-know is authorized in Section B. below by my supervisor. I understand a NATO Secret User Agency or Control Point must be established for my organization prior to maintaining NATO Secret materials.

I fully understand written justification signed by my respective Commander/Director will be forwarded through the organization's activity security manager and to the HQ U.S. Army HQ TRADOC Deputy Chief of Staff (DCS), G-2 NATO SECRET Sub-Registry Officer (ATIN-SE), 950 Jefferson Avenue, Fort Eustis, VA, 23604-5740, DSN 501-6170 or (757) 501-6170, if utilization or maintenance of NATO SECRET information is required to meet organization mission requirements.

I understand that the SIPRNET, JWICS, U.S. BICES, and CENTRIXS-ISAF are the only authorized networks authorized to process, store, and transmit NATO SECRET, NATO CONFIDENTIAL, and NATO RESTRICTED information. TRADOC organizations must have a current local NATO accreditation by the respective Designated Approving Authority prior to processing, storing, and/or transmitting NATO SECRET, NATO CONFIDENTIAL, or NATO RESTRICTED materials utilizing one or more systems mentioned above. NATO UNCLASSIFIED may be transmitted and stored via the non-secure Internet protocol router network utilizing encryption capability.

I will contact my activity security manager and supporting information technology team and provide identifying classified system information and any classified printers and/or scanners used with the system processing NATO SECRET information, i.e., system make and model, serial number, software, location. In turn, the activity security manager or IT team will contact and provide the information to the supporting Network Enterprise Center and HQ TRADOC NATO Secret Sub-Registry Control Officer.

I will contact my activity security manager, the HQ TRADOC NATO SECRET Sub-Registry Control Officer, and local counterintelligence officials immediately if I find any NATO material unsecured or unattended.

Figure Z-2. NATO Acknowledgement

NAME: GRADE/RANK: ORGANIZATION: ORGANIZATION ADDRESS: PHONE NUMBER:
SIGNATURE:
DATE:
Section B. (Completed by supervisor if above individual requires access to NATO materials)
SUPERVISOR NAME: GRADE/RANK: ORGANIZATION: PHONE NUMBER:
I certify above individual requires access to NATO materials to perform his/her duties and has a need-to-know.
SUPERVISOR SIGNATURE:
DATE:
Section C. NATO DEBRIEFING ACKNOWLEDGEMENT
I have been debriefed for NATO SECRET and below, 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:
DATE:
Figure Z-2. NATO Acknowledgement, continued

Z-3. Annual Security Refresher Training

- a. At a minimum, all military, civilians, and on-site contractors with access to classified information shall receive annual refresher training that reinforces the policies, principles, and procedures covered in their initial and specialized training.
- b. Military and civilians will complete the mandated ALMS online annual refresher training. Activity security managers are encouraged to also provide supplemental refresher security training specific to their respective organization.
- c. Supervisors/Managers are also required to complete the mandated ALMS online Annual Awareness: Managing Personnel with Clearances/Access to Classified Information annual training.
- d. Activity security managers will ensure the FSO provides annual fresher training to on-site contractors unless the contract specifically states the U.S. Government will provide the training, in which case, the contractor will receive annual security training from the respective activity security manager.

Z-4. Other Security Training Requirements

- a. Activity security managers will maintain all security training records for 2 years.
- b. Derivative Classification Training. Individuals will complete derivative classification training if the position held requires him/her to generate derivative classification decisions. The Defense Security Service (DSS) Center for Development of Security Excellence derivative classification online course may be completed to meet this requirement. The online course description can be viewed at: http://www.cdse.edu/catalog/information-security.html. Refresher derivative classification training is required every 2 years.

c. OCA Training.

- (1) The activity security manager is responsible for ensuring initial and annual OCA training is completed for those individuals having such authority within their respective organization. The DSS Center for Development of Security Excellence OCA online course may be completed to meet this requirement. The online course description can be viewed at: http://www.cdse.edu/catalog/information-security.html. The OCA will certify, in writing, the training has been received. The activity security manager will maintain the acknowledgement statement(s) and provide a copy to HQ TRADOC DCS, G-2 Security until the individual departs the command or no longer requires OCA.
- (2) In accordance with Enclosure 5, Volume 3, DOD Manual 5200.01, OCAs who do not receive the specified training at least once within a calendar year shall have their classification authority suspended by HQDA DCS, G-2 (for Secret OCA) or Under Secretary for Defense (Intelligence) (for Top Secret OCA) until the training has been completed.

- d. <u>AT/FP</u>. For those individuals pending travel outside the U.S. and its territories or possessions, overseas area-specific AT/FP training must be received within 6 months of departure date to the overseas area. Personnel will contact their respective organization's AT/FP Officer for this training.
- e. Critical Nuclear Weapons Design Information briefings will be provided by HQ TRADOC DCS, G-2 Security to TRADOC personnel requiring such access.
- f. Each TRADOC organization shall ensure SETA is appropriately evaluated during self-inspections and other oversight activities, to include assessing the quality and effectiveness of the efforts, ensuring appropriate coverage of the target audience, and maintaining security/CUI training records for 2 years.

Z-5. Security Debriefings

- a. All personnel who are retiring, resigning, being discharged, or will no longer have access to classified information will read and sign the SF 312 security debriefing acknowledgement. The SF 312 first page and the security debriefing acknowledgement are the only sections that require completion for debriefings. An entire SF 312 will be read and completed for those uncleared personnel who may have inadvertently had access to classified information. Activity security managers will remove all collateral accesses and remove the JPAS relationship upon completion of the security debriefing acknowledgement.
- b. Personnel having any special accesses, i.e., NATO, critical nuclear weapons design information, will also be debriefed prior to departing the command.
 - c. Activity security managers will maintain debriefings for 2 years.

Z-6. Security Training for Personnel Having Security Responsibilities

- a. Individuals designated as activity security managers, classification management officers, security specialists, or any other TRADOC individual whose duties significantly involve managing and overseeing classified information shall receive training that meets the training requirements outlined in Paragraph 10, Enclosure 5, Volume 3, DOD Manual 5200.01.
- b. There are a significant number of security online and classroom training available through the DSS Center for Development of Security Excellence. For more information, visit their website at http://www.cdse.edu/index.html.
- c. For those individuals interested in obtaining security professional certification, the DSS offers the Security Professional Education Development (SPeD) Program. The SPeD Certification Program is part of the DOD initiative to professionalize the security workforce. This initiative is intended to ensure there is a common set of competencies among security practitioners that promotes interoperability, facilitates professional development and training, and develops a workforce of certified security professionals.
- c. For more SPeD certification information, visit the DSS website at http://www.cdse.edu/certification/sped_what.html.

Glossary

Section I Abbreviations

AT/FP Antiterrorism/Force Protection
ALMS Army Learning Management System
ARCIC Army Capabilities Integration Center

AV audio visual

BICES Battlefield Information Collection and Exploitation Systems
CENTRIXS-ISAF Combined Enterprise Regional Information Exchange System-

International Security Assistance Force

CONUS continental U.S.
CTS COSMIC top secret

CTSA COSMIC top secret ATOMAL CUI controlled unclassified information

CUSR Central U.S. Registry
DA Department of the Army
DCS deputy chief of staff
DOD Department of Defense
DOE Department of Energy
DSS Defense Security Service

e-QIP Electronic Questionnaires for Investigations Processing

FOUO for official use only
FSO Facility Security Officer

GSA general services administration

HQ headquarters

IDS intrusion detection system IT information technology

JPAS Joint Personnel Adjudication System

JWICS Joint Worldwide Intelligence Communication System

NATO North Atlantic Treaty Organization

NC NATO Confidential
NR NATO restricted
NS NATO secret

NSA NATO secret ATOMAL NU NATO unclassified

OCA original classification authority
PII personally identifiable information

SCG security classification guide

SCI sensitive compartmented information SETA security education, training, and awareness

SF standard form

SIPRNET secret Internet protocol routing network SPeD security professional education development

U.S. United States

USACIMT U.S. Army Center for Initial Military Training

VTC video teleconference

Section II Terms

This section contains no entries.

Section III Special Abbreviations and Terms

This section contains no entries.