

Commander U.S. Army Garrison Baden- Wuerttemberg



Security Awareness Briefing

DPTMS-Security Division

This Briefing is unclassified in its entirety



Commander U.S. Army Garrison, DPTMS-Security

Why this briefing

- To provide you the resources to correctly handle classified information.
- To ensure you understand your duties and responsibilities with regard to classified information.
- To help deter and prevent loss of control or compromise of classified material
- Review Information Systems Security and Computer Security
- Identify types of Threats



Commander U.S. Army Garrison, DPTMS-Security

Why this briefing – con't

- Review Operations Security Measures (OPSEC)
- Demonstrations (Do's / Don'ts)
- Walk-ins
- Travel Advisory
- European Threat Update
- AT LEVEL I Training (VIDEO)



Commander U.S. Army Garrison, DPTMS-Security

Regulations

AR 380-67

Personnel Security Program
(09 Sep 1988)

AR 530-1

Operations Security
(3 March 1995)

AR 380-5

Department of the Army
Information Security Program
(29 Sep 2000)



Commander U.S. Army Garrison, DPTMS-Security

Classification Levels

- Levels (Must have a Need-To-Know)
 - Top Secret (Most Damaging to National Security)
 - Secret (Serious Damage)
 - Confidential (Damage)
- Levels
 - Based on expected damage to national security if subjected to unauthorized disclosure
- Levels (Must have a Need-To-Know)
- All data printed from **SIPRNET**
 - Unless it is specifically marked UNCLASSIFIED or certified as such by the Security Manager



Commander U.S. Army Garrison, DPTMS-Security

Safeguarding

- When out (exposed), classified information must be protected at all times
- Must have a cover sheet
- No one can remove the information from the work space without permission
- Must be properly secured when no longer in use



Commander U.S. Army Garrison, DPTMS-Security

Cover Sheets



Classified Labels

- Always use cover sheets (SF 703, 704, 705) and classified labels (SF 710, 708, 707, 706) while handling hard-copy classified documents
 - Security Manager can provide
- Deliver classified material to a person, not to an inbox
 - You will never know if it gets “buried”
- When reading classified information be aware of your environment and who is close to you.



Commander U.S. Army Garrison, DPTMS-Security

COVER SHEETS

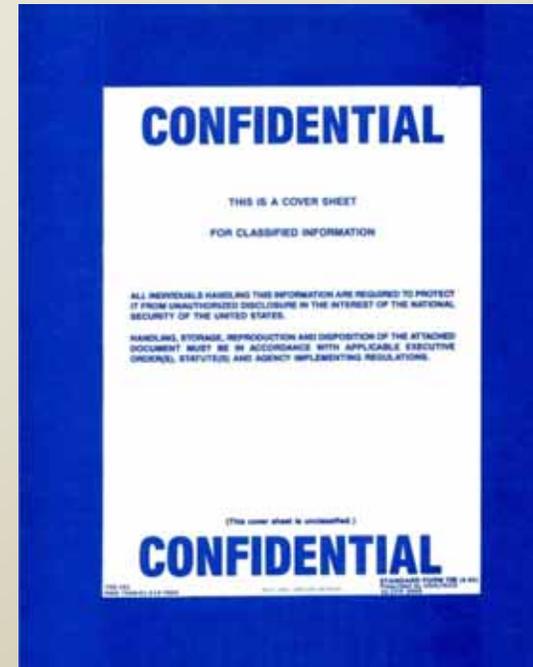
**SF 703, TOP
SECRET**



**SF 704,
SECRET**



**SF 705,
CONFIDENTIAL**





Commander U.S. Army Garrison, DPTMS-Security

SF 710, SF 708, SF 707 & SF 706 LABELS



UNCLAS/FOUO



Commander

Mark it and safeguard it!

- - Basic document markings apply to all media



AR 380-5 is clear, it is the users responsibility to properly control, handle, mark, and transport information

Security Education, Training and Awareness - - Do It!!

1. Computer disc must reflect the highest level of classification contained on the disc
2. Standard labels should be used for all levels of classification - if none available - - make your own.

- a. SF706 - Top Secret
- b. SF707 - Secret
- c. SF708 - Confidential
- d. SF709 - Classified
- e. SF710 - Unclassified
- f. SF711 - Data Descriptor
- g. SF712 - Classified SCI



3. No standard form (SF) and/or label(s) exist for Compact Discs (CDs)
 - a. The SF labels prescribed for removable storage media may be used for the marking of classified CDs and their cases
 - b. Classification must be conspicuously marked on the CD case and the CD itself
4. Personal drives - - must be marked personal!!

UNCLAS/FOUO



Commander U.S. Army Garrison, DPTMS-Security

DA LABEL 87, NOT A CLASSIFIED COVER SHEET

- > Information enclosed must also be safeguarded
- > Use only for protective marking
- > FOUO material must be destroyed at a minimum of tearing to preclude reconstruction
- > Treat as sensitive material



UNCLAS/FOUO



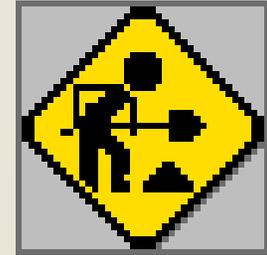
Commander U.S. Army Garrison, DPTMS-Security

Access to Classified Information

- Must have current, valid security clearance at or above the level of information
- Need-to-Know
- Holder of classified information (Security Manager / Directorate) - final determination if **you** have a Need-to-Know



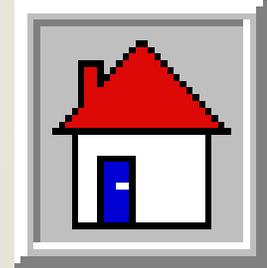
Working hours



- If classified material is left unattended (smoke break, restroom-call, ...), material will be secured either in an approved container or by presence of properly cleared coworker, or by securing office (locking door) in a manner that renders any tampering evident.
- Use of Non-lockable drawers AND open offices is NOT acceptable



After working hours



- Material will be stored in a Government Service Agency (GSA) approved / certified security container or vault
- STU-III Keys/STE Fortessa cards must be separated from their equipment when not in use in non-Open Storage areas.
 - They can be maintained in a locked drawer.



Commander U.S. Army Garrison, DPTMS-Security

CLEARANCES

- Send in SF86 (For Clearance Request) via Electronic Questionnaires for Investigations Processing {e-QIP} and SF85P (For Contractor Clearance and System Authorization Access Request {DA Form 2875} for government computer use (no clearance)
- Send SF86 thru [Joint Personnel Adjudication System \(JPAS\)](#) – Security Manager’s tool. This is sent to the [Office of Personnel Management \(OPM\)](#) for investigation process
- [DA Central Clearance Facility \(Army CCF\)](#) adjudicates clearance investigations for eligibility/determination
- Once assigned individuals granted clearance - commands assign access
- * Individual responsibility to obtain and maintain your clearance
 - Must be on your job description / MOS
 - If handling sensitive information, a commander can request you have a clearance, need memo from commander
 - **REMEMBER: Having a clearance is a Privilege NOT a Right**



Commander U.S. Army Garrison, DPTMS-Security

Adjudication Criteria (Clearance determination)

- Allegiance to U.S.
- Foreign Influence
- Foreign Preference
- Sexual Behavior
- Personal Conduct
- Financial Consideration
- Alcohol Consumption
- Drug Involvement
- Emotional, Mental & Personality Disorders
- Criminal Conduct
- Security Violations
- Outside Activities
- Misuse of Information Technology Systems



Commander U.S. Army Garrison, DPTMS-Security

PR Update Requirement

- To maintain access at all levels -
Periodic Reinvestigations required
 - Top Secret access - 5 years
 - Secret access - 10 years
 - Confidential access - 15 years



Commander U.S. Army Garrison, DPTMS-Security

Continuous Evaluation Program

- Purpose - Continuously monitor individuals with clearances to ensure continued loyalty, reliability and trustworthiness
- Command responsibility (Security Manager) to report derogatory information on individuals to ACCF



Commander U.S. Army Garrison, DPTMS-Security

Telephone Security



COMSEC

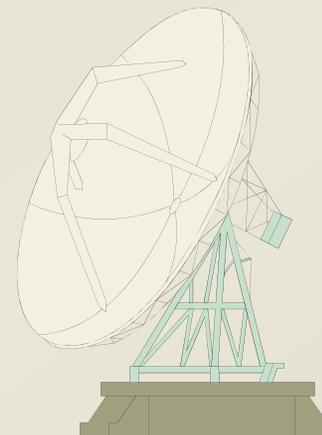
- Always use STU-IIIs or STEs in secure mode to discuss classified information
 - Ensure no un-cleared personnel, cell phone/other open line discussions are taking place in vicinity
 - STU-III keys or FORTESSA Cards are FOUO unless inserted in the equipment. They then are classified to the level of the equipment
- Always identify open lines as such when answering a phone:
 - DPTMS, Heidelberg, non-secure line, may I help you?
- Always be aware of classified discussions/secure radio transmissions in the vicinity of open-line telephonic discussions.
- Do not “talk around” classified topics. Invest the time and switch to a secure line or use SIPRNET e-mail.
- Ensure you use the secure fax for sending/receiving classified documents.



Commander U.S. Army Garrison, DPTMS-Security



Bear in mind.



CELLULAR PHONE

users

must assume

EAVESDROPPING!



UNCLAS/FOUO



Commander U.S. Army Garrison, DPTMS-Security

SECURITY CONTAINER

- **Store all classified in locked container unless someone is present in the room who is authorized access**
- **Fill out SF 702 (security container check sheet) each time you:**
 - **Open**
 - **Secure**
 - **Check the container**



Commander U.S. Army Garrison, DPTMS-Security

Combinations

- Memorize them... do not write them down.
- There are ways to make it simpler to remember
- The same applies to passwords



UNCLAS/FOUO



Commander U.S. Army Garrison, DPTMS-Security

Changing Combinations

Change combinations when:

1. An individual who knows the combination no longer needs access (PCS, change of duty position, termination, retirement, etc.)
2. Clearance revoked, suspended, or limited
3. The combination has been compromised or possibly compromised
4. Annually (minimum)





Commander U.S. Army Garrison, DPTMS-Security

Activity Check Sheets SF 701

- All areas handling classified material will have one and it will be used daily
 - Security Manager can provide
- Recommend you use one as a reminder
- It ensures you...
 - Appropriately store classified information
 - Appropriately safeguard burn bags
 - Lock you security containers and correctly record the action
 - Secure Windows and doors / turn off coffee pots
 - Do not put classified information in garbage cans
 - Clean your desk, that coworkers' desks are cleared, and no classified information is adrift
 - Check PDS SIPR Lines



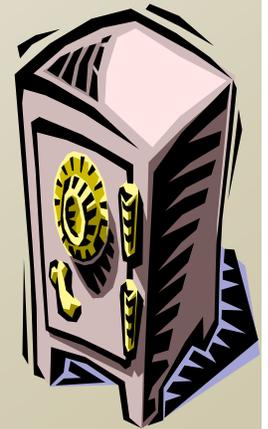


Commander U.S. Army Garrison, DPTMS-Security

SF 701-End of the Day Security Check



| ACTIVITY SECURITY CHECKLIST | | DIVISION/BRANCH/OFFICE | | | | | | | | | | ROOM NUMBER | | MONTH AND YEAR | | | | | | | | | | | | | | | | | |
|--|--------|--|--------|--------|--------|---|---|---|---|----|----|-----------------------|----|----------------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| | | S-2, 102D SIGNAL BATTALION | | | | | | | | | | 209 | | MARCH 2004 | | | | | | | | | | | | | | | | | |
| Irregularities discovered will be promptly reported to the designated Security Office for corrective action. | | Statement | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | I have conducted a security inspection of this work area and checked all the items listed below. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TO (if required) | | FROM (if required) | | | | | | | | | | THROUGH (if required) | | | | | | | | | | | | | | | | | | | |
| ITEM | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| 1. Security containers have been locked and checked. | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2. Desks, wastebaskets and other surfaces and receptacles are free of classified material. | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3. Windows and doors have been locked (where appropriate). | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4. Typewriter ribbons and ADP devices (e.g., disks, tapes) containing classified material have been removed and properly stored. | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5. Security alarm(s) and equipment have been activated (where appropriate). | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 6. LIGHTS OUT | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 7. COMPUTERS OFF | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 8. CABINETS LOCKED | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 9. KOV 14 SECURED | ✓ | ✓ | ✓ | ✓ | ✓ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| INITIAL FOR DAILY REPORT | Y.M.A. | G.H.F. | Y.M.A. | Y.M.A. | G.H.F. | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TIME | 1630 | 1631 | 1630 | 1630 | 1630 | | | | | | | | | | | | | | | | | | | | | | | | | | |



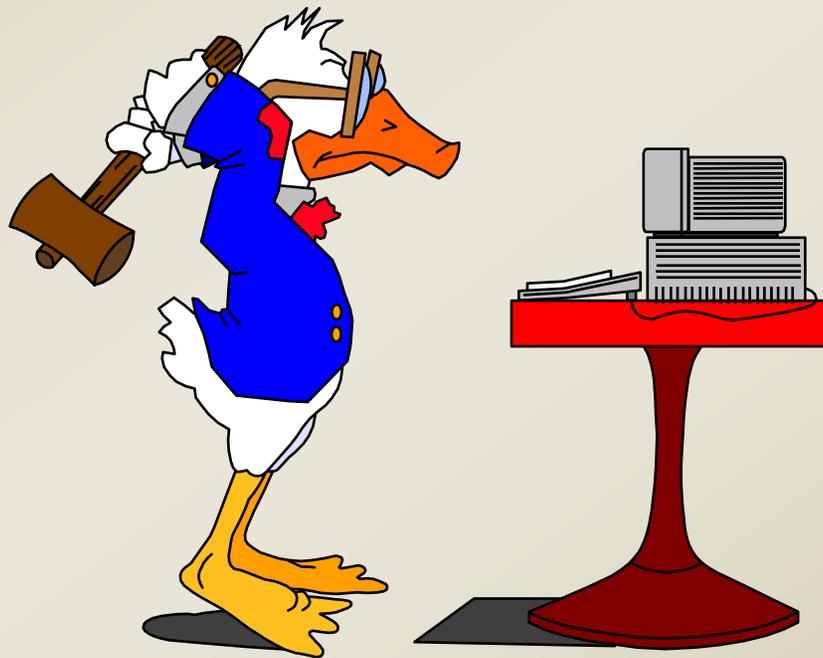
701-101
NSN 7540-01-213-3880

STANDARD FORM 701 (8-86)
Prescribed by GSA FPMR (41 CFR) 101-11.6
32 CFR 2003 GSAPP V1.00



Commander U.S. Army Garrison, DPTMS-Security

Computer/Information Security





Commander U.S. Army Garrison, DPTMS-Security

Command Information Systems



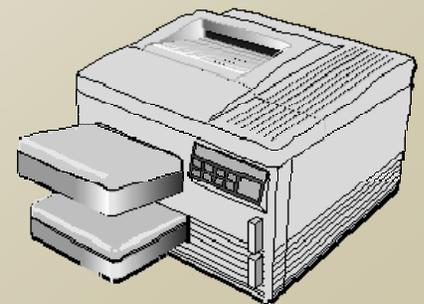
- **Minimize** printing of classified information. Ensure you know which printer you are using when printing classified information.
 - Color printers take longer to process a task and they need to be supervised until completion of classified printing job.
 - You are accountable for all classified information sent to a printer
- **Do not** transfer information (even unclassified) from SIPRNET to NIPRNET
 - If you need to move UNCLASSIFIED information from SIPRNET to NIPRNET talk with Information Assurance Manager (IAM) or Security Manager
- **Appropriately** mark all media with the highest classification of information.
 - ** All disks introduced to a SIPRNET drive will be classified SECRET regardless of what information is in them. * Take hard drives out of SIPR and lock up at end of day.
 - To keep a disk UNCLASSIFIED when you are moving information from NIPRNET to SIPRNET, engage the write-protect tab.
 - Do not leave classified material on a printer unless it is an open storage area... It will be treated as all other classified material – positive control.
- **Disclosure** of all official material (including NIPRNET) to foreign personnel will be cleared through the Foreign Disclosure Officer.
- **Pornographic** sites are unauthorized
- **Update** anti-virus software continuously
- **Safeguard** your password. Do not share it. Report compromised PW to IAO



Commander U.S. Army Garrison, DPTMS-Security

Copying and Fax machines

- Only use copiers and fax machines that have been authorized (as indicated by classification markings on the machines) for reproduction of classified material.
- Control classified material
 - Do not leave classified material in the machine
- See Security Manager with questions



UNCLAS/FOUO



Commander U.S. Army Garrison, DPTMS-Security

Loss or Compromise of Classified Information

- Anyone involved in a security incident will be held accountable for their actions
- Any security incident must be immediately reported to the Security Manager
 - Preliminary investigation
 - 15-6 Investigation



Commander U.S. Army Garrison, DPTMS-Security

Penalties

- Mishandling classified information - Range from command letter to major fines and possible imprisonment
- Engaging in espionage activities - Major fines and imprisonment



Commander U.S. Army Garrison, DPTMS-Security

Dissemination

- Classified information will only be disseminated to authorized personnel (those with a clearance and need-to-know)



Commander U.S. Army Garrison, DPTMS-Security

Hand-carrying Requirements

- Within command
- Outside command
- Commercial aircraft
- Government aircraft



Commander U.S. Army Garrison, DPTMS-Security

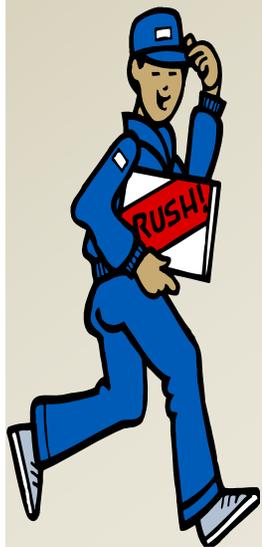
Hand-carrying Classified Info

- * Use SIPRNET e-mail or secure fax as much as possible
- Couriers will be issued courier cards ([DD Form 2501](#)) - Letter of Authorization and [AE Form 380-5E](#) when crossing international borders
 - See Security Manager
- Travel through commercial aircraft requires a letter and a courier card – (Will receive a detailed briefing from Security Manager)
 - Do not challenge security personnel at the Airport. If they insist in examining classified packages ask for the Airport security officer, present credentials and allow inspection in a isolated area (maintain watch on material)
 - Coordinate for proper storage
- All travel outside the post requires proper double wrapping of classified material
 - Travel within the post: briefcase can be used as outer wrapping
 - See Security Manager for wrapping requirements



Commander U.S. Army Garrison, DPTMS-Security

How to Prepare Classified Materials for Transmittal

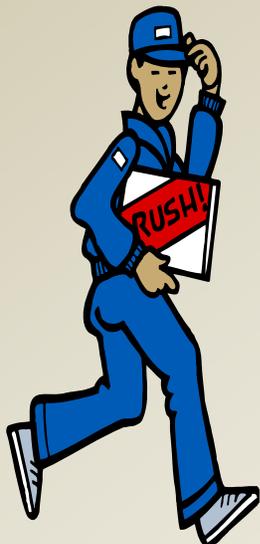


UNCLAS/FOUO



Commander U.S. Army Garrison, DPTMS-Security

Courier Card DD FORM 2501



| | | | |
|---|--|---------------------------------------|--|
| COURIER AUTHORIZATION | | SERIAL NUMBER AE 08465 | |
| C. ISSUE DATE 2 JAN 03 | | E. EXPIRATION DATE 1 JAN 04 | |
| 3. NAME (Last, first, middle initial) SMITH, WILLIAM | | | |
| 4. RANK OR GRADE SFC | | | |
| 6. AUTHORITY TOP SECRET | | | |
| 8. ADDRESS (Include street / route, street address, apartment or office number, city, state, and ZIP code) HEMPSTEAD (AETC-INT) COMMUNICATIONS CENTER APO SF 96319-0431 | | | |
| 10. SECURITY INFORMATION (Include security classification and authority) TOP SECRET | | | |
| 11. AUTHORIZED APPROVING OFFICIAL a. NAME A.B. JONES | | c. SIGNATURE <i>A.B. Jones</i> | |
| b. TITLE COMMANDER | | | |

DD Form 2501, MAR 88



UNCLAS/FOUO



Methods of Destruction

- Burning
- Crosscut shredding (approved for classified destruction)
- Pulverizers/Disintegrators
- CDs/Floppy Discs – Obtain a media shredder if possible

NOTE: See Garrison Emergency Destruction/ Evacuation Plan

- TS Material must be recorded/inventoried w/two cleared witnesses



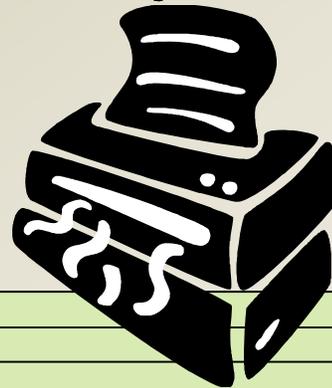
Commander U.S. Army Garrison, DPTMS-Security

Finished reading your mail? If your personal data is important to you, don't just toss it. **SHRED IT!**

DO



Shred or
tear into
pieces all
mail!



MAIL?
Don't just throw me away.
Shred Me!
Tear Me!



DON'T

Throw any
whole paper
in **trash cans**
or
dumpsters.



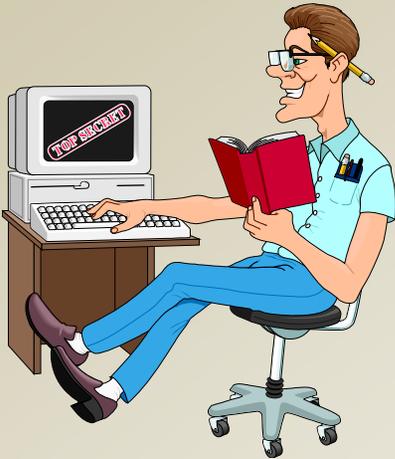
Why? To protect classified, for official use only, privacy act, and sensitive but unclassified information contained in documents. **ALWAYS THINK OPSEC.**

UNCLAS/FOUO



Commander U.S. Army Garrison, DPTMS-Security

Types of Threats



Hackers & Teens



Insiders/Auth Users



Criminals & Organized Crime



Malicious Codes



Industry & Economic Espionage



Foreign Countries



Terrorists

UNCLAS/FOUO



Commander

New technology poses new threats to security!

USB Memory Watch



USB E-Pen



USB Pen Drive



Scanning Devices



Miniaturization

Thumb Drive



Casio Watch Camera



Digital Media



Video Devices



Audio Recorders with USB connectivity



UNCLAS/FOUO



Commander U.S. Army Garrison, DPTMS-Security

Hostile Intelligence Threat



- US personnel are targets of several foreign intelligence service
 - See Security Manager for information
 - SAEDA Briefings
- If approached, if you suspect you have been targeted, or if you have any doubts, contact the Security Manager
 - Report any attempt (no matter the source) to obtain unauthorized information (classified or unclassified sensitive)

UNCLAS/FOUO



Commander U.S. Army Garrison, DPTMS-Security

Human Intelligence and you

- You may be approached...
 - With a direct provocation
 - With a “fishing expedition”
 - With a dangle
- Be suspicious of nosy questions ref official government business – even if unclassified
- Talk with the Security Manager if any doubts.
- Challenge need-to-know





Commander U.S. Army Garrison, DPTMS-Security

DEMONSTRATIONS

● Groups in opposition to either the German or American political or military policies may express their dissent by protests or demonstrations. If you find yourself near a demonstration, adhere to the Do's and Don't (s) listed below:

- a. **Do Not** become involved if at all possible.
- b. **Do Not** engage the protesters in discussion or name calling
- c. **Do Not** accept literature or any other items from them
- d. **Do** attempt to ignore the protesters
- e. **Do** attempt to leave the scene (if off post)
- f. **Do** enter a private establishment, e.g. stores, shop, etc
- g. **Do** request German Police assistance and escort from the area, if the situation looks like could get out of hand



Commander U.S. Army Garrison, DPTMS-Security

DEMONSTRATIONS Near Military Installations

- a. **Do** use a different entrance to the military base if the protest is obstructing the base entrance.
 - b. If on Guard Duty:
 - (1) **Do** call for Military Police assistance and instructions.
 - (2) **Do Not** use force to detain protesters penetrating the perimeter unless violence or destruction of sensitive materials is threatened or unless previously instructed differently.
- The German Police are on hand during most demonstrations and are not only better at this than the normal military guard, but may also do so without adverse publicity for either the US Army or Government.



Commander U.S. Army Garrison, DPTMS-Security

DEMONSTRATIONS

- Remember, most demonstrations in Germany are legal.
- Subjects of demonstrations may be Anti-American, Anti-NATO, etc., as well as protest against German immigration policy, etc.
- All demonstrations have the potential to turn violent. Avoid demonstrations if possible.



Commander U.S. Army Garrison, DPTMS-Security

WALK-INS

- The purpose of **Walk-In Program** is to ensure that proper actions are taken by soldiers and civilians in the handling and processing of Walk-Ins, to allow for successful intelligence exploitation. A Walk-In is anyone who contacts a member of the US Armed Forces asking for political asylum or aid in defection or who volunteers intelligence information and services. It is very important that soldiers and civilians who are contacted follow the **Do's and Don't (s) listed below:**
 - a. **Do** direct the individual to the Contract Security Guards/ Gate, have them to contact the Security manager/ S-2 or Military Police during duty hours / MPs after duty immediately
 - b. **Do** direct the individual to the USAG Heidelberg Watch Officer after duty hours
 - c. **Do Not** interrogate the individual
 - d. **Do Not** search the individual without just reasonable cause, e.g. your life or a fellow Soldier's life (or anyone) in immediate danger
 - e. **Do Not** make any commitments or promises on individual's faith or trust



Commander U.S. Army Garrison, DPTMS-Security

REPORTING FOREIGN TRAVEL

- **All personnel who plan official or unofficial foreign travel will report travel plans to local security officials and receive Travel Advisory Briefing**



UNCLAS/FOUO



Commander U.S. Army Garrison, DPTMS-Security

TRAVEL WARNINGS

- **Travel Warnings** are issued when the **State Department** decides, based on all relevant information, to recommend that Americans avoid travel to a certain country. Countries where avoidance of travel is recommended will have travel warnings as well as consular information sheets.



Commander U.S. Army Garrison, DPTMS-Security

TRAVEL WARNINGS con't

- You can also listen to travel warnings (as well as consular information sheets with facts about various countries and public announcements) 24 hours a day by calling stateside: 202-647-5225 from a touch tone phone.
- **Website: www.state.gov.**
 - **Travel Alerts & Public Announcements** > are a means to disseminate information about terrorist threats and other relatively short-term and /or trans-national conditions posing significant risks to the security of American travelers. They are made any time there is a perceived threat and usually have Americans as a particular target group.
 - **U.S. Consulate Sheets (Country Specifics)** > Consulate information sheets are available for every country in the world. They include such information as location of the U.S. Embassy or Consulate in the subject country, unusual immigration practices, health conditions, minor political disturbances, unusual currency and entry regulations, crime and security information, and drug penalties. If an unstable condition exists in a country that is not severe enough to warrant a travel warning, a description of the condition(s) may be included under an optional section entitled “areas of instability.”



Commander U.S. Army Garrison, DPTMS-Security

The Security Manager

- The Security Manager is responsible for the successful administration of the command's security program
- He/She can only be effective through the conscientious assistance of all personnel
- Please help us.





Security Awareness Briefing Conclusion

Commander U.S. Army Garrison,
Baden-Wuerttemberg, DPTMS Security

US Army Garrison Baden-Wuerttemberg

Certificate of Completion

is hereby granted to

to certify that he/she has completed to satisfaction

**ANNUAL SECURITY AWARENESS
TRAINING**