

# Information Security Briefing

---

**Your Security POCs for USAG  
Bavaria - Grafenwoehr:**

**Security Manager, 475-8121  
Security Specialist, 475-8828  
Security Specialist, 475-7138**



UNCLASSIFIED

# References

- **DoD Directive 5200.1 (Volumes 1-4)**  
**Information Security Program**
- **AR 380-5**  
**DA Information Security Program**
- **USAREUR/AE Supplements**
- **Commander's Guide To Incident Reporting**
- **USAG Bavaria Computer Incident Handling Pamphlet**



# Information Security

## 1. **Classified Information**

Levels & definitions

## 2. **Access**

Clearance + Nondisclosure Agreement + Need to Know

## 3. **Violations & Reporting Procedures**

It is **EVERYONE'S** responsibility to safeguard information & report violations



# What is classified information?

Official government information that has been determined to require protection, and has been so designated

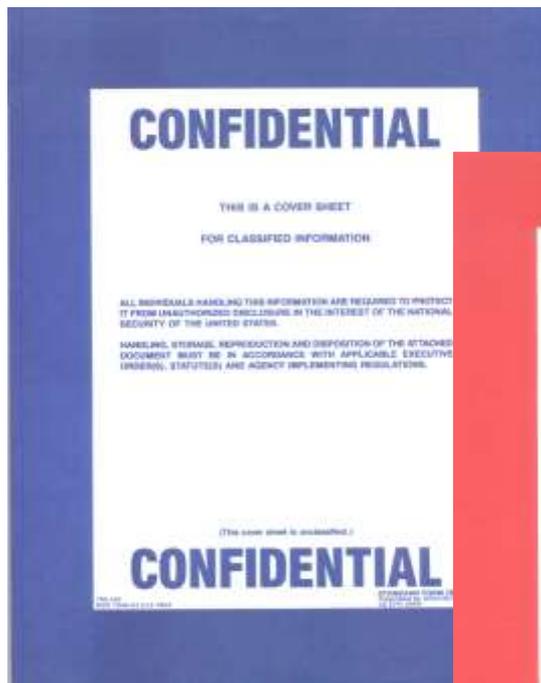
**Confidential – unauthorized disclosure will cause damage to our national security**

**Secret – unauthorized disclosure will cause serious damage to our national security**

**Top Secret – unauthorized disclosure will cause exceptionally grave damage to our national security**

# Recognizing Classified Documents

Classified material that has been removed from storage must have one of these coversheets attached.



**SF 705**



**SF 704**

UNCLASSIFIED



**SF 703**



# Recognizing Classified Information

- **Physically marking classified information serves to warn and inform holders of the degree of protection required.**

- **Overall classification & Page markings**

- **Top Secret**
- **Secret**
- **Confidential**

- **Portion (paragraph) markings**

- (TS), (S), (C) & (U)

- **Declassification instructions**

- Derived From, Date of Source, and Declassify On



**SECRET**

**SECRET**

(U) Ideally maps have the classification marking inside the borders. Otherwise, it must be marked immediately outside the map area.

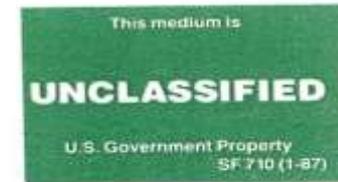
(C) Each paragraph must be marked with classification markings.

Classified By: John Smith, Ops NCO  
Derived from: OPORD209-X  
Date of Source: 1 Jan 2007  
Declassify on: 20171015

**SECRET**

Classification markings are for training purposes only

# Recognizing Classified Media



Always indicate highest Classification contained on the media:

- SF 710 (Unclassified label – Green)
- SF 708 (Confidential label – Blue)
- SF 707 (Secret label – Red)
- SF 706 (Top Secret label – Orange)

UNCLASSIFIED

# Access to Classified Information

In order to be granted access to classified information, you must have:

- ✓ Appropriate security clearance eligibility
- ✓ Nondisclosure Agreement (NDA)
- ✓ A need-to-know

*Never share classified information in your possession with anyone who does not have these three things!*



# Safeguarding

**All DA personnel** have the responsibility to safeguard national security information.

**All DA personnel** will report security violations.



# Security Violations

- **A security violation or infraction is any breach of security regulations, requirements, procedures or guidelines, whether or not it leads to a compromise of classified information.**
- **Individuals who commit security violations may be reported in JPAS (incident/derogatory report).**
- **In some cases, security violations may result in a revocation of security clearance, UCMJ or other civil/criminal action.**



# Security Violations

If you find classified material left unattended (for example, in a rest room or on a desk), it is **your responsibility** to ensure that the material is properly protected.

1. **Safeguard** the information immediately, even if you don't have a clearance.
2. **Contact** your Security Manager or S2 immediately.

**Unsecured !**



# End of the Day Security Check

- Check the entire work area for classified and sensitive materials
- Check the container to ensure it is locked
  - SF 702 required for all “Safes”
- Record checks on SF 701 (Activity Security Checklist)
  - Mandatory for Secure/Classified Storage Areas
  - Recommended for offices with Privacy Act, FOUO, or Personally Identifiable Information (PII)

ACTIVITY SECURITY CHECKLIST		DIVISION/BRANCH/OFFICE		ROOM NUMBER		MONTH AND YEAR																										
		S-2, 002D 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 off the items listed below.																												
TO (if repair)		FROM (if repair)		THROUGH (if repair)																												
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, workstations and other surfaces and receptacles are free of classified material.	✓	✓	✓	✓	✓																											
3. Windows and doors have been locked (where appropriate).	✓	✓	✓	✓	✓																											
4. Typewriter ribbons and RDP devices (e.g., disks, tapes) containing classified material have been removed and properly stored.	✓	✓	✓	✓	✓																											
5. Security alarms and equipment have been activated (where appropriate).	✓	✓	✓	✓	✓																											
6. LIGHTS OUT	✓	✓	✓	✓	✓																											
7. COMPUTERS OFF	✓	✓	✓	✓	✓																											
8. CABINETS LOCKED	✓	✓	✓	✓	✓																											
9. XOV/IA SECURED	✓	✓	✓	✓	✓																											
INITIAL FOR DAILY REPORT																																
TIME	1630	1631	1630	1630	1630																											
	Y.M.M	G.H.F	Y.M.M	Y.M.M	G.H.F																											



Classified material is not personal property!



*You can't take it with you.*

# Incident Reporting is Everyone's Responsibility



**COMMANDER'S GUIDE  
TO  
INCIDENT REPORTING**

**COMMANDER'S RESPONSIBILITY**  
Commanders are required to expeditiously report any adverse (derogatory) information to the DoD Consolidated Adjudication Facility (DoD CAF).

**REPORTING RELEVANCE**  
The security clearance process relies on three distinct functions, background investigation, adjudication, and continuous evaluation, to ensure trustworthy and reliable individuals are granted a security clearance. Incident reporting is an integral component of the continuous evaluation process.

**WHAT INFORMATION IS REPORTED?**  
Reportable derogatory information is information and behaviors that bring into question an individual's trustworthiness, judgment, and reliability to protect classified information. The National Adjudicative Guidelines provide a basis in determining what is reportable.

- Submit an incident report in the JPAS and informally suspend access until more information develops.
- Debrief access in JPAS and record locally.
- Allegiance to the United States
- Foreign Influence
- Foreign Preference
- Sexual Behavior
- Personal Conduct
- Financial Considerations
- Alcohol Consumption
- Drug Involvement
- Psychological Conditions
- Criminal Conduct
- Handling Protected Information
- Outside Activities
- Use of Information Technology Systems

U.S. Army Deputy Chief of Staff, G-3 (DAMG-C3) Memo  
Subject: National Adjudicative Guidelines for Determination  
for Access to Classified Information and other Purposes  
Art 13

**RESOURCES**  
[http://www.apd.army.mil/pdf/bsw340\\_07.pdf](http://www.apd.army.mil/pdf/bsw340_07.pdf)  
<http://www.dams.army.pentagon.mil/Info/PerSecInfo>  
<http://www.dlc.mil/whs/dowatches/compes/pdf/022002>  
<http://www.dams.army.pentagon.mil/Info/PerSecInfo>  
[http://www.dss.mil/documents/facility\\_clearance/03L-2011-04.pdf](http://www.dss.mil/documents/facility_clearance/03L-2011-04.pdf)

**INCIDENT REPORT PROCESS**

**Classified Spillage Reporting  
Actions**

The majority of spillage incidents result from careless methods, shortcuts, or untrained users who have intentionally or accidentally compromised sensitive and classified information vital to national security and operational processes. Follow these quick reference guidelines in the advent of a Spillage.

**DO:**

- Isolate and guard the affected IS(s) immediately.
- Disconnect network connections.
- Implement your Command's spillage incident response plan immediately.
- Restrict physical access to the IS or media until your security manager or IAM/IASO provides guidance.
- Complete initial unit information and Immediate Action Checklist.
- Provide Immediate Action Checklist to designated individuals (i.e. IASO/IAM/SA/NA etc).
- Notify Servicing Signal Battalion Information Assurance Staff.

**DO NOT:**

- Investigate actions on the IS until authorized by Commander or information security personnel.
- Contact any commercial Internet service provider (ISP) or ISP account identified.
- Confirm or deny a spillage incident occurrence in the public sector.
- Confirm or deny the compromise of sensitive or classified information in the public sector.
- Delay implementation of containment procedures awaiting notifications of key personnel.

# Information Security Briefing

---

*Contact your  
Security  
Manager, S-2  
or the Garrison  
Security Office*



## USAG Bavaria Security Office

Security Manager ■ 475-8121

Security Specialist ■ 475-8828

Security Specialist ■ 475-7138

UNCLASSIFIED