SECURITY MANAGER DUTIES AND RESPONSIBILITIES
SECURITY IS A COMMAND FUNCTION.

RESPONSIBILITY FOR SECURITY IN A UNIT LIES WITH THE COMMANDER
SECURITY AREAS

- Information Security
- Personnel Security
- Operations Security (OPSEC)
- Physical Security
- Information Systems Security
- Communications Security (COMSEC)
- Anti-Terrorism / Force Protection (AT/FP)
SECURITY MANAGER RESPONSIBILITIES

- Program Management
- Personnel Security Program
- Information Security
- Physical Security
1

PROGRAM MANAGEMENT

• General Responsibilities
• References
• Training and Education
• Inspections and Evaluations
• Record Keeping
GENERAL RESPONSIBILITIES

- Advise/Represent Commanders
- Security Education Program
- Oversee Access to Classified Information
- Classification Guidance
- Classification Review
- Classified Document Management
- Security Inspections
- Advice and Assistance on Regulation Enforcement
- Security Point of Contact
- Standard Operating Procedures
REQUIRED REFERENCE MATERIALS

• AR 380-5, DA Information Security Program
• AR 380-13, Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations
• AR 380-53, Communications Security Monitoring
• AR 381-12, Subversion and Espionage Directed Against the US Army
• AR 380-67, Personal Security Program
• AR 381-10, US Army Intelligence Activities
• AR 380-19, Information Systems Security
• V Corps PAM 380-1, Security Manager’s Reference Guide
• Applicable Unit/Section/Activity Security SOPs
ADDITIONAL USEFUL REFERENCES

AR 340-17, Release of Information and Records From Army Files
AR 380-20, Restricted Areas
AR 381-20, US Army Counterintelligence Activities
AR 525-13, The Army Terrorism Counteraction Program
AR 530-1, Operations Security
AR 530-2, Communications Security
AR 380-40, Policy For Safeguarding and Controlling Communications Security (COMSEC) Material
TB 380-41-1, Procedures For Safeguarding, Accounting, and Supply Control of COMSEC Material
• Security Education Program
• Refresher Briefings
• SAEDA
• Force Protection Briefings (Level I)
• Foreign Travel Briefings
Initial Security Training and Refresher Briefings Must Include:

• Individual Responsibility to Protect Classified Information

• Proper Use of the Classification System

• Security Requirements of the Individuals Particular Assignment

• Techniques Used By FIS to Obtain Classified Information and the Obligation to Report These Attempts
Initial Security Training and Refresher Briefings Must Include:

- Penalties of Espionage
- Prohibition of Discussing Classified Material Over an Unclassified Telephone
- Instructing Personnel of Requirements to Have Access to Classified Information
- Obligation to Report Deficiencies, Compromise of Classified Information or Adverse Information on Individuals with Security Clearances
- Sensitivity of Intelligence Information
Subversion and Espionage Directed Against the US Army (SAEDA):

• Initial SAEDA Briefing and Annual SAEDA Training IAW AR 381-12

• Security Managers request assistance from local CI Detachments
Anti-Terrorism/Force Protection (AT/FP) Brief:

- Level I briefs given during inprocessing at inprocessing centers
- Refresher training required annually; Level II instructor required
- Level II training required for unit AT/FP officers; recertify every three years
- Additional briefs required for personnel traveling in high risk areas
Foreign Travel Briefings:

• Information Briefed IAW AR 380-5

• Personnel with access to classified information who will be in contact with foreigners when traveling or on official business
INSPECTIONS AND EVALUATIONS

• Announced Inspections
• Unannounced After Duty Hours Inspections
• Duty Hours Spot Checks
• Advice and Assistance Visits
• Security Evaluations
Announced Inspections

Preparation and Inspection:

• Review security SOPs, previous inspection reports and other records
• Establish depth and scope of inspection
• Review inspection checklist
• Determine necessary resources
• Schedule inspection with the unit
• Provide in brief and exit brief

Inspection report must be written with findings, recommendations, and comments. One report is filed and one is given to inspected unit.
Unannounced After Duty Hours Inspections

Preparation and Inspection:

• Review security SOPs, previous inspection reports and other records
• Arrange for access to work areas
• Provide an exit brief to inspected security manager or SDO

Inspection report will be a copy of the checklist. One report is filed and one is given to inspected unit’s security manager
Duty Hour Spot Checks

- Quarterly
- Security managers discretion for scope and areas to be checked
- Personnel who handle classified material in their daily operation

Inspection report will be a memorandum for record
Advice and Assistance Visits

- Security Managers will be available to subordinate security managers; quarterly visits
- Solely for assisting subordinate security managers
Security Evaluations

• All staff elements, DISCOM, battalions and companies which handle, process, or store classified information are subject to annual announced security evaluations and annual unannounced evaluations.

• Personnel from G2, CI or DISCOM S2 will conduct these inspections.
Security Managers must maintain written records of all actions pertaining to security and must be in one location for easy access. The records must include:

- SAEDA training records
- Announced security manager inspection results
- Annual file inspections for classification downgrading
- Certification of reproduction equipment
- Authorization for restricted areas and open storage areas
Security managers must maintain written records of all Actions pertaining to security and must be in one location for easy access. The records must include:

- Security clearance actions
- Security manager appointment orders
- Security reference material
- Reports of security evaluations
- Debriefings