

Security / Iron-net and You



Commander's Directed Training CY 17

Welcome

- Exits
- Restrooms
- Silence cell phones
- 60 minutes



Security / Iron-Net and You Awareness Level Training

Awareness of Threats to Security

See something ...

... say something.

Mission Statement

The 40th Support Command will provide professionally trained deployable military forces for civil, emergency, training, exercise and mobilization support to the California National Guard, the California State Military Department, and designated civil agencies and will be prepared to augment them during Civil Support Operations (CSO) operations.

Commander's Directed Training

- Create a Common Operating Picture
- Create a Common Skill Set
- Soldier Values
- Emergency Response and You
- Security / Iron-net and You
- Disaster Life Saving

Purpose of this Class

- Bring an awareness level understanding of security issues & potential threats
- Bring an awareness level understanding of Pre-Incident Indicators & Assessments
- Threat, Risk & Vulnerability Assessment
- Bring an awareness level understanding of Internet security vulnerabilities
- Bring an awareness of Social Media use & Interoperability Basic Concepts

Scope

- California State Military Reserve
 - Optional instruction for Common Operating Picture
 - Interpretation of outside training resources
- 40th Support Command
 - Mandatory Commander's Directed Training
 - Common Operating Foundation for Command Operations

What is Security

- The protection of something of value.
- A sense of preparation or readiness.
- A melding of multiple components to reduce vulnerabilities.
- Something in your possession.
- Something secured for you by others.
- Reducing the assets vulnerability

Types of Security

- Physical
 - Personal
 - Emotional
 - Cyber
-
- Reactive
 - Proactive



Levels of Security

- None
- Minimal
- Functional
- Aggressive
- High



Enabling Learning Objectives



The Fabulous Four



Time



Distance



Shielding



Detection

Example #1 - Secure your home

- How do I protect my home?
- Identify the threats
- Look for vulnerabilities to those threats
- Harden your home as a target, make it less vulnerable.
- Better locks, better lighting, security cameras, security alarms.
- Discuss and train security issues as a family.

Short checklist

- Make sure all door and locks work
- Be careful of what you leave open when sleeping or away.
- Inspect fences and gates.
- Spend irregular times inside looking outside to see what is going on in your neighborhood.

How Can I Be More Safe When In Public and Traveling?

ACOOK

&

071-COM-0501

071-COM-0541

Awareness is Safety in Public

- Constantly observing and recognizing the critical events or situations which are happening around you is the first and most important step in being safe in a public area.
- When you travel you are typically very public.
- We call this focus of attention situational awareness.

Situational Awareness

- Learn about where you are going.
- Research in pairs, travel in pairs.
- Practice this when you go to drill.
- Pay attention to who is watching you.
- Pre-Plan Alternate Routes (ACOOK)
- Be cognizant of all potential hazards.
- Know where the “Safe Locations” are.
- When you are in uniform you are a target

Example #2

ACOOK

Safe & Secure Travel ACOOK

- Avenues of approach
 - Cover & concealment
 - Obstacles and terrain
 - Observation fields, fields of fire
 - Key terrain features
-
- Map reading skills



Avenues of Approach

- Choke points and visibility
- Escape routes
- Friendly forces
- Enemy forces
- Visual indicators
- Audible indicators
- Coded signals
- Coordination and timing



Cover and Concealment

- Cover protects you from the hazard
 - Block wall
 - Engine block
- Concealment disguises or hides you from view
 - Bush (Foliage)
 - Sheets or netting
- ATTP 3-34.39 (formerly FM 20-3)



Obstacles and Terrain

- Obstacles can be both a friend providing separation from a hazard and a source of the hazard itself.
- Terrain can both aid impede the mission.
- Certain terrain features can provide cover or concealment.



Key Terrain Features

- Higher Key features can be seen over a greater area (Good for general location)
- Indexing features allow you to precisely locate
- Triggering features signal an expected response
- Communication features are altered subtly to provide a message

Fields of Observation (Fire)

- What is the best path to give you the observation advantage.
- You (your unit) will not be seen
- Others can be readily observed approaching you providing opportunity
 - Engage
 - Avoid
 - Follow



Warrior Tasks

- 071-COM-0501 - Move as a Member of a Team (although for combat it has great concepts)
- 071-COM-0541 - Perform Exterior Movement Techniques During an Urban Operation
- Contact your Tactical Operations Center (TOC) at the beginning and end of travel

Be Observant of Others

- See who is watching you
- What are they taking pictures of
- What appears to be their current purpose
- What is their demeanor



Rural Settings

- Although we have a significant number of soldiers with rural backgrounds, the majority of our soldiers live and work in urban settings.
- Rural areas have their own set of risks due to isolation, local environmental threats, local human threats.
- 071-COM-0815 Practice Noise, Light, and Litter Discipline.

Can I Have a Concealed Carry Permit?

- Joining the CSMR neither grants you a Concealed Carry Permit (CCP) or forbids you from obtaining one.
- You must inform your Chain of Command that you have one if you do.
- You are not allowed to bring any weapons to an armory or base unless you are POF (Personally Owned Firearms) approved.
- Declare weapon at gate (JFTB approval only).

Issued Military Weapons

- Must be authorized DA1687 Signature Card to check out any equipment
- Must be signed in and signed out DA2062 Hand Receipt
- The Hand Receipt can be enhanced by using a DA 3749 Equipment Receipt for routine check-in check-out
- Must be trained or being trained in the use of weapon in your possession.

Issued Military Weapons (Cont.)

- Do not conceal your issued weapon
- Do not enter a POV with an issued weapon
- Do not remove an issued weapon from base without prior authorization
- Same applies for disabled weapons used for parade and ceremony

What Is Terrorism?

What it *IS* and
What it is *NOT*

What Terrorism Is

- Acts of violence, unlawful force, intimidation or coercion ...
- To influence an individual or group to act differently against their will
- To promote their own social, economic, religious, environmental or political objective
- There is no silver bullet

Common Myths

- A terrorist can be simply identified by their looks.
- Terrorists fit into a specific age, sex, race, religion, economic, social, or educational pattern.
- Terrorists never do random acts
- Terrorists will not hurt those on the same side.

Lead Agency

- Department of Homeland Security
- Work in close partnership with
 - Department of Defense
 - Department of Justice
 - Department of State



Targets of Terrorists

- Government facilities
- Government officials, soldiers, police, diplomats
- Banks, financial institutions
- Symbolic public monuments
- Civilian crowds, events, ships, airplanes, trains, cars, malls, resorts
- Medical facilities, schools
- Electric power plants, dams, grids
- Water supplies and pipelines
- Communication stations and towers
- Computers and computer networks

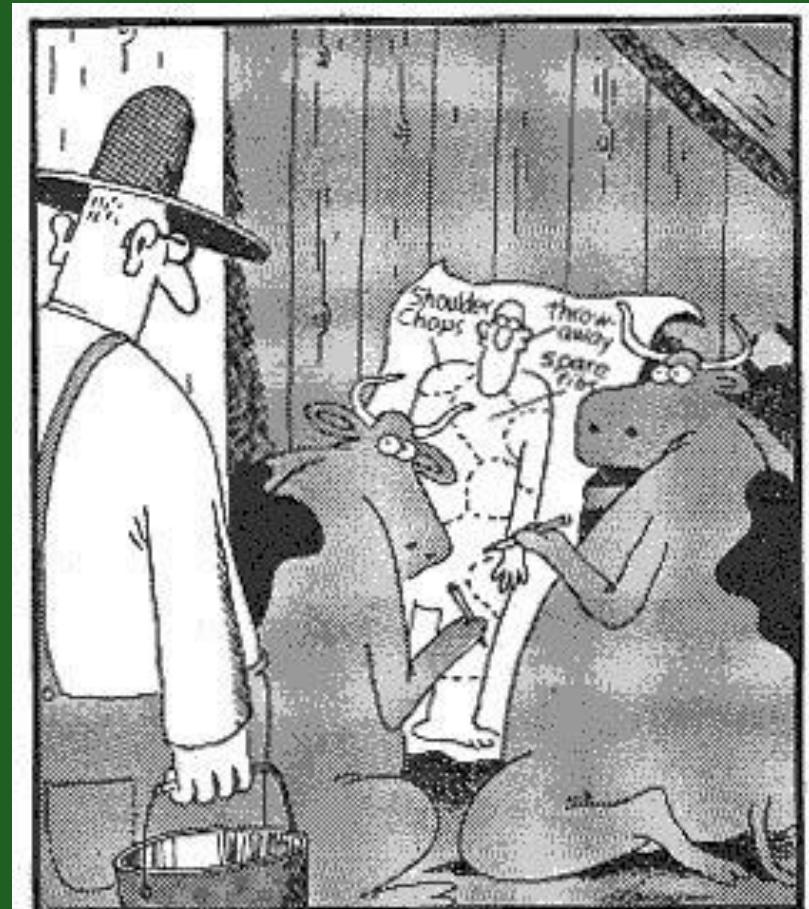


Informational Sites

- See something Say something
- Infragard www.infragard.losangeles.com
- www.csmrsoldier.com
- Lessons Learned Information Sharing
www.llis.gov
- Anti-Defamation League www.adl.org
- Tripwire

Recognizing Pre-Incident Indicators

Awareness Level
Situational Awareness



Farmer Brown froze in his tracks; the cows stared wide-eyed back at him. Somewhere, off in the distance, a dog barked.

Risky Behavior

- Constant anger or jealousy towards an individual or group
- Talking about violent intents
- Short fuse
- Very quiet and withdrawn
- Never sharing or being a part of the group
- Lone wolf, isolated, alone against the world



Phishing

- In the terrorist surveillance process they will probe you for information.
- Report unusual conversations when approached about the CSMR.
- Most people will want to simply thank you for your service.
- Probing personal questions about you, your unit or the CSMR should be politely terminated then reported through your chain of command.
- Most are press or freelance writers

Planning Stages of Terrorists

- Recruiting
- Indoctrination
- Training
- Scouting
- Targeting
- Surveillance & Planning
- Testing targets
- Test Runs
- Execution



When Do I Become a Target?

- When you put on a uniform.
- Post personal information on social media
- Display controversial images or messages on your vehicle.
- When you enter certain emergency situations
- When certain events are covered by the media creating animosity towards the military

Surveillance Video



Protect Your Uniform & ID

- Do not leave your uniform unattended in publicly accessible places.
- Keep all your identification documents secure
- Picture ID
- Birth Certificate
- Credit Cards
- Social Security Card



How do I react to an active shooter in a building?

- If you can run from the building or at least the area of the building far away or inaccessible to the shooter(s).
- Hide in a place which provides cover (best) or at least concealment (2nd choice)
- Fight wait and prepare an ambush for the shooter when he enters the room. Throw anything you have to distract him, hit him with anything you can find.

How do I react to an active shooter when in open space?

- If you can, determine where the shots are coming from, and see if you have a viable escape route then use it.
- Hide in a place which provides cover (best) or at least concealment (2nd choice)
- If in striking distance ambush the shooter. Throw anything you have to distract him, hit him with anything you can find.
- 071-COM-0815 Practice Noise, Light, and Litter Discipline.

Threat Risk & Vulnerability

- Threats what can actually go wrong
- Risks are what actually has gone wrong, how often and how damaging
- Vulnerability is how susceptible you are to each threat.
- An assessment is a structured standardized means of scoring your threat, risk and vulnerability matrix

Enabling Learning Objectives



Assessments Require Experience

- Identify Threats (What might go wrong)
- Determine if you are vulnerable to that threat
- Look up the history and see how often and how bad it has happened
- What are ways to reduce this vulnerability
- Is the benefit worth the cost?

Other Training

- Screening Persons & Observational Techniques (SPOT AWR 219) LSU
- Soft Target Frontline Responder UNLV
- Fake ID awareness through LSU
 Online Classes
- IS 106 Workplace Security
- IS 906 Active Shooter Awareness
- Run, Hide, Fight

Internet Threats, Risks and Vulnerability Awareness

Introducing Iron-net



How do I make telephone use more secure?

- Do not store passwords on your phone
- Lock your phone with a Security Code
- Keep your phone physically secure when not in use.
- See if you can install find my “phone” app.
Must install before you loose it.



Computer Security Preventative Measures

- Store critical information on a detached drive.
- Know how to disconnect and reconnect your computer to the internet.
- Install name brand anti-virus anti-spyware on your computer.
- Do not save passwords for critical information
- Surf the net through a proxy server.



Better Bookmarks

- A URL is Universal Resource Locator or www.yourbank.com
- An IP Address or Internet Protocol Address is a series of four or six numbers like this 256.123.4.56 each number will be to 256.
- IP addresses starting with .256 and .64 have the highest incidents of hacking be extra careful of these.

OPERATION IRON NET: OPORD 3004-11-01

INTERNET AND COMPUTER SECURITY TRAINING

SITUATION

- CNG
 - ARNG
 - ANG
 - CSMR
 - All Other Components
- Will Comply with HQDA directives
 - to deter
 - prevent
 - or mitigate
- continued cyber security threats within our organization



THREAT

- Recent intelligence indicates malicious cyber actors intend to target
 - US Army Networks
 - DoD users
 - and their families
- Most recent attacks concentrate on financial accounts
- Ultimate goal identity theft

Levels of Information

- Public Domain
- Copyrighted, Trademarked, or Patented
- Unclassified
 - Intellectual Property (IP)
 - Medical (PCI) & Financial Records (HIPAA)
 - Unclassified For Official Use Only (U//FOUO)
 - Law Enforcement Sensitive (U//FOUO(LE))
- Classified
- Secret
- Top Secret

Sensitive Information (SI)

- Under this OPORD Sensitive Information (SI) is any information that is not intended for public release
- The civilian equivalent is Unclassified// For Official Use Only U//FOUO
- (LE) this designation at the end means Law Enforcement Sensitive

Sensitive Information (Cont.)

- CAESADS requires a Volunteer Logical Access Card (VOLAC) or a Common Access Card (CAC) to access the intranet
- Ever-Bridge does not require a VOLAC nor a CAC but does require a user name and a password. This is accessed via internet
- These both are sensitive information

How Do I Handle U/FOUO Info?

- Printed Materials - should be in envelopes and under locked storage.
- Electronic Materials - should be only placed on Password protected computers.
- Portable drives must have a security feature must have password access or be encrypted.
- Do not send to gmail or hotmail type accounts.

Identity Theft

- Protect your Personal Information
- Passwords
- ID Cards and Uniforms



Fake Identification

- Spotting Fakes
- Criminal Offense
- Training Purposes
- Fake Military ID
- Fake LEO
- Fake Security



MISSION

- All CNG and CSMR personnel will complete network security and threat awareness training and execute cyber security procedures as outlined in this annually.



EXECUTION

- Commanders / Directors will ensure all personnel within their organization complete the directed network security training and implement procedures contained in this OPORD.



REQUIRED TRAINING

- Phishing (In class or Online)
- Social Media and Operational Security (In class or Online FEMA IS-42)
- Anti Terrorism Awareness Training Level 1 (in class or online)
- AKO registration (non sponsored and sponsored accounts)
- Many online classes require an AKO Account or some form of registration

ONLINE TRAINING SITES

- AKO registration www.us.army.mil
- Anti Terrorism Level 1
<https://atlevel1.dtic.mil/at>
this class.
- Phishing and Social Media
<https://ia.signal.army.mil/courses.asp>
or FEMA IS-42



Social Media

Rules of Thumb for Safe Use

What is Social Media

- Facebook
 - Twitter
 - Linked-In
 - Pinterest
 - MySpace
-
- FEMA Independent Study IS-42



Adding us on
FACEBOOK



Follow us on
TWITTER



Subscribe to our
RSS FEED



Circle us on
GOOGLE+

General Rules

- Do not post upcoming training, deployments or operational plans.
- Do not post current activities
- Get approval from Company Commander or higher before posting anything related to CSMR
- When in doubt place request in writing using Form 601-1

Safe Phone Use

- Do not have sensitive conversations if others are listening.
- Do not “eaves drop” yourself.
- Store your phone in a secure place when not in use.
- Report your stolen or lost phone upline.

Safe Computer Use

- Name brand anti-virus anti-spyware get updates sooner than off brands that is what you are paying for.
- Physically protect your computer (especially lap-tops) from physical theft.
- Be careful when surfing the net
- Shop for a proxy server.
- Be careful of “Free” software

Using Credit Cards Online

- Use secure connection - Look for https://
- Trusted Companies
- Know your card provider's policy
- Watch credit/debit card receipts
- Look for security certificate



If you think you are hacked

- Unplug the internet cable or turn off the WiFi connection.
- Run your anti-virus anti-spyware
- Inform your CoC.
- If hacking is confirmed report to local Law Enforcement Officers and sometimes the Federal Bureau of Investigation.
- Be careful and save yourself the embarrassment.

Basic Interoperability Concepts

Simple Do's and Don'ts to Achieve
Interoperability

If You Cannot Share

- Failure to share data will result in failure to protect
- Interoperability allows the proper sharing of information, space, resources and personnel
- DHS appointed by the President to set the standards for our entire Nation for Interoperability.
- It is not just radios!

Interoperability Concepts

- Information
- Equipment
- Standards
- Sharing
- Back-up/Alternatives
- Absence of Conflicts
- Cooperative Training
- Common Operating Picture



Information sharing

- Word, Excel, PowerPoint Adobe Acrobat
- Pictures .jpg .gif .bmp
- Filename.doc vs. Filename.docx
- Filename.xls vs. Filename.xlsx
- Filename.ppt vs. Filename.pptx
- Five Paragraph Order & ICS Forms

Interoperable Equipment

- Fire Hydrants
- Telephones
- Radios
- Computers
- Gasoline, Diesel, etc
- Power supplies

Use of Standards

- Standards already required
- Standards already in use
- Combining standards
- Developing new standards
- Standard Forms
- Standard Terms

Sharing

- Sharing information, ideas, training, equipment as permitted
- A Test is worth a thousand expert Opinions.
- Work out conflict prior to actual need.



Back-up & Alternate Systems

- Keeping both primary and back-up systems on same file system and same software updates
- Shared back-up systems
- Shared alternate sites
- Teamwork
- Same level of security!

Conflicts & Interoperability

- Conflicting Standing Orders
- Conflicting Personalities
- Conflicting Rules of Engagement
- Conflicting Areas of Operation
- Conflicting Operating Platforms



Interoperability Goal

- Common Operating Picture
- Common Operating Environment
- Better communication
 - Less misunderstanding
 - Easy but secure sharing
- Establishing standards only when necessary
- Balanced and aligned - Unified Command

What Now

- Take some Independent Study classes listed in this presentation.
- Fine Tune your Warrior Tasks & Drills
- Be more aware of your daily routines
- Change your bad habits
- Pick a battle buddy to police and challenge one-another to achieve better Operational Security OPSEC

Vision Statement

The 40th Support Command will provide a ready competent professional reserve to support the California National Guard in their civil support training, and military operations missions, and to augment National Guard and emergency civilian response authorities to natural and man-made disasters.

Questions?



Conclusion
Commander's Direction Training
Security Awareness Module



CY 17



PROPERTY ACCOUNTABILITY AND PHYSICAL SECURITY

U/FOUO/UNCLASSIFIED



PROPERTY ACCOUNTABILITY AND PHYSICAL SECURITY



- Purpose: to provide a refresher on property accountability and an awareness of Army physical security.



Agenda

- Government Property Accountability
 - Equipment
 - Sensitive Items
 - Weapons
- Physical Security



Government Property

- OCIE
 - Your personal equipment
- Unit/Section Equipment
 - Tentage, Radios, Vehicles, Anything Green
- Vehicle BII
 - Driver or TC responsible for



Accountability

- Delegation of Authority (DA 1687)
 - Officer with fiscal responsibility authorizes which individuals are to be issued which property
- Hand Receipt (DA 2062)
 - Used to document who got what and when
- Equipment Receipt (DA 3749)
 - Used for kits, weapons, radio/battery/accessory or items frequently checked and returned by same person



Sensitive Items

- Cannot be lost
- Report immediately to the chain of command if missing
 - Comsec equipment
 - Weapons
 - Certain Technology
 - SINCGARS
 - NBC Alarms, NVG's



Weapons

- Individuals issued arms are responsible for their security at all times.
- Each issued weapon will be carried on the person at all times.
- Weapons will not be entrusted to the custody of another person.
- Pistols will be secured with a lanyard.
- AR 190-11



Responsibility

- You are responsible for all US Army equipment you sign for.
 - You can be charged for missing or damaged equipment.
- If you lose it, report it!
 - A field loss can be investigated if reported immediately. You buy it on the showdown.



Physical Security (Defined)

“That part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material and documents, and to safeguard them against espionage, sabotage, damage, and theft.”

AR 190-16



What Does That Mean?

- Physical security is meant to counter the threat during peace and war.
- Threat can range from enemy forces to terrorists to civilian criminals or saboteurs.



How to Practice Physical Security



- Limit Access
- Secure Equipment
 - Guards
 - Locks
- Physical Barriers
 - Fences
 - Buildings



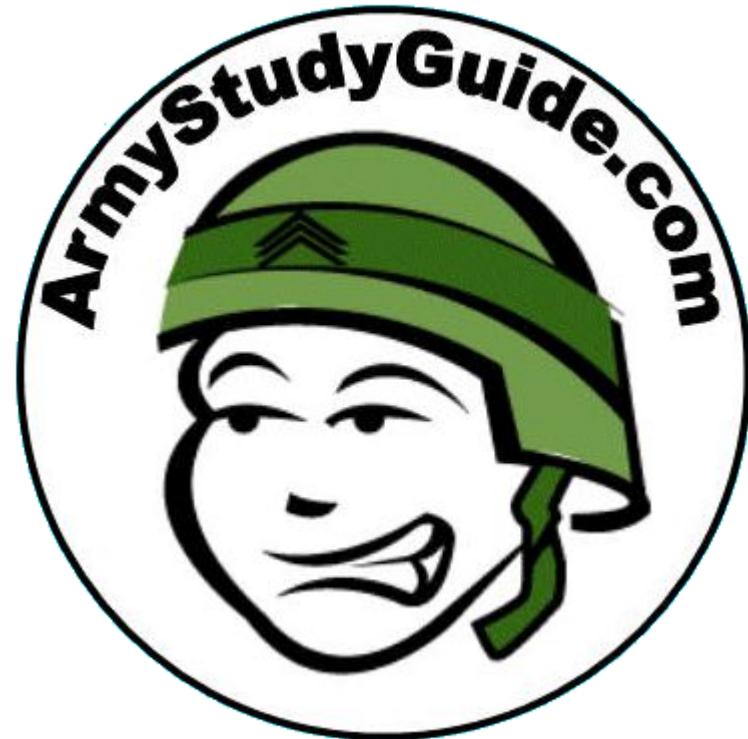
Access

- Military Installations (Armories) will have access control.
 - Installation Specific
- Varies based on Threat.



Conclusion

- Secure equipment!
- Remember – You signed for it, you own it.
- Treat your weapon as if your life depends on it!
- Limit access! “Should that person be here?”





BREAK

Five minute

PHYSICAL & PERSONNEL SECURITY

For the CSMR

TERMINAL LEARNING OBJECTIVE

- ◆ ACTION: Understand a unit physical security plan and personnel security policies
- ◆ CONDITION: CSMR will support CANG in various environments, to remain compliant with AR 380-67 & FM 3-19.30 (08 JAN 01)
- ◆ STANDARD: Maintain a unit security plan and personnel security policies which safeguard the unit's assets from theft, loss, misuse, and sabotage in accordance with FM 3-19.30

ADMINISTRATIVE REQUIREMENTS

- ◆ ENVIRONMENTAL CONSIDERATIONS:
 - ↳ Physical accessibility and public visibility
- ◆ SAFETY REQUIREMENTS:
 - ↳ Composite Risk Assessment
- ◆ RISK ASSESSMENT LEVEL:
 - ↳ Low – Classroom Formation Parade
 - ↳ Medium – Severe weather, strenuous
 - ↳ High – Threat to life or limb (Grave Danger)

REFERENCES

- ◆ AR 190-51 The Army Physical Security Program
- ◆ FM 3-19.30 Physical Security
- ◆ Update 10-3 Physical Security Update
- ◆ AR 380-67 Personnel Security Program
- ◆ Memo Subject: Single Scope Background Investigation (SSBI)

OUTLINE

- ◆ **Maintain a unit physical security plan**
 - ◆ MEVAs
 - ◆ Categories & Risk.
 - ◆ AA&E
 - ◆ POW & Ammo
 - ◆ Deterrence Measures
- ◆ **Match your unit personnel security plan to the mission**
 - ◆ Components & Responsibilities
 - ◆ NAC / NACI / SSBI
 - ◆ Eligibility
 - ◆ Interim & Final Clearances
 - ◆ Derogatory Information
 - ◆ Commanders Options

AR 190-51

- ◆ Security requirements equal type of equipment or property relative to the level of threat



UNIT PHYSICAL SECURITY

- ◆ ACTION: Maintain a Unit Physical Security Plan
- ◆ CONDITION: Given a requirement to protect Army property at unit level, the risk level from a physical security risk analysis, and FM 3-19.30, and Physical Security Update 10-3

UNIT PHYSICAL SECURITY

- ◆ STANDARD: Developed a unit security plan that implements measures safeguarding the unit's assets from theft, loss, misuse, and sabotage in accordance with FM 3-19.30, and Physical Security Update 10-3

MEVAS

(MISSION ESSENTIAL VULNERABLE AREA)

- ◆ Information
 - ◆ Equipment
 - ◆ Property
 - ◆ Facilities
-
- ◆ What's Mission Essential?
 - ◆ METL review

Require Increased
Measures



SAMPLE MEVAS

- ◆ Arms, ammunition, and explosive storage areas
- ◆ Airfields
- ◆ Field maintenance shops
- ◆ Motor pools



Patriot



CATEGORIES OF ARMY PROPERTY

- ◆ Aircraft and components at army aviation facilities
- ◆ Aircraft and components not at army aviation facilities
- ◆ Communications and electronic equipment and night vision devices
- ◆ Repair parts not at installation level support activities and direct support units
- ◆ Aircraft and vehicles with classified onboard equipment or components
- ◆ Mission essential Industrial and utility equipment

CATEGORIES OF RISK

- ◆ **Level I**
- ◆ **Level II**
- ◆ **Level III**
- ◆ Each level involves:
 - ◆ Physical Protective Measures
 - ◆ Security Procedural Measures
 - ◆ Terrorism Counteraction Measures

CLASSIFIED MATERIAL

- ◆ Coordinate with S2 or MI representative
- ◆ Programs and systems
 - ◆ Top Secret
 - ◆ Secret
 - ◆ Confidential
 - ◆ For Official Use Only (FOUO)



AA&E (ARMS, AMMUNITION, EXPLOSIVES)

- ◆ Complex storage requirements - Call your Post Physical Security Officer



AA&E MEASURES

- ◆ Positive control
- ◆ Lanyards in the field
- ◆ Approved storage facilities and containers
- ◆ Inventories
- ◆ Key and lock control
- ◆ Transportation measures



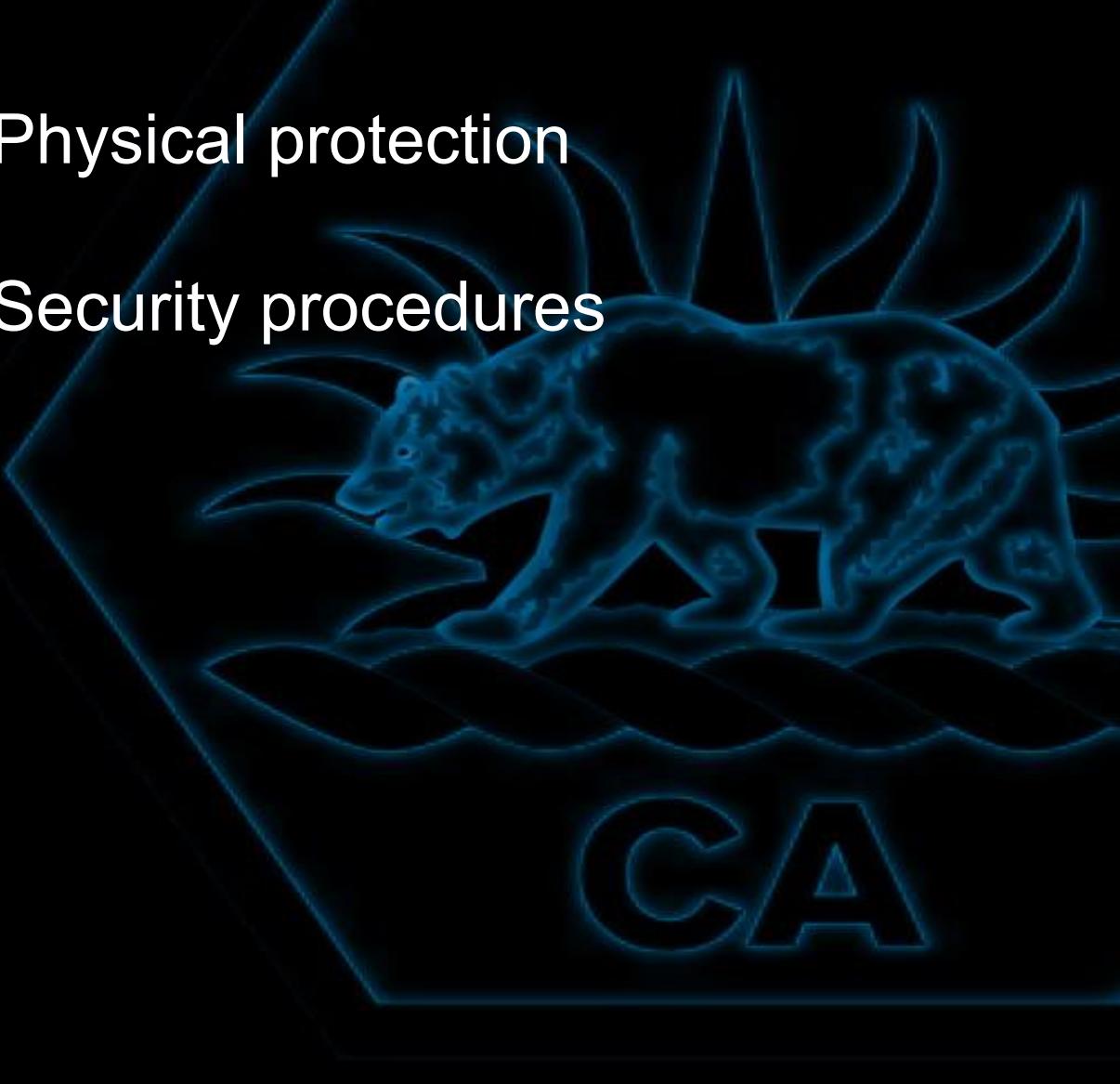
PRIVATELY OWNED WEAPONS AND AMMUNITION

- ◆ Locked container
- ◆ Properly registered
- ◆ Stored separately
- ◆ Received
- ◆ Approved issuance
-(The Commander)



PHYSICAL SECURITY MEASURES

- ◆ Physical protection
- ◆ Security procedures



HARDEN THE TARGET - DETERRENCE

- ◆ Protective barriers
- ◆ Lighting
- ◆ Access Control
 - ◆ Barriers
 - ◆ Procedures



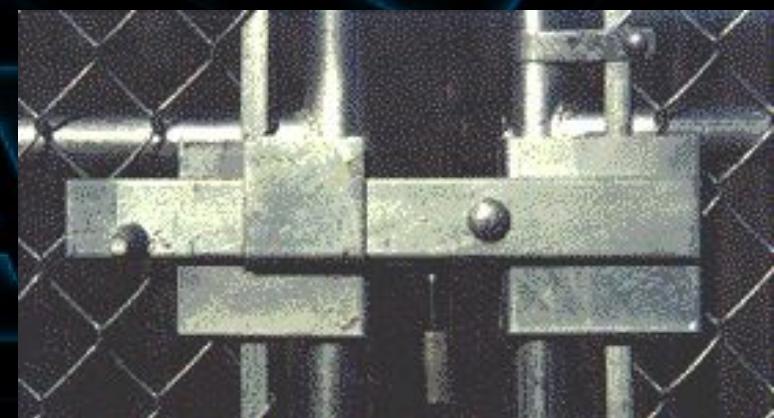
WARNING SIGNS

- ◆ Warn intruders of the area restrictions
- ◆ Must be at entry points
- ◆ Must be at intervals of 100 feet
- ◆ Must be multi-lingual when appropriate



LOCK TYPES

- ◆ Dead bolt latches
- ◆ Combination locks
- ◆ Cipher locks (push button) keyed padlocks which include:
 - ◆ High security padlocks
 - ◆ Medium security padlocks
 - ◆ Low security padlocks



GUARD FORCE OPERATIONS

- ◆ Organizational guidance:
 - ◆ Fixed
 - ◆ Mobile
 - ◆ Reserves
 - ◆ Combination
- ◆ Operational guidance:
 - ◆ SOP
 - ◆ General orders
 - ◆ Special orders
 - ◆ Temporary orders

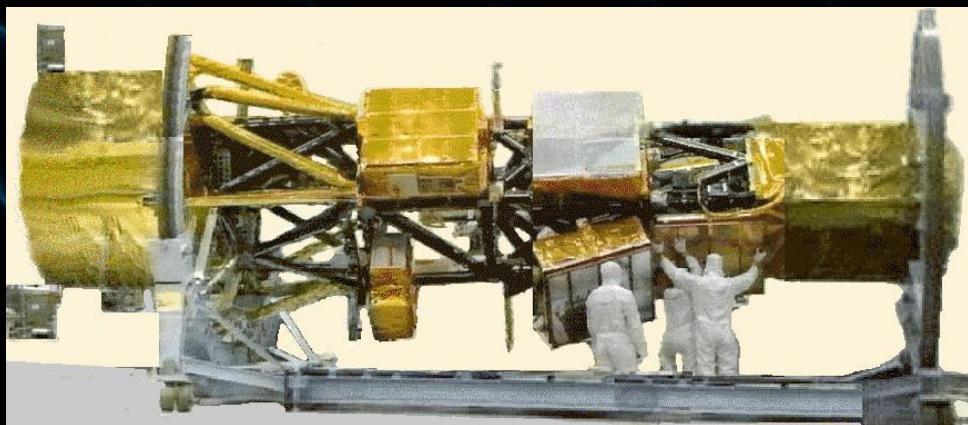
Written Annex to Unit Security Plan

OBJECTIVES

- ◆ Ensure only properly investigated personnel receive clearances
- ◆ Remove clearances from personnel who become vulnerable or unsuitable for continued access

COMPONENTS

- ◆ Determine and document what positions require access
- ◆ Control the granting of access to classified information
- ◆ Program for the withdrawal or denial of access



COMMANDER / FIRST SERGEANT

RESPONSIBILITIES

- ◆ Determine and document personnel positions which require access
- ◆ Assign personnel to fill vacancies requiring such access



SECURITY MANAGER

RESPONSIBILITIES

- ◆ Implement and monitor a security education and training program
- ◆ Assist candidates in preparation of forms
- ◆ Complete local records checks and processing interim and final clearances



NATIONAL AGENCY CHECK (NAC)

- ◆ Records check of designated agencies
- ◆ Technical fingerprint search of FBI files
- ◆ Basis for granting military personnel final **SECRET** clearance
- ◆ Periodic Review every 10 years for Secret

NATIONAL AGENCY CHECK WITH WRITTEN INQUIRIES (NACI)

- ◆ Combines NAC with inquiries to law enforcement agencies, former employers, references and schools
- ◆ Basis for granting DOD civilians final SECRET clearance

SINGLE SCOPE BACKGROUND INVESTIGATION (SSBI)

- ◆ Starts with a NAC or NACI
- ◆ Basis for Granting military personnel and DOD civilians a final **TOP SECRET** clearance
- ◆ Determines Eligibility for Sensitive Compartmented Information (SCI) access
- ◆ Requires a Periodic Reinvestigation (PR) every 5 years

SECURITY CLEARANCE ELIGIBILITY

- ◆ Must be a US citizen
- ◆ Appropriate investigation must be completed



PARAMETERS FOR INTERIM CLEARANCES

- ◆ Interim clearance is designed to accommodate field **operational** requirements
- ◆ Authority generally rests with Division, Corps, or installation security managers as delegated by their MACOM
- ◆ Definite **lifetime** (90 days, extendible total 180 days)

PARAMETERS FOR INTERIM CLEARANCES

- ◆ Actions taken leading to a final clearance musts:
 - ◆ Favorable local records check
 - ◆ Favorable review of applicable forms
 - ◆ Initiation of corresponding investigation

FINAL CLEARANCE REQUIREMENTS

- ◆ Verify full identification and citizenship
- ◆ Verify that a local records check was conducted
- ◆ Verify no break in service since completion of last investigation
- ◆ Verify the submission of a completed local files check
- ◆ Verify the submission of DA 5247-R to Central Clearance Facility (CCF)
- ◆ Consider interim clearance option (if immediate access is required)

REPORTING DEROGATORY INFORMATION

- ◆ Commanders must report credible derogatory information to CCF whether a person has a clearance or not. This establishes an historical file should a clearance ever be requested
- ◆ Derogatory information is reported on DA Form 5248-R

CA

SOURCES of DEROGATORY INFORMATION

- ◆ MP / CID reports & blotter entries
- ◆ Courts-martial / Article 15s
- ◆ Medical reports/psychiatric examinations
- ◆ Letters of indebtedness / reprimand
- ◆ Absence Without Leave (AWOL)
- ◆ Drug / alcohol incidents

LETTERS OF INTENT (LOI) TO SUSPEND / REVOKE ACCESS

- ◆ Forwarded through commander to individual
- ◆ Individual can respond in writing (60 day limit)
- ◆ Commander informs soldier / endorses acknowledgment and response to LOI
- ◆ CCF adjudicates response to LOI and furnishes commander with final determination
- ◆ CCF's determination is final (local commanders cannot ignore or overturn CCF's decision)

COMMANDER'S OPTIONS

- ◆ Commanders can **suspend access immediately**, conducts an inquiry or requests an investigation as appropriate
- ◆ Commander determines that an inquiry or investigation will be of no use - He **suspends** access immediately and **forwards** the information to CCF

COMMANDER'S OPTIONS

- ◆ The commander forwards the information but **does not suspend access** because the incident does not warrant the suspension - This allows the service member to continue to serve in their position.

Follow up 5248-Rs must be submitted every 90 days until the matter is finally adjudicated

SUMMARY

- ◆ **Maintain a unit physical security plan**
 - ◆ MEVAs
 - ◆ Categories & Risk.
 - ◆ AA&E
 - ◆ POW & Ammo
 - ◆ Deterrence Measures
- ◆ **Match your unit personnel security plan to the mission**
 - ◆ Components & Responsibilities
 - ◆ NAC / NACI / SSBI
 - ◆ Eligibility
 - ◆ Interim & Final Clearances
 - ◆ Derogatory Information
 - ◆ Commanders Options

CLOSING THOUGHT

- ◆ Physical Security and Personnel Security are only as good as you make them. They may seem successful, but you cannot tell until you evaluate and implement, maintain supervision, and maintain ever constant vigilance.
- ◆ If you think this is not necessary, think about the FBI & Robert P. Hanssen
 - aka “B”*
 - aka “Ramon Garcia”*
 - aka “Jim Baker”*
 - aka “G. Robertson”*
 - Aka “Alleged Traitor”*



PHYSICAL & PERSONNEL SECURITY

For the CSMR

Concluded

Security / Iron-net & You



Commander's Directed Training

U//FOUO - Unclassified for Official Use Only