Virginia Army National Guard
Personnel Security
Initial Security Education Briefing

12 May 2005
References:

- AR 380-5 Department of the Army Information Security Program, 29 September 2000
- DoD 5200.2-R Personnel Security Program, January 1987 (with changes to 8 Nov 1995)
- E.O. 12958 Classified National Security Information, as Amended 25 March 2003
A security clearance is a determination of trust, which makes you eligible for access to classified information.

A security clearance is not permanent. It expires at a time frame dependent on the type of investigation - 10 years for Secret and 5 years for Top Secret.
Requirements for holding a security clearance

- Attend a briefing designed to teach you proper procedures for handling and protecting classified information. Attend a refresher briefing each year. For reference see: www.archives.gov/isoo/security_forms/standard_form_312.pdf

- Sign a Non-Disclosure Agreement (SF-312)
What is an SF-312 Non-Disclosure Agreement?

- A legally binding agreement between US Government and you. It is a life long agreement.

- It is to ensure that you understand the damage to National Security which could occur from unauthorized disclosure of classified information.
SF-312 Non-Disclosure Agreement

- Agree to pre-publication review

- Classified information is United States GOVERNMENT PROPERTY. It is NOT yours to disclose in any way
SF-312 and the Penalties of Disclosure

Should you improperly disclose classified information

Under E.O. 12958, Section 5.5. Sanctions:
SF-312 and the Penalties of Disclosure

- Loss or denial of security clearance
- Termination of employment
- Criminal prosecution (prison/fines)
- Loss of monetary gains made from improper disclosure
National Security Information

Official information which relates to the national defense or foreign relations of the United States, which has been deemed to require protection from unauthorized disclosure.
National Security Information

There are levels of classification to describe national security information. Unauthorized disclosure of this information could cause damage to our nation’s security

- CONFIDENTIAL - Damage
- SECRET - Serious Damage
- TOP SECRET - Exceptionally Grave Damage
The Threat

Why must we protect classified information?

- Economic espionage is on the rise
- Intelligence needs are economic as well as military
- Present/former adversaries and our allies are conducting intelligence activities against us.
“Countries don’t have friends, they have interests”

Charles deGaulle
The Threat

- Don’t forget the insider!
- Counterintelligence is your responsibility
- Report suspicious activities to your Security Officer immediately
Classification of Information

How does information become classified?

- **Original Classification**: initial determination that information, in the interests of national security, needs protection

- **Derivative Classification**: incorporating, paraphrasing, restating, or generating in new form, information that is already classified
National Security Information

Classified information must fall under one of the following categories:

- Military plans, weapons systems or operations
- Foreign government information
- Intelligence activities, sources or methods to include cryptology
- Foreign relations or foreign activities of the U.S., including confidential sources
National Security Information

- Scientific, technological, or economic matters relating to national security, which includes defense against transnational terrorism

- Programs for safeguarding nuclear materials or facilities

- Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to national security, which includes defense against transnational terrorism

- Weapons of mass destruction
Reasons to NOT classify information

- To conceal violation of law, inefficiency, or administrative error
- To prevent embarrassment to a person, organization, or agency
Reasons to NOT classify information

- To restrain competition

- To prevent or delay the release of information that does not require protection in the interests of national security
Declassification

Documents are marked for automatic declassification within ten years unless:

- The document is exempt from automatic declassification at 10 years under E.O. 12958. Additional reviews at 10 and 5 year intervals

- All classified documents are declassified at 25 years (with a few exceptions).
Marked Documents

- Title and/or subject should be marked
- Paragraphs and sub-paragraphs must be marked
- Illustrations and pictures also
Marked Documents

- Overall classification is determined by the highest portion marking

- Classification marked on top/bottom of every page
Derivative Classification

- When incorporating classified information, be sure to:
  - Observe and respect original markings.
  - Carry forward all classification markings.
  - Carry forward declassification instructions (using the most stringent)
  - List all sources
Accountability of Classified Information

Required for both Secret and Top Secret
Accountability:

- Identify who, what, when, where, how

- Annual inventory is required!

- Use cover sheets and classified receipts!
Storage of Material

- Sensitive, For Official Use Only (FOUO), Privacy Act, proprietary information must be stored under one level of lock (desk, drawer, file cabinet)

- Classified information must be stored in a GSA approved security container (safe)

- Note that each safe should have a SF700, SF702 and open/closed sign
Combinations

- Security container combinations are classified at the level of information in the safe

- Should always be memorized; never write them down

- Don’t share with anyone who does not need to know it
Combinations

- Change your combination when:
  - the security container is found open and unattended
  - someone who has the combination leaves
  - if you feel the combination has been compromised
  - when the security container is taken out of service
Control and Access

- You are responsible for protecting and controlling classified information.

- You must limit access to authorized persons by verifying:
  - Identification
  - Clearance
  - Need to know

You are responsible for allowing proper access to your material!!
LEAKS

- Most leaks result from:
  - Casual conversations
    - Don’t discuss classified information outside the office!
  - Open Sources
    - Publication does not infer declassification!
Transmission: Telephone/Fax

- Standard and cell phones are not secure

- Is there a secure phone in your office? If not, where is the nearest one?
Transmission: Double Wrapping

- Must be done to prepare for hand carry, courier, or US Postal
- Affords 2 layers of protection
- Protects against damage
- Use opaque envelopes
- Don’t forget a receipt
Transmission

- **Outer Wrapping:**
  - Full address of receiver
  - Full return address
  - NO CLASSIFICATION MARKINGS
  - Recommend that you put “If undeliverable, return to sender”
Transmission

- **Inner Wrapping:**
  - full address
  - Return address
  - Classification markings top/bottom and front/back
  - Information and receipt placed inside
Transmission

- **To send Top Secret:**
  - Call your security officer

- **Secret and Confidential**
  - Hand-carry
  - Approved courier
  - US Postal Service
Transmission

- **Hand Carry:**
  - No overnight stay without proper storage
  - No aircraft overseas
  - Courier: check authorization

- **US Postal:**
  - Secret: Registered
  - Confidential: Certified, Express or First class
Computer Security
Do not process classified unless:

- You have contacted your information technology rep
- Your computer has a removable hard drive
Computer Security

Do not process classified unless:

It is in a stand-alone configuration (no modem or network connection unless it has been properly accredited-SPRNET)
Reproduction

- Various ways to reproduce classified information:
  - Paper (photocopier) - MUST be approved copier for classified information...if not, DO NOT copy
  - Electronically
  - Other means (video and/or cassettes)
    - Use approved equipment for that purpose
  - Account for your copies!
Reproduction

- **Approved photocopiiers:**
  - Are in controlled environments
  - Do not have memories
  - Are sanitized after classified copies are made
  - Are serviced by cleared personnel or service personnel are monitored while repairs are made
Classified material destruction

- **Approved methods:**
  - Burning (at an approved facility)
  - Shredding (using an approved cross cut shredder)
  - Use small classified waste “burn bags”
  - Other types (FOUO, Privacy Act, Sensitive But Unclassified (SBU), etc.): SBU should be shredded using cross cut shredder. At a minimum tear up other types
Overseas Travel

- Contact your security officer for a briefing before you go
- Do not bring classified
- Limit sensitive information
- Notify U.S. Embassy of your visit
Reporting Requirements

- All employees must report contact with a foreign national who:
  - Requests classified information
  - Wants more information than they need to know
  - Acts suspiciously
  - Report incidents to your security officer immediately
End of Day Security Checks

- All security containers
  - windows/doors
  - desk tops for classified

- Complete the SF 701 “Activity Security Checklist.” The office manager is responsible for the implementation of the SF 701
Your Security Officer

- Your security officer is there to help you!

- Report to your security officer:
  - Security violations
  - Loss or compromise of classified information
  - Security incidents or problems
When You Depart VA ARNG

- If you are leaving the VA ARNG you must:
  - Turn all classified material over to your classified control point
  - Contact your Security Officer (S2) for a debriefing
  - Turn in your ID, keys, and access cards
Finally....

Who is responsible for security in the Virginia Army National Guard?

YOU ARE!
"Wow! That must have been one pretty effective security briefing!"
QUESTIONS?