# Department of Commerce
# Office of Security

## Security Education
## Refresher Briefing

# Security Clearance

- You are being rebriefed because you hold a security clearance.
- Remember, a security clearance is not permanent; it expires when you leave your position.
- Your SF-312 Non-Disclosure Agreement is still in effect.  It is a life long agreement between you and the U.S. Government.

# Improper Disclosure: Penalties

- Performance Plan:
  - Performance Rating/Awards
  - Reprimands/Suspensions (Without Pay)
- Loss of monetary gains made from improper disclosure
- Loss of security clearance
- Termination of employment
- Criminal prosecution (prison/fines)

# 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.

# The Threat cont...

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

# Marking Documents

- Title and/or subject should be marked
- Paragraphs and sub-paragraph must be marked
- Illustrations and pictures also
- Overall classification is determined by the highest portion marking
- Mark classification on top/bottom of every page.

# Marking cont...

- The bottom of the document should have the following:

  Classified by: Jack Smith, Director, OSY

  Reason for Classification: 1.5 (d) E.O. 12958

  Declassify on: 1 June 2007 or x1-8 (exempt)

# Derivative Marking

- If derivatively classifying a document, the bottom right corner of the should have:

Derived by: Carroll Ward, DOC, OSY

Derived from: CIP Terrorism Report, 3/97

Declassify on: 3/1/07 (or x1-8)

# Derivative Marking cont...

- When derivatively classifying a document using multiple sources, either list each source or list “multiple sources” and maintain a list of the sources on file copy.
- Always use the most stringent declassification date.
- If source is marked OADR, list “Source marked OADR” and list date of document.

# Other Markings

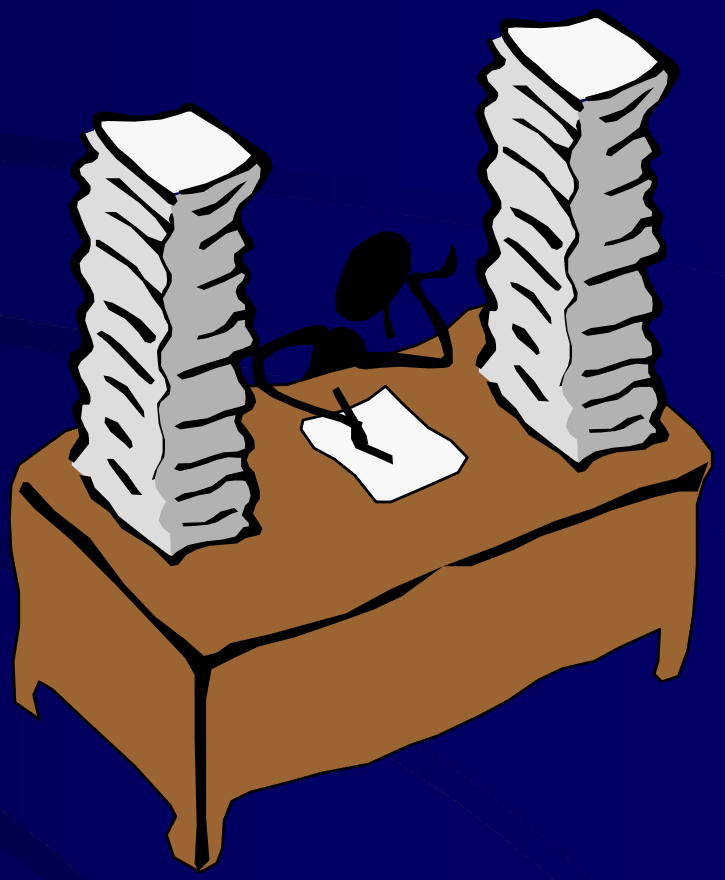
- US Only (old NOFORN): do not release to foreign nationals
- ORCON: Originator controlled
- Restricted Data/Formerly Restricted Data
- Handle via ____ Channels
- This document is unclassified when classified attachments are removed.

# 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). No document series at Commerce are exempt.

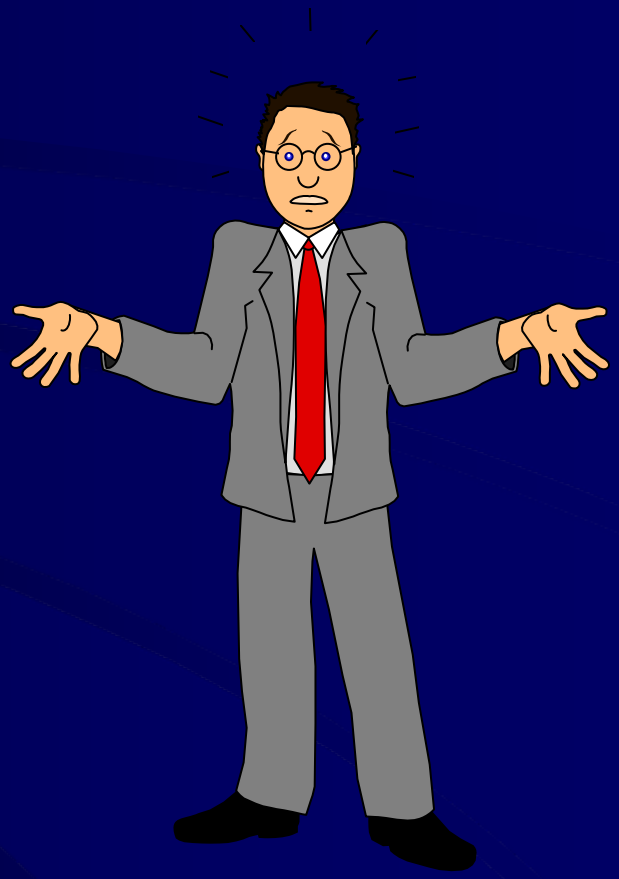
# Accountability of Classified

- Required for Secret and Top Secret
- Use of form CD481 (will be switched to a computer database)
- Identify who, what, when, where, how.
- Annual inventory is required!



# Accountability cont…

- Annual review must include:
  - review of classified holdings
  - determination of what classified is still needed
  - proper disposal of unneeded documents



# Storage of Material

- Sensitive, 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

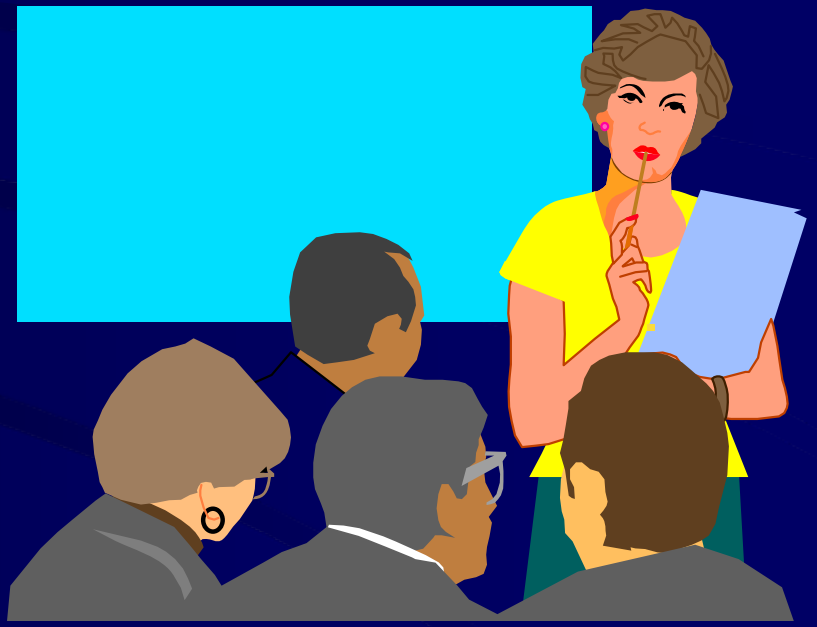
- Security container must contain an accurate SF-700.
- Combinations are classified at the level of information in the safe.
- Should always be memorized; never write them down.
- Don’t share with anyone who does not need to know it.

# Combinations cont...

- Change your security container combination when:
  - The 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



# Transmission of Classified Information: Telephone/Fax

- Always use a STU III phone or fax
- Standard and cell phones are not secure
- Is there a secure phone in your office? If not, where is the nearest one?

# Transmission of Classified Information: 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

- Inner wrapping: full address.
- Return address
- Classification markings top/bottom and front/back
- Information and receipt placed inside

# Transmission of Classified cont...

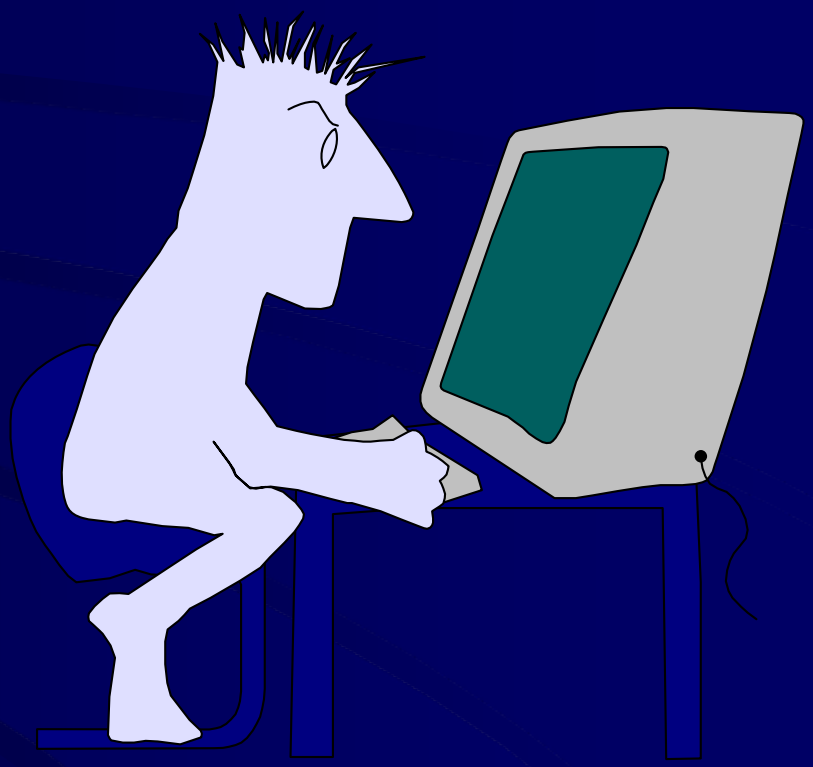
- Outer Wrapping:
  - Full address of receiver
  - Full return address
  - NO CLASSIFICATION MARKINGS
  - Recommend that you put “If undeliverable, return to sender”

# Transmission of Classified cont...

- To send Top Secret: call your security officer.
- Secret and Confidential
  - Hand-carry
  - Approved courier
  - US Postal Service
- 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 representative
- Your computer has a removable hard drive
- Is in a stand-alone configuration (no modem/network unless accredited)



# Reproduction of Classified Information

- Various ways to reproduce classified information:
- Paper (photocopier)
- Electronically
- Other means (video and/or cassettes)
- Use approved equipment for that purpose
- Account for your copies!

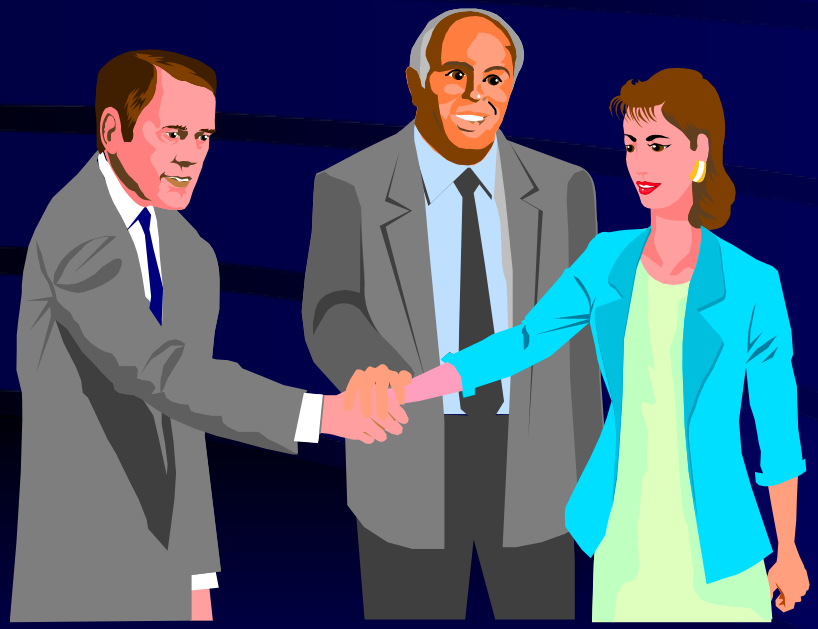
# Reproduction of Classified cont...

- Approved photocopiers:
  - 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
- Contact your security officer if your copier jams while working with classified

# Destruction of Classified and Sensitive Information

- 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, 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

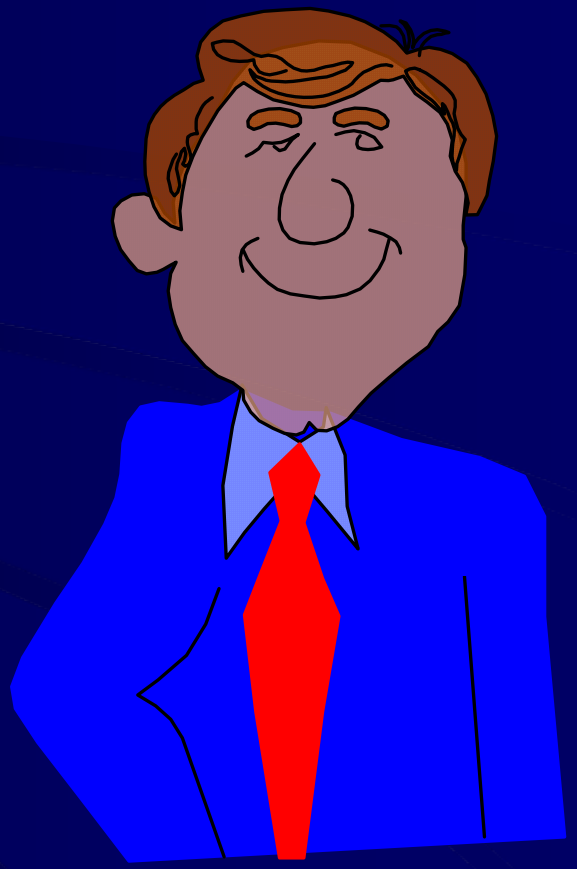
- All employees must report contact with a foreign national who:
  - Requests classified information
  - Wants more information than they need to know
  - Acts suspiciously
  - Report incidents to your security officer immediately.

# End of Day Checks

- All security containers
  windows/doors
  desk tops for classified
- Complete the SF701 “Activity Security Checklist.” The office manager is responsible for implementing the SF 701.

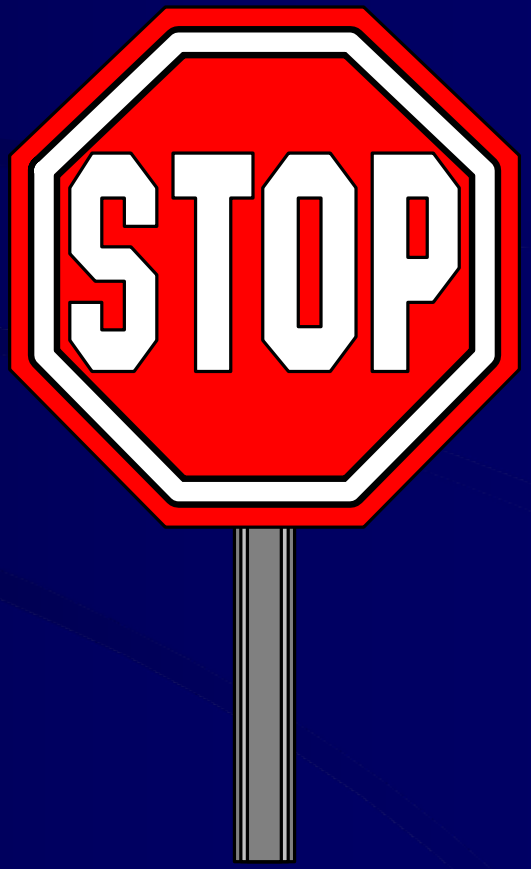
# Your Security Officer

- Your security officer is there to help you!
- Report to your security officers:
  - Security violations
  - Loss or compromise of classified information
  - Security incidents or problems



# When You Depart Commerce

- If you are leaving the Department, you must:
  - Turn over all classified material to your classified control point
  - Be debriefed by your Security Officer
  - Turn in all keys, ID, and access cards



# Finally….

- Who is responsible for security at the Department of Commerce?

- YOU ARE! Have a secure day! Remember, SECURITY MATTERS!

# DEPARTMENT OF COMMERCE
# OFFICE OF SECURITY
# EASTERN REGION

- Carroll Ward,
  Eastern Regional Security Officer
  (757) 441-3431

- Pam Ruhlen
  Eastern Regional Asst. Security Officer
  (757) 441-3415/3620

- Fax (757) 441-3422