# Department of Commerce
# Office of Security

## Initial Information Security Briefing

# Security Clearance

- 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 when you leave your position.

# Requirements for holding a security clearance

- Attend a briefing designed to teach you proper procedures for handling and protecting classified information. Refresher briefing every year.
- Sign a Non-Disclosure Agreement (SF-312).

# SF-312 Non-Disclosure Agreement Is

- A legally binding agreement between US Government and you. It is a life long agreement.
- An understanding of damage that could occur from unauthorized disclosure.
- An agreement to a pre-publication review
- An understanding that Classified information is US GOVERNMENT PROPERTY

# SF-312 and Penalties

- Should you improperly disclose classified:
- Under E.O. 12958, Performance Plan:
  - Performance Appraisal/Awards affected
  - Reprimand/Suspension (Without Pay)
- Loss of monetary gains made from improper disclosure
- Loss of security clearance
- Termination of employment
- Criminal prosecution (prison/fines)

# What is National Security Information

- Official information which relates to the national defense or foreign relations of the United States, which has been deemed requiring protection from unauthorized disclosure.

# National Security Information

- There are three levels of classification used 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”

deGaulle

# The Threat cont....

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

# Classification of Information

- How does information become classified?
- Original Classification:  An 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

# National Security Information cont...

- Foreign relations or activities of the U.S.
- Scientific, technological, or economic matters relating to national security
- Programs for safeguarding nuclear materials or facilities
- Vulnerabilities or capabilities of systems, installations, projects, or plans

# Reasons to NOT classify information

- To conceal violation of law, inefficiency, or administrative error
- To prevent embarrassment to a person, organization, or agency
- 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). No document series at Commerce are exempt.

# Marking Documents

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

# Marking cont....

- The bottom of the cover or title page 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 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

# Derivative Marking

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

Derived by: Joe Burns, DOC, OSY

Derived from: CIA Terrorism Report, 3/01

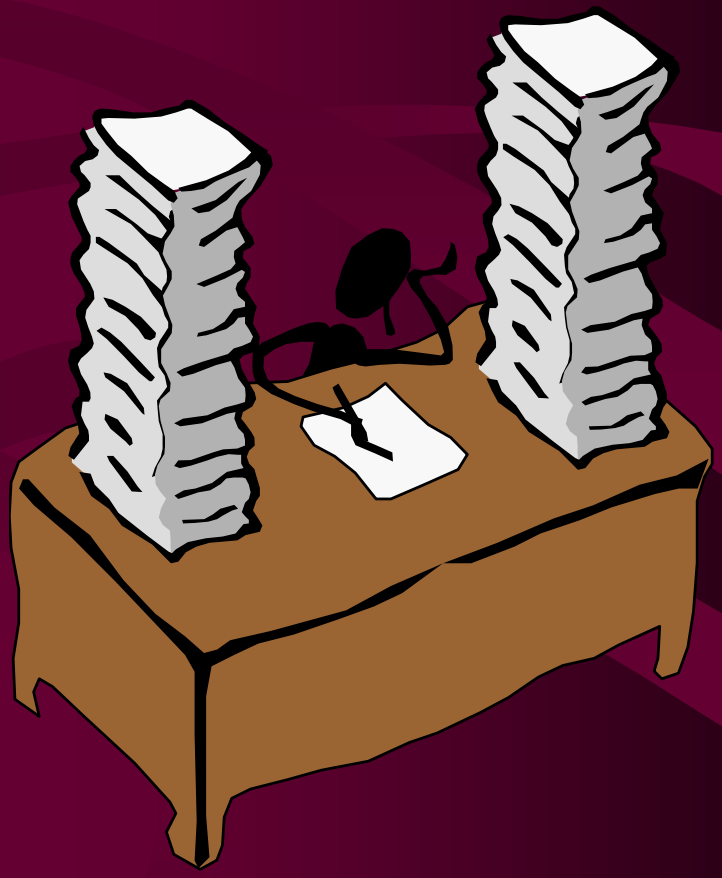
Declassify on: 3/1/11 (or x1-8)

# 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.

# Accountability of Classified

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



# 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

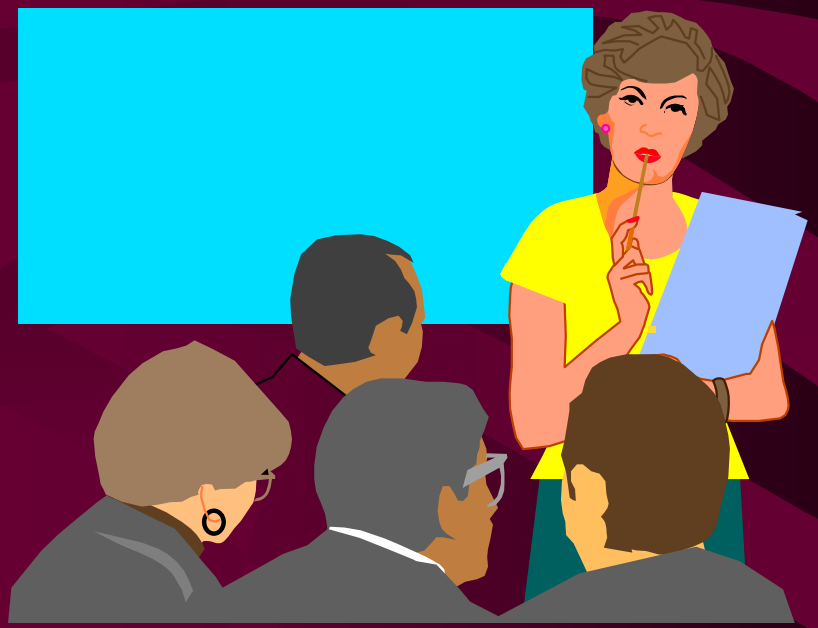
- Security container combinations are classified at the level of information in the safe.
- Should always be memorized; never write them down.
- Don’t share with anyone who does not need to know it.

# Combinations cont....

- Change your 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



# LEAKS

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

# Transmission: 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: 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 cont....

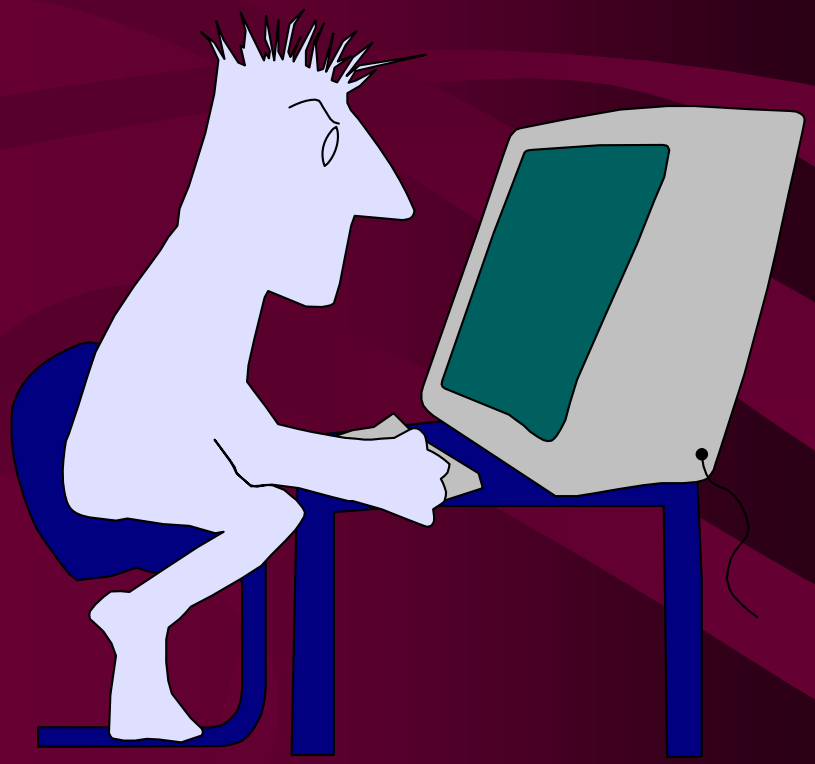
- Outer Wrapping:
  - Full address of receiver
  - Full return address
  - NO CLASSIFICATION MARKINGS
  - Recommend that you put “If undeliverable, return to sender”

# Transmission cont....

- To send Top Secret: call the Office of Security.
- 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 an Office of Security Representative
- Your computer has a removable hard drive
- Is in a stand-alone configuration (no modem/network unless accredited)



# Reproduction

- 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!

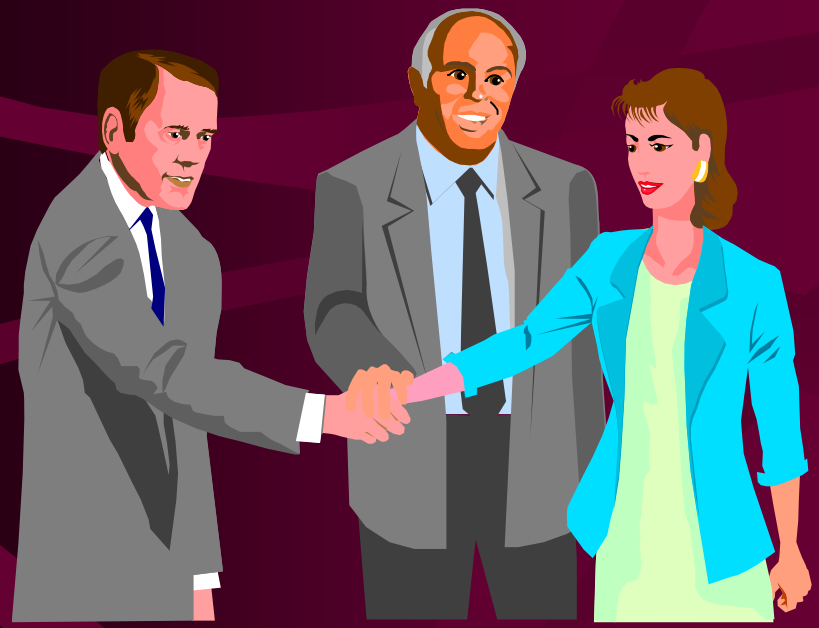
# Reproduction cont....

- 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 the Office of Security if your copier jams while working with classified

# DESTRUCTION

- 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



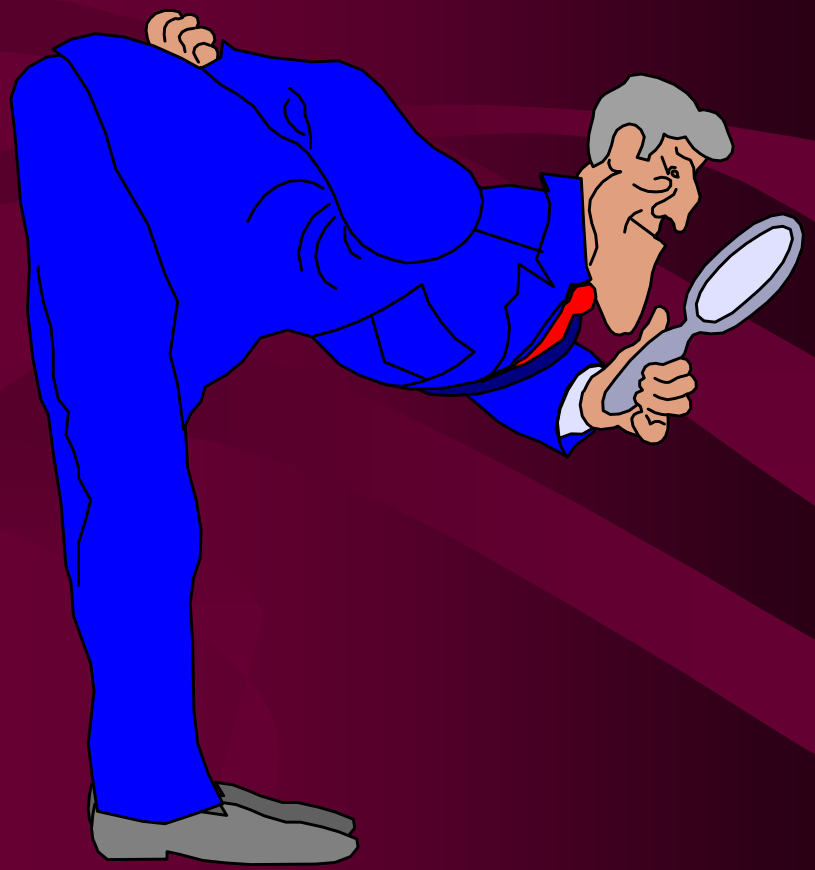
- Contact the Office of Security for a briefing before you go.
- Do not bring classified
- Limit sensitive information
- Notify U.S. Embassy of your visit

# 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.

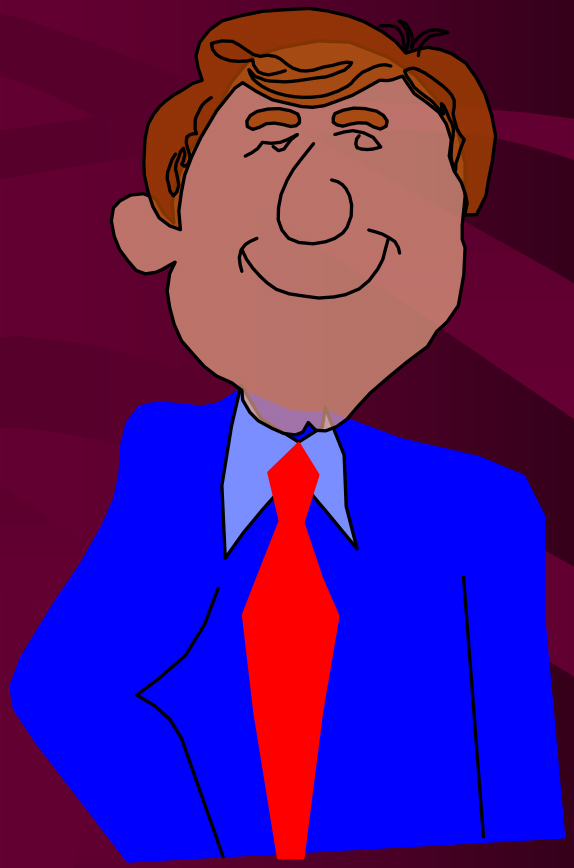
# End of Day Security Checks

- 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

- The Office of Security is there to help you!
- Report to an Office of Security Rep:
  - 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 all classified material over to your classified control point
  - Contact your Security Officer for a debriefing
  - Turn in your ID, keys, and access cards

# Finally….

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

- YOU ARE!  Have a secure day!