Introduction to Identifying Intelligence Community Classifications and Control Markings

OVERVIEW

- Executive Order

- Classification Management

- Types of Classification

- Sensitive Compartmented Information (SCI)

- Identifying classification markings

- What is an intelligence compromise

- How to report a compromise

Executive Order 12958

- Executive Order 12958 as amended, prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism.

Classification Management

▪Classification Management is exercising good judgment in the management of information requiring protection in the interest of national security.

Classification Markings

- TOP SECRET- The level applied to information whose unauthorized disclosure could cause exceptionally grave damage to national security.

- SECRET- Information whose unauthorized disclosure could reasonably cause serious damage to national security.

- CONFIDENTIAL- Information whose unauthorized disclosure could cause damage to national security.

- UNCLASSIFIED- Information that is not classified under the EO 12958, as amended.

Categories of Classification

G-2

- US Classifications for collateral
  - Spelled out in full, in uppercase
  - Portion markings are the first letters in each word capitalized in parentheses
  - Four classifications   Portion Markings
    - TOP SECRET   (TS)
    - SECRET   (S)
    - CONFIDENTIAL   (C)
    - UNCLASSIFIED   (U)

Collateral Information

- Information identified as national security information under the provisions of EO 12958 but which is not subject to enhanced security protection required for SAPs or other compartmented information.

Sensitive Compartmented Information (SCI)

▪Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence (DCI).

Categories of Classification G-2

SCI Control Systems and Code Words

- Three SCI systems in published Register:

-COMINT (SI)

-GAMMA (-G) sub-control system of COMINT

-TALENT KEYHOLE (TK)

-HUMINT (HCS)

Marking Requirements

- Portion markings

- Interior pages at the highest level of document

- First page at the highest level of document

- Title page (if there is one)
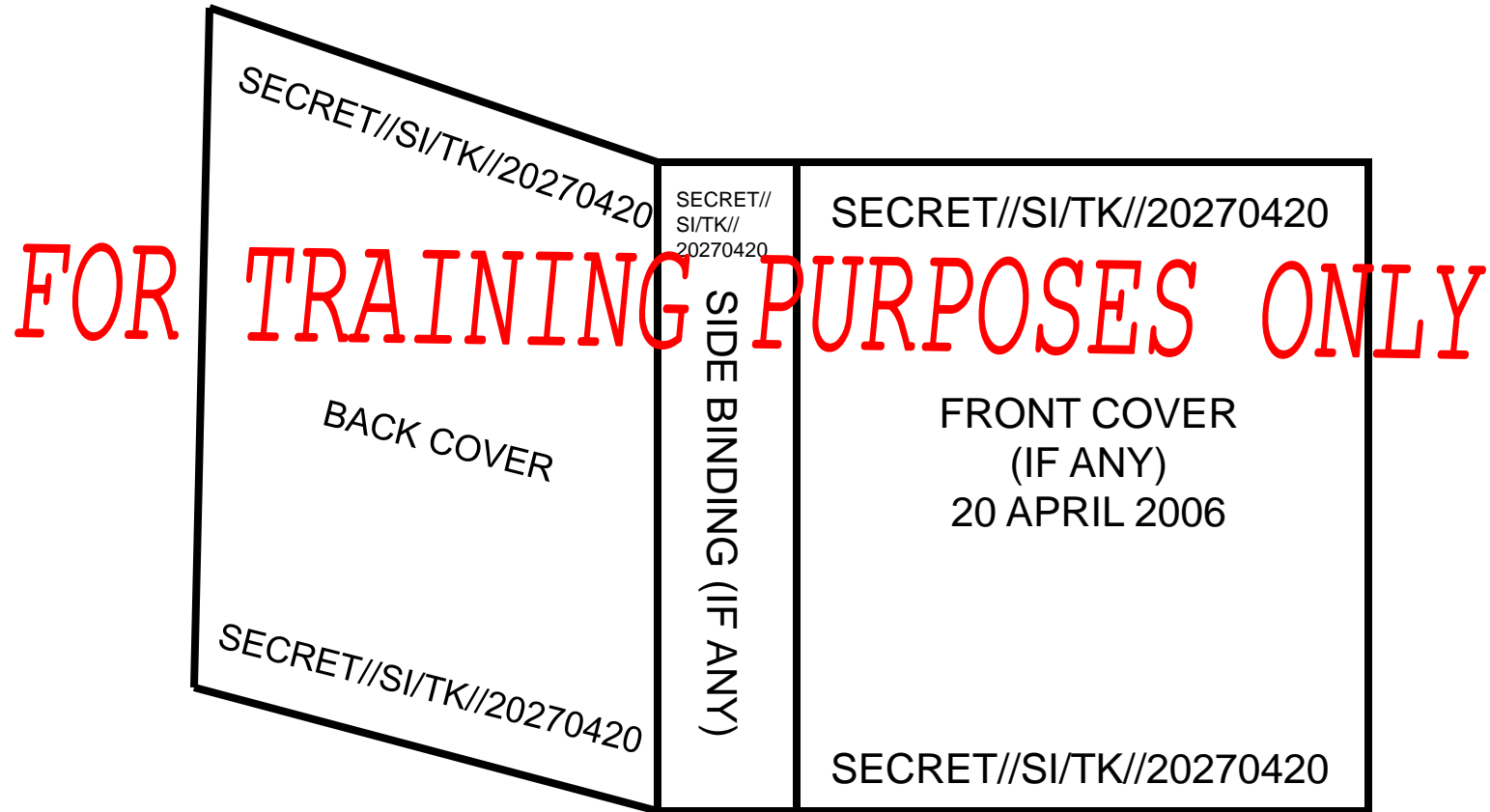
- Front and back covers (if there are covers)

Sample Requirements

SECRET//SI/TK//20270420

BACK COVER

SECRET//SI/TK//20270420

SECRET//SI/TK//20270420

SIDE BINDING (IF ANY)

SECRET//SI/TK//20270420

FRONT COVER
(IF ANY)
20 APRIL 2006

SECRET//SI/TK//20270420

FOR TRAINING PURPOSES ONLY

Sample Requirements

Portion Markings

(TS) The following information would be classified TOP SECRET.

(S//SI/TK) The following information would be classified SECRET and contain SCI information.

(U) Mark unclassified documents when transmitting via classified systems and when there are other control markings (e.g. FOUO).

Intelligence Compromise

Examples of how classified material can be compromised.

- Classified information in the media

- Classified documents left in an unsecured area

- Classified discussions in an unauthorized area

- Confirming or denying classified information to an uncleared source

- Transportation of classified material by other than an authorized courier

- Higher classified material being transmitted on a lower classified system

Intelligence Compromise

What to do if there is a compromise.

1. Isolate the information and exposure.

2. Contact the appropriate security official.

    1. GENSER compromise contact G-1 Security Branch at 477-8420/8995.

    2. SCI compromise contact G-2 Special Security Official (SSO) at 477-8451/8453.

    3. SAPs compromise contact Louis Johnson at 477-8915.

    4. After hours contact the G-3 Command Operations Center at 477-0077.

Intelligence Compromise

(Continued)

3. The security official will take the necessary steps to further notify the proper individuals.

4. If there are questions about a classification call a security official.

Do not ignore a compromise. You never know what information, products or lives may be at risk.