CHAPTER 2

Classified Information

When confronted with documents or other material containing classified information, all parties to a case must understand what classified information is, as well as duties and obligations with respect to creating, handling, storing, communicating, disseminating, and transmitting classified information. This chapter introduces classified information and explains the rules and procedures that are in place to protect classified information. Appendix 2-A is a list of references relating to classified information.

Practice Pointer: As a judge advocate involved in a classified information case, you need to know how to handle classified information. Thus, it is your duty to familiarize yourself with the references prior to handling classified information and consult with the experts for any questions you have.

A. What is classified information? Definitions of "classified information" vary. However, they all discuss information that (1) an authorized official of the executive branch has determined falls within listed categories, (2) is within the custody or control of the U. S. Government, and (3) reasonably can be expected to cause damage to the national security or foreign relations of the United States if disclosed to unauthorized recipients.

Executive Order (E.O.) 12958 defines classified information as "**information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form**." §6.1(h). Executive Order 12958 defines information as "any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government." Id., at § 6.1(s).

Secretary of the Navy Manual (SECNAV-M) - 5510.36 defines classified information as "[i]nformation that has been determined to require protection against unauthorized disclosure in the interest of national security and is classified for such purpose by appropriate classifying authority per the provisions of E.O. 12958, as Amended, or any predecessor Order." [1]

As used in the Classified Information Nondisclosure Agreement Standard Form 312 (Rev. 1-00),[2] classified information is "marked or unmarked classified information, including oral

[1] E.O. 12958, as amended, signed by President Clinton on April 20, 1995 and further amended by E.O. 13292, signed by President George W. Bush on March 25, 2003.

communications, that is classified under the standards of E.O. 12958, or under any other executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in …E.O. 12958, or under any other executive order or statute that requires protection for such information in the interest of national security."

Many statutes include "Restricted Data" within their definitions of classified information as a shorthand reference to information protected for interests of national security. However, Restricted Data is distinct from classified information because it is defined by the Atomic Energy Act of 1954 (42 USC §§ 2011 et seq.), is protected from unauthorized disclosure whether or not it meets the standards for classification set forth in E.O. 12958, and is subject to a regulatory regime completely separate from that governing information classified pursuant to E.O. 12958. Restricted Data is defined as "all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to section 2162 of this title." 42 USC § 2014(y). Statutes that include Restricted Data as classified information include:

> The National Security Act of 1947 ("any information that has been determined pursuant to E.O. 12356 of April 2, 1982, or successor orders, or the Atomic Energy Act of 1954 (42 U.S.C. §§ 2011 et seq.), to require protection against unauthorized disclosure and that is so designated"), at 50 U.S.C. § 438(b)(2); and
>
> The Classified Information Procedures Act (CIPA) ("any information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security, and any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954 (42 U.S.C. § 2014(y))"), at 18 U.S.C. App. III, § 1(a).

Importantly, the Military Rule of Evidence (M.R.E.) 505 definition of classified information tracks that used for CIPA: "any information or material that has been determined by the United States Government pursuant to an executive order, statute, or regulations, to require protection against unauthorized disclosure for reasons of national security, and any restricted data, as defined in 42 U.S.C. § 2014(y)." MRE 505(b)(1). Therefore, restrictive data is protected during courts-martial using MRE 505 procedures in the same way as information classified under E.O. 12958.

Practice Pointer: Trial counsel prosecuting a case involving Restricted Data will need a court security officer who understands and has experience with the requirements for safeguarding Restricted Data.

[2] All government employees, military and civilian, are required to execute the SF 312 prior to obtaining access to classified information. Civilian defense counsel that receive access to classified information through the procedures described in Chapter 6 must also sign an SF 312 prior to receiving any classified material.

B. <u>Substance of Classified Information</u>. For information to be classified under E.O. 12958,[3] it must be owned by, produced by or for, or be under the control of the United States Government, and fall within one or more of the following categories of information:

1. Military plans, weapons systems, or operations;

2. Foreign government information;

3. Intelligence activities (including special activities), intelligence sources or methods, or cryptology;

4. Foreign relations or foreign activities of the United States, including confidential sources;

5. Scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism;

6. United States Government programs for safeguarding nuclear materials or facilities;

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

8. Weapons of Mass Destruction.

Assuming the information meets the above criteria, it can be classified only if an Original Classification Authority (OCA) determines that the unauthorized disclosure of the information reasonably could be expected to cause damage to the national security and is able to identify or describe that possible damage. *See*, E.O. 12958, § 1.1. An OCA is an official authorized in writing by the President, or by certain authorized officials, to classify information in the first instance.

The only OCAs are the President and, in the performance of executive duties, the Vice President; agency heads and officials so designated by the President in the Federal Register; and United States Government officials delegated OCA authority. E.O. 12958, § 1.3(a). OCAs within DON are identified at www.navysecurity.navy.mil/documents/information/don-oca.htm, as well as in SECNAV M-5510.36, Exhibit 4A at pages 4A-1 to 4A-7.

Once an OCA determines the information falls within one or more of the E.O. 12598 categories of information, the OCA must assign a classification level to the information. There are only three classification levels: TOP SECRET, SECRET, and CONFIDENTIAL. The common designation FOR OFFICIAL USE ONLY (FOUO) is NOT a classification level. FOUO information is unclassified. The OCA assigns a classification level to information based on the

[3] E.O. 12958 § 1.4 (a) – (h)

OCA's subjective evaluation of the *severity of the damage* to the national security that the OCA reasonably expects to occur from the unauthorized disclosure of the information:

Top Secret	-	Exceptionally Grave Damage
Secret	-	Serious Damage
Confidential	-	Damage

See, E.O. 12958, § 1.2(a).

Practice Pointer: Confidential Attorney-Client Information. Attorney-client or attorney work-product should not be marked "CONFIDENTIAL" unless it is, in fact, classified information which the unauthorized disclosure of would cause damage to national security. If it is not classified, attorneys should refrain from using the "Confidential" label, and use instead, labels like "PRIVILEGED," "ATTORNEY CLIENT PRIVATE INFORMATION", or "ATTORNEY WORK PRODUCT."

Non-OCAs who create information that they believe should be classified must protect the information as classified and forward it to an appropriate OCA or agency head for a formal classification determination. E.O. 12958 provides that when "an employee, government contractor, licensee, certificate holder, or grantee of an agency who does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with [E.O. 12958] and its implementing directives." That person must send the information promptly to the agency that has appropriate subject matter interest and classification authority. That agency must decide within 30 days whether to classify this information. If it is unclear which agency has the classification responsibility for the information in question, the information must be sent to the Director of the Information Security Oversight Office. *See* E.O. 12958, § 1.3(e) and SECNAV M-5510.36, paragraph 4-14. This situation rarely occurs. Instead, most people apply pre-existing classification guidance prepared by an OCA.

C. Derivative Classification. Generally, people working with classified information are not creating new classified information, i.e. they are not acting as an OCA. Instead they are "incorporating, paraphrasing, restating or generating in a new form information that is already classified." E.O. 12958, § 6.1(n). This process is called "**derivative classification**." Anyone who comes in contact with and uses classified information can be a derivative classifier. Applying derivative classification authority requires that the new document be marked consistent with the source material, including the declassification data. *Id.* In addition, using an OCA's security classification guide to properly classify information is also a method of derivative classification. *Id.* However, merely reproducing existing classified information, for example by photocopying or scanning, is not derivative classification because the classified information is not incorporated into a new form. *Id.*

E.O. 12958, Section 6.1 further provides:

a. ‘‘Classification guide’’ means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

b. ‘‘Source document’’ means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

c. ‘‘Multiple sources’’ means two or more source documents, classification guides, or a combination of both.

Persons who apply a derivative classification are required to observe and respect the original classification determinations made by OCAs. *See* E.O. 12958, at §2.1(b)(1); and SECNAV M-5510.36, at 4-9.2. Normally, this is done by reference to a source document or classification guide. Such guides are merely the recording of original classification decisions whose purpose is to "facilitate the proper and uniform derivative classification of information." *See* E.O. 12958, at § 2.2(a) and SECNAV M-5510.36, at 5-1.1 However, the absence of a classification guide does not negate an OCA's determination to classify information.

Practice Pointer: YOU are a derivative classifier. Unless you work for an OCA and have received the appropriate delegation of authority in accordance with E.O. 12958, § 1.3, you will rarely, if ever, use original classification authority. While working on a case involving classified information, all your briefs, memos, emails, and notes that contain classified information related to the case will be derivatively classified. Make sure you carry over the classification markings, identify your source document(s) on your new documents, and the latest declassification date.

D. Classification Markings. Persons exercising either original classification authority or derivative classification authority are responsible for determining whether the information is classified and marking it accordingly. The marking guidelines apply to any type of document that contains classified information, including correspondence, emails, reports, briefing slides, regulations, instructions, and internal memorandums or notes. Once a document has been determined to contain classified information, E.O. 12958 and implementing regulations require the document to be marked to indicate the level of classified information in the document. Failure to mark or properly mark the document does not render the *information* unclassified. Proper markings put the handler on notice that the document contains classified information and must be protected accordingly. The handling of classified documents, even if improperly marked, carries with it the obligation to protect the information in accordance with the relevant regulations. A person who believes a document is improperly marked is obligated to treat it as

classified until obtaining an official determination otherwise, by using the classification challenge process described in E.O. 12958 §1.8 and SECNAV M-5510.36, paragraph 4-12.

1. Overall classification marking. A document's cover and back pages must be marked at the top and bottom with the highest level of classified information found anywhere in the document. The top and bottom of each page of the document must also be marked. There are two acceptable methods of marking the pages of a classified document. First, the pages can be marked at the top and bottom with the highest level of classification contained on that page. Each page of the document might then reflect a different classification, or even be marked as unclassified, based on the highest level of classification contained on that page. This method, although more labor-intensive, is the more discriminating approach and makes handling and use easier. The more common method of marking pages is to mark the top and bottom of each page with the highest level of classified information contained in the document, regardless of the highest level on that particular page. In this case, the marking becomes easier because of the ability to use the same header and footer throughout the document. It should be noted that the marking at the top and bottom of the page does not mean that everything on the page is classified at that level. In fact, if a page contains only unclassified information (based on proper portion marking as described below), yet is marked at the top and bottom of the page with SECRET because the second method of page marking is in use, that page may be separated from the rest of the document and be freely distributed. The distributor would simply mark through the classification marking at the top of the page. A common error when derivatively classifying documents is to take material from a paragraph portion-marked as unclassified , and then mark it as classified in the new document based on the overall classification of the source document as indicated by the markings on the cover and pages (when the second method is used).

2. Portion-marking. Absent an authorized exception, each portion (usually meaning a paragraph) is preceded with parentheses containing capitalized letters identifying the highest level of classified information contained in that paragraph. This portion-marking identifies that paragraph as containing classified information and is unrelated to the classification of information elsewhere in the document. The most commonly used portion-marking abbreviations are:

(U)	-	Unclassified
(FOUO)	-	For Official Use Only
(C)	-	CONFIDENTIAL
(S)	-	SECRET
(TS)	-	TOP SECRET

Other commonly seen markings that follow the classification level marking are dissemination controls and handling caveats. While dissemination controls and handling caveats are not classification markings, they advise the holders of a document of additional protective measures such as restrictions on reproduction, dissemination, or extraction. Such markings are further defined in Chapter 6 of SECNAV M-5510.36 and include:

NOFORN - NOT RELEASABLE TO FOREIGN NATIONALS

ORCON - DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR

REL TO - AUTHORIZED FOR RELEASE TO

SPECAT - SPECIAL CATEGORY

PROPIN - CAUTION PROPRIETARY INFORMATION INVOLVED

SAMI - SOURCES AND METHODS INFORMATION

3. Additional Required Markings. In addition to marking the overall level of classification and applying portion markings, the drafter must annotate the basis for classification and the declassification date, usually near the bottom of the page. OCAs must also indicate who classified the information. Examples:

If using original classification authority:

Classified by: LCDR I.M. Incredible (N3)
Reason: 1.4(c)
Declassify on: 31 Oct 2009

If using derivative classification authority:

Derived from: OPNAVINST S5513.5B, enclosure (17)
Declassify on: 31 Oct 2009

 **Practice Pointer:** As a derivative classifier, you would follow the second example. More specific guidance can be found in Chapter Six of SECNAV M-5510.36.

Additionally, mark your drafts and notes as "WORKING PAPERS" in addition to carrying over the classification markings from your source.

E. <u>Classification Prohibitions</u>. E.O. 12958 § 1.7 prohibits classifying information in order to:

a. conceal violations of law, inefficiency, or administrative error;
b. prevent embarrassment to a person, organization, or agency;
c. restrain competition; or
d. prevent or delay the release of information that does not require protection in the interests of national security.

F. Access to Classified Information. In order to receive access to classified information, one must have a valid and current security clearance, have signed a Classified Information Nondisclosure Agreement (SF 312), and have a "need-to-know" the information. E.O. 12958 § 4.1(a).[4]

In the pre-referral discovery context, the convening authority will determine if the defense counsel has a "need-to-know" before permitting disclosure of classified information to properly-cleared defense counsel. "Need-to-know" would normally require that the requested discovery be relevant to the defense or government case. Under the Third-Agency Rule,[5] however, the convening authority may only share with military or civilian defense counsel classified information that belongs to the Department of Defense (DoD). An agency cannot disclose information originally classified by another agency without the permission of the other agency. Thus, if the information is owned by a non-DoD agency, the convening authority must request permission to disclose that information to military or civilian defense counsel.[6] Although a member of the Department of Defense, because of unique considerations relating to the National Security Agency (NSA), the convening authority must seek permission from NSA to disclose NSA-owned classified information to defense counsel, military or civilian.

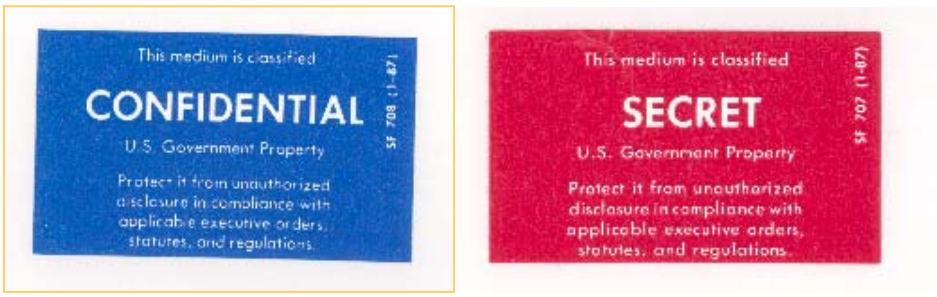
Practice Pointer: BEWARE: All SIGINT information is owned by NSA, even if it originates with a Navy command or Navy-run program! You MUST receive permission from NSA before sharing such information with the defense team.

G. Classified Media. Just as classified documents must be marked with the appropriate classification markings, so too must classified media such as CD-ROMs, diskettes, thumbdrives and zip disks. Media are marked by using labels (SF 706 - 711)

[4] "Need-to-know" is a determination by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized government function. E.O. 12958 § 6.1(z).

[5] Third-Agency Rule: "classified information originating in one agency shall not be disseminated outside any other agency to which it has been made available without the consent of the originating agency…. For purposes of this section, the Department of Defense shall be considered one agency." E.O. 12958 § 4.1(i).

[6] Disclosure to a military defense counsel is considered to be disclosure outside DoD because, although wearing a uniform and technically part of DoD, military defense counsel is actually acting in a personal representational capacity AGAINST the government. He is acting not in the interests of DoD or the government, but for the interest of his client.



H. <u>Storage, handling, transmission, reproduction, and destruction</u>. There are many specific rules designed to protect classified information and prevent its disclosure. In the Navy and Marine Corps, the primary reference for these matters is SECNAVINST 5510.36A, currently implemented via the SECNAV M - 5510.36. Any person handling classified information must become familiar with this reference. The command security manager or special security officer (SSO) is an excellent resource that all counsel, both trial and defense, should utilize.

1. Storage. When not under the personal control or observation of an appropriately cleared person, classified information shall be stored in a Government Service Administration (GSA)-approved security container, e.g., safe, vault, modular vault, or secure room. A secure room is an area constructed to specific standards described in exhibit 10A of SECNAV M-5510.36, Chapter 10. Storage of TOP SECRET information also requires at least one additional supplemental control, as detailed in SECNAV M-5510.36, paragraph 10-3.1.a(1). SECRET and CONFIDENTIAL information are not subject to such supplemental controls. Residential storage of classified information is not normally authorized. Approval authorities for residential storage are specified in SECNAV M-5510.36 at paragraph 10-10 and are generally high-ranking officers or civilians in the Department of the Navy.

Practice Pointer: Your office may not have its own safe so you may have to share classified storage with your colleagues, or even another command. To protect the privacy of your notes and to restrict need-to-know access, seal them in an envelope, sign across the seal, and label it clearly with your name, contact number, and the classification level of the contents. Then place the envelope in the GSA-approved safe.

2. Handling. Classified information can be easily and routinely used in the work place if is properly safeguarded. The protective measures put in place shall ensure that unauthorized personnel will not gain access to classified information. Classified information may be used and discussed in government spaces, but classified information should not be left unattended unless in a secure room or a sensitive compartmented information facility (SCIF). Guidelines discussed below are for handling material outside the above mentioned spaces. Particular handling guidelines are in place for Sensitive Compartmented Information (SCI). SCI material cannot be viewed or discussed unless in a SCIF, as discussed in DoD 5105.21-M-1

While working with classified information it must be kept in your personal control. When work material has served its purpose or at the end of the day, it must be destroyed or stored away in a GSA approved safe. Please keep in mind that locking it away in an office or desk drawer is not acceptable.

You can have a discussion regarding classified subject matter in several places, such as government conference rooms or office spaces. Use the common sense approach – make sure that you are away from uncleared personnel, all cell phones are off and those discussing the information are cleared to the appropriate level and have the "need to know." You should never discuss classified information over non-secure telephone lines.

3. Transmission. Procedures for transporting and transmitting material vary according to the classification level of the material concerned. Classified material may not be opened or read in any area where it can be seen by unauthorized personnel. Specific guidance is provided in SECNAV M-5510.36. Below are the basic guidelines for transmitting Top Secret, Secret and Confidential information between the U.S., its territories and Canada.

Unlike other categories of classified information, Top Secret material generally must be transported person-to-person and not through any mail system. This may be accomplished by direct contact between cleared U.S. Personnel, delivery by the Defense Courier Service or Department of State Diplomatic Courier Service. Transmission of Top Secret information can also occur via communications protected by a cryptographic system which has been authorized by NSA. Top Secret material may not be transmitted over SIPRNET, which is only cleared up to the Secret level. Top Secret material may also be discussed over appropriately cleared secure telephones or sent by secure fax.

Secret and Confidential material can be transmitted by any means approved for Top Secret material, along with the following additional means: U.S. Postal Service (USPS) registered mail; USPS and Canadian Registered mail with a mail receipt between governments. Also, Secret information may be sent via a GSA authorized Carriers, which include DHL and Federal Express. For a complete listing please go to www.navysecurity.navy.mil/info-trans.htm.

Classified material or information must be double wrapped and sealed with tape that can retain the impression of any postal stamp. The inner wrapping must be stamped with the classification of the highest level of material contained within. The outer wrapper must not contain any indication that the package contains classified information. A Record of Receipt (OPNAV 5511/10) must be included within the package. The use of roadside postal drop boxes is not authorized. Detailed instructions for mailing classified information can be found in Chapter 9 of SECNAV M-5510.36.

Information on the transmission of SCI may be found in DoD 5105.21-M-1.

4. Reproduction. Reproduction of classified material is limited to that necessary to carry out the mission of the organization. Reproduction of classified information may only be

done on specially-designated copiers and IT equipment, including printers. That equipment must meet the requirements set forth in SECNAV M-5510.36 in order to be authorized for copying classified information. Control measures are applied to copies of classified information in accordance with the classification marking on the original document.

5. Destruction. Classified information that is no longer needed for operational purposes must be destroyed. There are several methods authorized for the destruction of classified material. The most common are burning, shredding and mutilation.

If shredding the information, it must be done with a cross-cut shredder that reduces the material to no more than five square millimeters. Once the material has been properly shredded, the resulting material may simply be thrown away with the regular trash. (If using a shredder that was purchased prior to 1 January 2003 the bag containing the shred must be stirred or agitated prior to disposal)

Material that is awaiting destruction, whether in burn bags or some other method of collection, must be protected in accordance with the procedures for the highest level of classification in the container. If stored in an office that is not a secure room or SCIF, the burn bag or material must be locked in a GSA approved safe.

Two people are required to witness the destruction of Top Secret material and destruction must be documented using OPNAV 5511/12. The destruction of SCI material is covered in DoD 5105.21-M-1.

I. <u>Compartmented Information</u>. Classified information is often confused with compartmented information. They are not the same. While all compartmented information is classified, the overwhelming majority of classified information is not compartmented. In addition, compartmented information is NOT another level of classification "above TOP SECRET."[7] As stated earlier in the chapter, there are only three levels of classification: TOP SECRET, SECRET, and CONFIDENTIAL. Compartmented information is information within a formal system, which strictly controls the dissemination, handling, and storage of a specific class of classified information, thereby limiting access to individuals with a specific need-to-know. Compartmented information is often referred to as "codeword information." This paragraph will discuss the two principal categories of compartmented information: Special Access Programs and Sensitive Compartmented Information.

1. <u>Special Access Programs</u>. E.O. 12958, at § 6.1(kk) defines "Special Access Programs" (SAP) as "a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level." E.O. 12958, at § 4.3(a) limits the authority to establish SAPs to "the Secretaries of State, Defense and Energy, and the Director of Central Intelligence, or the principal deputy of each." It further cautions that these officials shall keep the number of

[7] In fact, it is possible to have compartmented information that is classified at the Secret level, i.e., “Secret/SI,” but is still subject to special handling procedures.

programs at an absolute minimum, and shall establish them only upon a specific finding that:

a. The vulnerability of, or threat to, specific information is exceptional; and

b. The normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure.

The Secretary of Defense (SECDEF) or Deputy SECDEF must authorize all DOD SAPs. Within the Navy, the Director, Special Programs Division (N89), receives and reviews requests to establish SAPs and the Under Secretary of the Navy must formally approve the establishment of each SAP in coordination with the Deputy SECDEF. SECNAV M-5510.36, at 1-4.7. See Appendix 2-A for a list of authorities and regulations relevant to SAPs

SAP information is typically identified with one or more classified codewords. A person obtains authorized access to the SAP information by successfully completing the personnel security processing unique to that particular SAP and signing a SAP Nondisclosure Agreement. Further, that person may not disclose SAP information to anyone else without verifying the other person has authorized access to the SAP and a specific "need-to-know" for the specific SAP information. SAP information need to be stored in areas that have security measures exceeding those required for TOP SECRET. Most non-intelligence SAPs in DOD pertain to weapons systems.

2. <u>Sensitive Compartmented Information (SCI)</u>. The Office of the Director of National Intelligence (ODNI), is responsible for all Controlled Access Programs within the National Foreign Intelligence Program.[8] Controlled Access Programs include Sensitive Compartmented Information (SCI) and other special access programs. Director of Central Intelligence Directive (DCID) 6/1 defines SCI as"classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled exclusively within formal access control systems established by the DCI." Examples of SCI control systems are SIGINT (SI) and Talent-Keyhole (TK), which pertain to signals intelligence and imagery intelligence, respectively. Only the DCI or Deputy DCI, may create, modify, or terminate a controlled access program.[9]

The Director, Defense Intelligence Agency (DIA), is responsible for administering security policies and procedures issued for the Department of Defense (DOD), with the exception of the National Security Agency (NSA) and the National Reconnaissance Office (NRO). The Director of Naval Intelligence (DNI), as the Department of the Navy

[8] The Director of Central Intelligence, commonly referred to as the DCI was replaced by the Office of Director of National Intelligence (ODNI) by the passage of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. § 401 note, 50 U.S.C. § 403). Any references to the DCI in Executive Order 12958 should now be read to mean the ODNI.

[9] To date, the ODNI is in the process of transitioning all DCIDs to Intelligence Community Directives (ICD). It is likely that DCID 6/1 will be rolled into an ODNI ICD in the near future. Until specifically rescinded, DCIDs remain in full force and effect.

(DON) Senior Official of the Intelligence Community (SOIC), is responsible for protecting intelligence and intelligence sources and methods from unauthorized disclosure and for administering SCI programs within the DON. DNI further delegated management oversight of DoN SCI programs to the Office of Naval Intelligence. *See* DOD Directive 8520.1, at 5.3.1 and 5.5.1 and SECNAV M-5510.36, at 1-4(5).[10] Within DOD and DON, the DCIDs are implemented by DoD 5105.21-M-1, DoD Sensitive Compartmented Information Administrative Security Manual, 3 Aug 98, and the Navy Department's Supplement to the M-1, March 1997.

> "Access to SCI shall be based on need-to-know, formal access approval, and indoctrination. As a general principle, SCI disseminated to persons meeting those criteria shall be provided at the lowest level of classification and compartmentation that will satisfy official requirements applicable to the recipients. Source and method data shall be provided only to the extent necessary to fulfill such requirements. Sanitization of material shall be accomplished to the extent possible to protect against damage to sources and methods through unauthorized disclosure, espionage, or other compromise." DCID 6/1.
>
> "The primary security principle in safeguarding SCI is to ensure that it is accessible only by those persons with appropriate clearance, access approval, clearly identified need-to-know, and an appropriate indoctrination. Even when approved for a specific access, the holder is expected to practice a need-to-know discipline in acquiring or disseminating information about the program(s) or project(s) involved. Intrinsic to this discipline is acquiring or disseminating only that information essential to effectively carrying out the assignment." DCID 6/1.

Documents containing SCI information are marked in accordance with the *Intelligence Community Classification and Control Markings Implementation Manual.* The classification line that reflects the overall classification of the document or of the individual page is placed at the top and bottom of each page, to include the cover and back page. There are seven categories of classification and control markings. They are:

1. U.S. Classification;
2. Non-U.S. Classification;
3. Joint Classification Marking Usage;
4. SCI Control Systems and Sub-categories;
5. Special Access Program Usage;

[10] DoD Directive 8520.1 is currently under review and slated for cancellation. It is expected that the substance will be contained in a new Instruction,, not yet published.

6. Foreign Government Information;

7. Dissemination Controls;

8. Non-Intelligence Community Markings; and

9. Declassification Date Marking.

Examples of SCI marking variations that would appear at the top and bottom of an SCI document are:

SECRET//NOFORN,PROPIN//20051015

TOP SECRET//TALENT KEYHOLE//RISK SENSITIVE//25X1

TOP SECRET//TK//RSEN//25X1

TOP SECRET//COMINT//REL TO USA and GBR//25X1

Every portion (including title) shall be portion marked on all classified documents. Portion markings are always placed at the beginning of the portions and enclosed in parentheses. Portion markings utilize the same separators as are used for the classification markings at the top and bottom of the page. In classified documents or in unclassified documents that bear any control markings, the unclassified portions that do not require any control markings shall always be marked with (U). Any unmarked portions must be assumed to be classified at the overall classification level marked at the top and bottom of page.

As stated above, special access programs are established only upon a finding that the security requirements normally applied to information classified at the same level are inadequate due to the exceptional threat to or vulnerability of the information. Therefore, personnel, information, and physical security requirements governing compartmented information are generally more stringent than those for TOP SECRET, SECRET, or CONFIDENTIAL information.

For example, SCI may be discussed and stored only in SCIFs. The structural and security requirements for SCIFs are set forth in DCID 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF). The Nondisclosure Agreement for access to SCI is different than the one for non-compartmented information. There are some SCI compartments that require records to be maintained identifying everyone authorized access to that compartment. There are SCI programs that may require further compartmentation (subcompartments) when the program office desires to further restrict need-to-know of a discrete body of information contained within the program. In such cases, a person must not only have authorized access to the compartment, but also must have authorized access to the specific subcompartment.

Practice Pointer: Trial counsel should ensure that the investigation or court-martial security officer assigned to provide security guidance and control in such cases is well-versed in the specific requirements of the SAPs or SCI programs at issue.

J. Government Information other than Classified Information. When government information is not classified but still needs protection from disclosure, MRE 506 applies. Under 506(b), government information includes "official communications and documents and other information within the custody or control of the Federal Government." Its disclosure has to be "detrimental to the public interest" for this rule to apply and does not include classified information or the identities of informants, which are protected under MRE 505 and 507, respectively.

The types of information that fall under MRE 506 is a non-exclusive list that must meet the "detrimental to public interest" test. MRE 506 would not apply to information whose disclosure is mandated by Congress, such as documents under the Freedom of Information Act (FOIA). But it would conceivably apply to information that is exempted from disclosure under FOIA, such as names and social security numbers.

This page intentionally left blank

APPENDIX 2-A

Classified Information References

1. Executive Order No. 12958, "Classified National Security Information," Apr 17, 1995, as amended by Executive Order 13292, Mar 25, 2003, 68 Fed. Reg. 15315.

2. Executive Order No. 12968, "Access to Classified Information," Aug 2, 1995, 60 Fed. Reg. 40425.

3. Executive Order No. 12951, "Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems," Feb 22, 1995, 60 Fed. Reg. 10789.

4. Order of President of the United States, “National Security Information,” dated Oct 13, 1995, 60 Fed. Reg. 53845, designating original classification authorities, reprinted at 50 U.S.C. § 435 note.

5. Information Security Oversight Office Directive No. 1, "Classified National Security Information," as amended, Sep 22, 2003, at 32 C.F.R. 2001 & 2004.

6. DOD Directive 5200.1, DOD Information Security Program, Dec 13, 1996, reprinted at 32 C.F.R. 159.

7. DOD 5200.1-R, DOD Information Security Program Regulation, Jan 14, 1997, reprinted at 32 C.F.R. 159a.

8. DOD 5200.2, DOD Personnel Security Program, Apr 9, 1999, reprinted at 32 C.F.R. 156.

9. DOD 5200.2-R, DOD Personnel Security Program Regulation, through change 3, Feb 23, 1996, reprinted at 32 C.F.R. 154.

10. SECNAVINST 5510.36 [series], DoN Information Security Program (ISP).

11. SECNAVINST 5510.30 [series], DoN Personnel Security Program (PSP).

12. http://www.navysecurity.navy.mil, contains updates on the DoN Information and Personnel Security Programs.

13. Director of Central Intelligence Directive (DCID) 6/1, "Security Policy for Sensitive compartmented Information and Security Policy Manual," Mar 1, 1995.

14. Director of Central Intelligence Directive (DCID) 6/9, "Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF)," Nov 18, 2002.

15. Director of Central Intelligence Directive (DCID) 6/4, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI), Jul 2, 1998.

16. Department of Defense Manual 5105.21-M-1, DOD Sensitive Compartmented Information Administrative Security Manual, Mar, 1995 (NOTAL).

17. Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. § 401 note.