QUICK GUIDE TO CLASSIFIED EVIDENCE PROCEDURES

I. ESSENTIAL REFERENCES[1]

A. U.S. Dep't of the Navy, Office of the Judge Advocate General, National Security and Intelligence Law Division (Code 17), *The Judge Advocate's Handbook for Litigating National Security Cases: Prosecuting, Defending and Adjudicating National Security Cases* (2002)

B. Executive Order (EO) No. 12598, "Classified National Security Information," April 17, 1995, 60 Fed. Reg. 19825, reprinted at 50 U.S.C. § 435 note.

C. Order of the President of the United States, dated Oct. 13, 1995, 60 Fed. Reg. 53485, designating original classification authorities, reprinted at 50 U.S.C. § 435 note.

D. DoD Directive 5200.1, DoD Information Security Program, 13 Dec 96.

E. DoD 5200.1-R, DoD Information Security Program Regulation, 14 Jan 97.

F. U.S. Dep't of the Army, Reg. 380-67, Personnel Security Program, 9 Sep 88.

G. U.S. Dep't of the Army, Reg. 27-10, Military Justice, 6 Sep 02.

H. Classified Information Procedures Act (CIPA), 18 U.S.C. appx. III, §§ 1-16 and interpretative caselaw.

I. Military Rule of Evidence (MRE) 505, Classified Information.

II. KEY DEFINITIONS

A. Classified National Security Information.

1. "Classified national security information" (hereafter "classified information") means 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." From EO 12958.

[1] Note: Some of these references are provided in electronic format in the "Classified Evidence" folder of your course CD-ROM.

MAJ Chris Behan
2004 Military Justice Manager's Course
August 2004

2. Types of Classified Information. Information that concerns:

a) Military plans, weapons systems, or operations;

b) Foreign government information;

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

d) Foreign relations or foreign activities of the United States, including confidential sources;

e) Scientific, technological, or economic matters relating to the national security;

f) United States Government programs for safeguarding nuclear materials or facilities; or

g) Vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

B. Original Classification Authority (OCA). "An individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance." For all practical purposes, the OCA owns the information and must ultimately approve its release. *See* EO 12958, para. 4.2(b).

C. Levels of Classification.

1. Top Secret. Information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

2. Secret. Information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

3. Confidential. Information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

D. Graymail. An attempt, whether for legitimate reasons or otherwise, by a defendant to derail a criminal trial by threatening to disclose classified evidence. Two competing values:

1. Accused's right to a fair trial.

2. The Government's interest in preserving national security.

III. RULES FOR DEALING WITH THE GRAYMAIL PROBLEM

A. Common Law Government Secrets Privilege. The intent of this privilege is to protect material that is vital to national security. Applies particularly to military matters, intelligence-gathering methods and capabilities, and information concerning diplomatic relations with foreign governments. The government as the holder of the privilege must assert it.

B. CIPA. Much broader than the state secrets privilege.

1. Recognizes the power of the executive branch to determine that public disclosure of classified evidence will not be made in a criminal trial.

2. Outlines procedures to protect against threat of disclosure or unnecessary disclosure.

3. Requires the defendant to give notice of intent to reveal classified information as part of the defense.

4. Gives several options to government:

a) Seek a ruling that some or all of the information is immaterial.

b) Move for substitution of non-sensitive summary information.

c) Move for redaction of sensitive information.

d) Admit facts sought to be proven.

5. If government is unwilling or unable to disclose, court may dismiss charges or provide appropriate relief.

6. CIPA cases are the primary source of interpretative materials related to the government secrets privilege.

C. MRE 505. In all key respects, mirrors CIPA. Applies at all stages of the proceedings, including Art. 32, sentencing, post-trial and appeal.

IV. A BRIEF GALLOP THROUGH MRE 505

A. **RULE ONE: COORDINATE ALL THE WAY UP THE TECHNICAL CHAIN WHENEVER THESE ISSUES ARISE. IMMEDIATELY.**

B. Claiming the privilege. Only the head of the executive or military department or government agency concerned can claim the privilege. **Note: This Means the OCA!!!** Authority of TC or witness to claim the privilege is presumed in absence of evidence to contrary. Must make 2 findings.

1. Information is properly classified.

2. Disclosure would be detrimental to national security.

C. Pre-Referral options available to convening authority. If the privilege is claimed prior to referral, CA may:

1. Delete specified items of classified evidence from documents made available to the accused;

2. Substitute a portion or summary of the information for the classified documents;

3. Substitute a statement admitting relevant facts the classified evidence would tend to prove.

4. Provide documents subject to conditions that will guard against compromise of information;

5. Withhold disclosure if necessary to protect national security.

D. Post-Referral. If claim of privilege has been made, and the evidence is **relevant** and **necessary** and **otherwise admissible in evidence**, CA may:

1. Try to obtain the classified information for use of the military judge for an *in camera* hearing;

2. Dismiss the charges;

3. Dismiss the charges or specifications or both to which the information may relate;

4. Take such other action as required by the interests of justice.

5. The MJ can dismiss the charges if the evidence hasn't been provided in a reasonable time and proceeding without it would materially prejudice a substantial right of the accused.

E. Note that MRE 505 is not an independent rule of admissibility! The other rules of evidence still apply.

F. Protective Orders. MRE 505 provides for comprehensive protective orders to preserve classified evidence. Security requirements can be quite onerous and will trump normal working procedures.

G. Accused must notify of intent to use classified information. Information must be in writing and must include a brief description of the evidence. This is a continuing duty.

H. MJ can conduct an *in-camera* review of information in order to determine whether and how it may be disclosed at a court-martial proceeding. An example of how this is done under CIPA is *United States v. Moussaoui*, 333 F.3d 509 (4th Cir. 2003), in which the 4th Circuit, sitting *en banc*, affirmed the decision of a district court under CIPA that an unnamed enemy combatant in US custody was relevant and material to Zacharias Moussaoui's defense but that the interests of national security required a Fed. R. Crim. Proc. Rule 15 deposition rather than unfettered access to the witness.

I. Heightened Relevance Standard. Evidence must be:

1. Relevant; and

2. Necessary; and

3. Otherwise admissible in evidence.

J. Where evidence is necessary to a defense, but the OCA will not authorize disclosure, MRE 505 contemplates, and due process requires, the Government to elect between disclosure and dismissal. *See United States v. Lonetree*, 35 M.J. 396 (CMA 1992).

K. MJ may order sessions of trial closed that will disclose classified material.

V. IDEALIZED APPROACH TO A CLASSIFIED CASE[2]

A. The Beginning Stages:

1. A Crime regarding Classified Information is discovered.

2. The classified information is protected and the breach in security is closed.

3. Special Security Officer is informed of the possible breach (Navy--notifies Det. 17 and NCIS).

4. Law Enforcement begins to investigate.

5. The suspected classified information is sent to the various "equity holders."

6. The "equity holders" screen the information to determine potential level of classification.

7. The information that is suspected of being classified undergoes a classification review.

8. Once the review is completed the OCA verifies the findings of the review and determines whether release should be permitted.

9. In instances where the privilege under MRE 505 is to be invoked memos from OCAs articulating the danger of release of the classified information are produced.

B. Preferral

1. Charges are preferred.

2. Panel is reviewed for security clearances.

3. Government secures an interim security clearance for accused and clearances for defense counsel.

C. Article 32

[2] This journey through the stages of handling a classified case in an ideal world is courtesy of MAJ Timothy MacDonnell, TCAP.

1. An investigation security officer (ISO) and subject matter expert (SE) is assigned to the Article 32 IO.

2. Convening Authority issues a protective order to defense.

3. Article 32 begins with a Grunden hearing (to determine whether the Art. 32 should be open or closed).

4. 32 completed.

5. Charges are referred.

D. Trial.

1. Court has Court Security Officer and a Subject Matter Expert regarding classified information assigned. Note: you should consider appointing a security expert to the defense team.

2. Government or defense moves under MRE 505 for a 39a session to address issues regarding classified material.

3. Court Security Officer insures that the courtroom is prepared should a closed session be necessary-Judge, counsel, accused, bailiff, escorts have clearances; courtroom is appropriate for the presentation of evidence; etc. (Court Reporter may want to use a different machine for recording).

4. Trial has a Grunden hearing.

5. The Court makes specific findings regarding classified issues.

E. The Navy Code 17 publication contains extremely thorough and useful checklists for the SJA, trial counsel, and military judge. **Read it!**

VI. CONCLUSION

A. Classified cases are not easy, but early coordination and planning will help you set the conditions for success.

B. Do not be intimated by MRE 505 or CIPA: they are your (obnoxious) friends.

C. Remember: the OCA controls the information, and if you can't gain release, you may have to dismiss in the interests of justice.