

Primer for Litigating Classified Information Cases



Prosecuting, Defending, and Adjudicating Cases Involving Classified Information

December 2007

National Security and Intelligence Law Division (Code 17)
Office of the Judge Advocate General
Department of the Navy
1322 Patterson Avenue
Washington Navy Yard, D.C. 20374-5066

ACKNOWLEDGEMENTS

This Primer, as well as the very existence of Code 17, is due in large part to the recommendations of the National Security Case Commission Report, signed by Brigadier General David C. Hague, USMC (Ret), on 29 June 2001. This well written and insightful document, also known as the King Commission Report (KCR), is available at Code 17's NKO website. The KCR and this Primer are mandatory reading for any judge advocate facing a case with classified information issues.

This Primer builds on previous editions. Specifically, the 2002 "Handbook for Litigating National Security Cases" finalized by Captain P.M. Delaney, JAGC, U.S. Navy; its predecessor, "Prosecuting National Security Cases: A Handbook for Trial Counsel," promulgated by Commander Homer S. Pointer, JAGC, USN (Ret); and an earlier addition drafted by Major Frank Short, USMC (Ret). These documents, along with the vision of Captain Peter J. McLaughlin, JAGC, USN (Ret), the original Code 17 Division Director, provided a firm foundation for this Primer.

Since 2002, many have dedicated their time and effort to making this Primer a reality. Lieutenant Commander Paul Walker, JAGC, USN, spent hundreds of hours during his Code 17 tenure updating issues and collecting insights including the rewrite of several chapters. Paul's effort was indispensable. Also, Commander George Reilly and Lieutenant Commander Laurin Eskridge spent a great deal of time on this project during their Code 17 tenures as well as members of the reserve unit supporting Code 17, especially Captain Bill Wheeler, JAGC, USNR, Lieutenant Commander Todd Lundquist, JAGC, USNR, and Lieutenant Commander Jennifer Strazza, JAGC, USNR. Finally, two very important individuals assigned to Code 17, Ms. Heidi Beasley and CTA1 Edward Reeves, helped the cause on a daily basis, both directly and indirectly by taking care of other Code 17 business while others were focusing on this Primer.

/s/

P. D. SCHMID

Commander, JAGC, U. S. Navy
Deputy Assistant Judge advocate General
(National Security Litigation and
Intelligence Law)

FOR OFFICIAL USE ONLY

This Page intentionally left blank

FOR OFFICIAL USE ONLY

TABLE OF CONTENTS

<u>Introduction</u>	
<u>Chapter 1:</u>	Litigation of Classified Information Cases – An Overview
<u>Chapter 2:</u>	Classified Information
	- Appendix 2-A (Classified Information References)
<u>Chapter 3:</u>	Reporting Requirements
	- Appendix 3-A (Reporting Check List)
<u>Chapter 4:</u>	National Security Cases
	- Appendix 4-A (Information Paper on National Security Cases)
	- Appendix 4-B (Talking Points on National Security Cases)
<u>Chapter 5:</u>	Other Cases Involving Classified Information
<u>Chapter 6:</u>	Security Requirements
	- Appendix 6-A (Attorney Access Authorization Request)
	- Appendix 6-B (Accused Access Request)
	- Appendix 6-C (Sample Protective Order and MOU)
<u>Chapter 7:</u>	Classification Reviews
	- Appendix 7-A (Sample Classification Review Affidavit)
	- Appendix 7-B (Sample OCA Cover Letter)
<u>Chapter 8:</u>	Charges in Classified Information and National Security Cases
	- Appendix 8-A (Sample Specifications)
<u>Chapter 9:</u>	Military Rule of Evidence 505
<u>Chapter 10:</u>	Courtroom Closures
<u>Chapter 11:</u>	Pretrial Agreements & Grants of Immunity
	- Appendix 11-A (Sample Pretrial Agreement)
	- Appendix 11-B (18 USC 793 Providency & Element Breakdown)
<u>Chapter 12:</u>	The Sentencing Case
<u>Chapter 13:</u>	Post-Trial Matters
<u>Annex A:</u>	Staff Judge Advocate/Trial Counsel Checklist
<u>Annex B:</u>	Defense Counsel Checklist

FOR OFFICIAL USE ONLY

<u>Annex C:</u>	Investigation/Court Security Officer Summary
<u>Annex D:</u>	Classified Information Protections: MRE 505 & CIPA Comparison
<u>Annex E:</u>	DOD-DOJ Memorandum of Understanding

FOR OFFICIAL USE ONLY

INTRODUCTION TO SECOND EDITION

The “Primer for Litigating Classified Information Cases” (the Primer) applies to investigations and courts-martial with classified information issues. It builds on a first edition, released in August 2002. While judge advocates from other services and civilian practitioners involved in the military justice process are encouraged to use this Primer as a reference, the Primer does not include a comprehensive review of Army and Air Force guidance and regulations. However, there are many areas of classified information practice that are universal to all courts-martial, most importantly the application of Military Rule of Evidence 505 and Rule for Court Martial 806. Judge advocates of all services will benefit from the Primer.

Since the release of the first edition, the Navy has successfully litigated two designated national security cases, the first since the *King* case came to an abrupt end in 2001. One of those cases involved espionage on behalf of a foreign power and ended in a guilty plea (*Weinmann*). The other involved a willful compromise of classified information to an unauthorized representative of a non-governmental organization and ended in a conviction following trial before members (*Diaz*). Code 17 is also involved in numerous other cases with classified information issues, including several arising from actions in Operations Iraqi Freedom and Enduring Freedom. These military operations have generated a number of courts-martial and other proceedings in which classified information, although not an element of charged offenses, is relevant and material, to the prosecution’s case, the defense case, or both. In these cases, classified information, such as rules of engagement or SIPR-net email, has been subject to discovery or introduced into evidence. As discussed more fully in Chapter Five, the classified information need not be an element of a charge or specification to be discoverable and potentially relevant to a case. Therefore, it is important for all judge advocates to be aware that the involvement of any classified material in a case literally and figuratively changes the rules.

This Primer is for staff judge advocates, trial and defense counsel, civilian counsel, investigating officers, military judges, and personnel detailed as investigation security officers and/or court security officers. Code 17 will update this Primer as needed, based upon suggestions and comments from practitioners, court opinions, and changes in rules, regulations, or statutes. The Primer is available on the Navy Knowledge Online (NKO) website.

An article in the June 1986 Army Lawyer provides an interesting perspective on litigating a case involving classified information:

The hope of trying a “Big Case” is the fuel that fires the furnace of ambition inside every trial lawyer. For the civilian plaintiff and defense bars, Big cases are usually defined in terms of money damages ... for the military criminal lawyer [a Big case] is defined in terms of the offense...Among the murders, rapes, and other mayhem that we traditionally associate with big cases is a category which is unsurpassed in importance, complexity, and potential for hazard to the advocate—those cases involving classified information. This is so for a fairly obvious reason. The government’s interest in prosecution outweighs its interest in limiting access to the classified material. This usually means that the underlying offense is one involving big money, big issues, or big people. In any event, the lawyer who girds himself or herself with shield and sword to champion the cause of his or her client, faces difficulties and challenges in classified trials that are not encountered in his normal practice.

Major Joseph A. Woodruff, U.S. Army, *Trial Defense Service Notes: Practical Aspects of Trying Cases Involving Classified Information*, 1986 Army Lawyer 50.

Checklists, sample documents, and background information to help illustrate points and issues are appended to this Primer. Annex A is a checklist for staff judge advocates and trial counsel to use when preparing a case involving classified information. Annex B is a checklist for defense counsel to use when defending a case involving classified information. Annex C is summary for investigation and court security officers. Annex D is a comparison of the classified information protections offered by the Classified Information Procedures Act used in federal court and Military Rule of Evidence 505. Annex E is a Department of Defense Instruction that implements the Memorandum of Understanding between the Departments of Justice and Defense regarding the investigation and prosecution of certain types of crimes.

CHAPTER 1

Litigation of Classified Information Cases – An Overview

"What has puzzled us before seems less mysterious, and
the crooked paths look straighter as we approach the
end."

Jean Paul Richter
German novelist and humorist, 1763-1825

The goal of this Primer is to provide all judge advocates with a basic understanding of the evidentiary rules, courtroom closure process, and coordination principles applicable to all investigations and courts-martial involving classified information. This is especially important in today's operationally oriented environment that has resulted in an increase in the number of courts-martial involving classified information.

From an evidentiary standpoint, Military Rule of Evidence (M.R.E) 505 is the center of gravity for any case with classified information issues. M.R.E. 505 is primarily an evidentiary procedure that focuses on what classified information is relevant and necessary, and, if relevant and necessary, what form of discovery is most appropriate. It is the fundamental building block for the pieces of the court-martial puzzle that involve classified information. M.R.E. 505 is a very unique rule that adds an additional layer of complexity to the court-martial. It provides a host of issues and opportunities for both trial and defense counsel to explore and litigate in pursuant of their client's interests. Judge advocates must fully appreciate the quantity and quality of relevant classified information as early in the court-martial process as possible.

For the courtroom closure process, Rule for Court-Martial (R.C.M.) 806 codifies the procedures found in U.S. v Grunden, 2 M.J. 116 (C.M.A. 1977). If closure is an issue, either at an Article 32 investigation or trial, R.C.M. 806(b)(2) provides the resolution framework. In any case involving classified information, judge advocates, especially staff judge advocates and trial counsel, should start thinking about closure issues early in the process.

The Primer's chapters on M.R.E. 505 and courtroom closure process, Chapters 9 and 10 respectively, represent the core chapters of the Primer. A good understanding of the issues discussed in these two chapters, and perhaps most importantly the interplay between M.R.E. 505 and R.C.M. 806, represent the foundation of a judge advocate's successful involvement with any case with classified information issues. Judge advocates should view M.R.E. 505 as a first step that determines what, if any, classified information is relevant and necessary to any given case. The relevance of the courtroom closure process only begins if M.R.E. 505 determines that certain classified information is relevant and necessary. If so, litigants must address courtroom closure issues. These two issues are the two primary differences between a court-martial with classified information

and a court-martial without classified information. Judge advocates should fully understand the different issues at stake in M.R.E. 505 and R.C.M. 806 and appreciate important overlapping issues, most importantly, the requirement to consider alternatives to classified information, e.g., redactions, substitutions or “gists,” and stipulations.

Finally, these types of cases include unique coordination requirements. The intelligence community (IC) has equities in most courts-martial involving classified information. Whoever owns the classified information will have considerable interest in the case. Coordination with IC members must occur at all stages of the process: investigation, trial, and post-trial. Judge advocates involved in classified information cases should view this coordination requirement as significant as the host of laws and regulations associated with the handling of classified information. Neglecting either requirement may not only raise questions regarding professional competence, but also adversely affect, perhaps fatally, the court-martial process. Like security related requirements, IC coordination must start upon a case’s inception and continue until the conclusion of the court-martial process.

In the ideal world, all judge advocates would become intimately familiar with the issues and answers found in this Primer. It is much more probable that judge advocates will take this Primer “off the shelf” when first confronted with a classified information issue. In either case, Code 17 hopes that the Primer will serve a significant purpose and prompt additional interaction with Code 17 personnel. Ultimately, the intent of the Primer is to afford judge advocates the necessary foundation to both zealously represent their clients and protect the interests of national security.

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.

FOR OFFICIAL USE ONLY

B. Substance of Classified Information. 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-OCA's 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:

FOR OFFICIAL USE ONLY

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. Classification Prohibitions. 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.



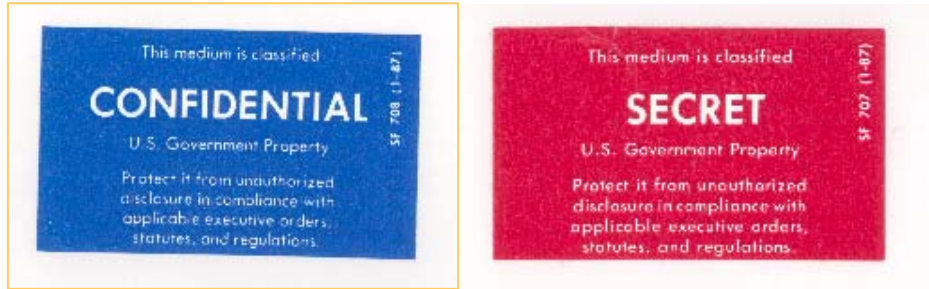
Practice Pointer: BEWARE: All SIGINT information is owned by NSA, even if it originates with a Navy command or Navy-run program! You MUST receive permission from NSA before sharing such information with the defense team.

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. Storage, handling, transmission, reproduction, and destruction. 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. Compartmented Information. 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. Special Access Programs. 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. Sensitive Compartmented Information (SCI). 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.

FOR OFFICIAL USE ONLY

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.

FOR OFFICIAL USE ONLY

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.

FOR OFFICIAL USE ONLY

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.

CHAPTER 3

Reporting Requirements

Due to the sensitive and complex nature of cases involving classified information, especially those designated as national security cases, DoD and DON regulations have established specific reporting requirements. Responsibility for these reports falls in varying degrees upon the local command (commanding officer/security manager), the local law enforcement community (Naval Criminal Investigative Service (NCIS)), and the local legal community (staff judge advocate/trial counsel). Although the staff judge advocate and trial counsel are not personally responsible for all of the reports, they need to be familiar with them to ensure proper case processing. As is often the case, once a judge advocate becomes affiliated with the case, other parties rely on the judge advocate to manage the case.

A. Command-Immediate Actions. Upon discovery of a possible loss or compromise of classified information, chapter 12 of SECNAV M-5510.36 (the Manual) requires the cognizant commanding officer or security manager to initiate a preliminary inquiry (PI). If it is discovered during the PI that a loss or compromise of classified information occurred, the command must promptly notify the local NCIS office. NCIS will determine whether it needs to open an investigation or not, and, in any event, provide assistance to the completion of the PI. Paragraph 12-1 of the Manual defines “loss,” “compromise,” and “possible compromise.” A loss of classified information occurs when it cannot be accounted for or physically located. A compromise is the unauthorized disclosure of classified information to a person who does not have a valid security clearance, authorized access, or need-to-know. A possible compromise occurs when classified information is not properly controlled. The Manual clearly recognizes that every instance of mishandling classified information is not automatically a loss or compromise.

The Manual adds that “[t]imely referral to the NCIS is imperative to ensure preservation of evidence for any possible counterintelligence (CI) or criminal investigation.” (Emphasis added.) The Manual does not require a command to notify NCIS of a “possible compromise.”

Preliminary Inquiry. The PI must be completed within 72 hours, and should contain a conclusion as to the likelihood of an actual loss or compromise. Paragraph 12-5 of the Manual discusses the other information that must be in the PI. The command is required to conduct a PI regardless of whether NCIS has initiated its own investigation. According to paragraph 12-4 of the Manual, the completion of the PI should not normally be delayed because of the pending NCIS investigation. In certain cases, however, the NCIS Special Agent in Charge may request the commanding officer to delay the PI in order to preserve evidence for CI or criminal investigations. Such a request from NCIS is the only reason permitted for holding the completion of a PI in abeyance. The mere fact that a concurrent NCIS investigation is occurring is not sufficient reason to delay the PI since the PI is only a preliminary examination of what occurred and not a complete examination of the facts and circumstances surrounding the loss or compromise.

B. Command -72 Hour Report. Within 72 hours of discovery of the violation, the PI must be completed and sent to the organizations listed in paragraph 12-4 of the Manual, unless the PI concludes that a loss or compromise did not occur, or that the possibility of compromise is remote. If the possible loss or compromise involves special types of classified information, such as Sensitive Compartmented Information (SCI) or Special Access Program (SAP), paragraph 12-8 requires that the PI also be sent to the offices listed for that specific type of information. See Appendix 3-A for a list of the offices that receive the PI.

Special attention should be given to cases that involve SCI and SAP information. It is important to ensure that the special security officer (SSO) has been notified. The involvement of the SSO is vital in cases that involve SCI and SAP material to ensure proper handling of the information and the PI.

1. JAGMAN Investigation. If the PI determines that a loss or compromise occurred, the command having custodial responsibility over the lost or compromised information must initiate a full-scale investigation under Chapter 2 of the Manual of the Judge Advocate General (JAGMAN). The JAGMAN will normally provide a detailed factual investigation and recommend disciplinary action and, if necessary, additional corrective action above and beyond that recommended in the PI. Paragraphs 12-9 to 12-14 of the Manual and Chapter 2 of the JAGMAN discuss this requirement in extensive detail.

2. National Security Cases. If the PI determines that the case may meet the requirements for a national security designated case under JAGMAN § 0126a, the Commanding Officer and NCIS, shall notify the Office of the Judge Advocate (OJAG) (Code 17) for Navy cases and, for Marine cases, the Judge Advocate Division (Military Justice) , within the same 72 hours, .

C. NCIS Reports. If NCIS initiates an investigation for a case that meets the criteria for a national security designated case under JAGMAN § 0126a, NCIS is required to notify the appropriate Department of Justice investigative agency in compliance with the Memorandum of Understanding between the Departments of Defense and Justice and DODD 5525.7, which is Annex E to this Guide.

When the NCIS investigation involves allegations of espionage, SECNAVINST 5500.30F, requires NCIS to notify the Under Secretary of the Navy. Allegations of espionage include those offenses that are described in Article 106a, UCMJ; section 783 of title 50, U.S.C.; and chapter 37 of title 18, U.S.C.

D. Report to National Security Case Disposition Authority (NSCDA). As discussed in Chapter 4, only certain officers are authorized to initially dispose of national security cases. These officers are listed in JAGMAN § 0126f and are designated as national security case disposition authorities (NSCDA). If facts contained in the PI, NCIS investigation, and/or the JAGMAN investigation suggest that the criteria in JAGMAN § 0126a may be satisfied, in addition to the notification requirements detailed above, the command must notify the first NSCDA in the command's administrative chain-of-command during the same 72-hour period. Once the formal JAGMAN investigation and/or NCIS investigation is completed in such a case,

it is to be forwarded to the NSCDA for disposition. The NSCDA, using the criteria discussed in Chapter 4, then must determine whether to designate the case as a national security case. Even if designated as a national security case, the NSCDA can delegate the disposition of the case to any convening authority.

E. NSCDA Reports. Once informed of a potential case by a subordinate command, JAGMAN 0126i requires a NSCDA to submit a SITREP every 15 days to CNO and Navy JAG, via certain staff codes designated in the section. The reports continue until it is either determined that the case is not a national security case or until it is resolved by conviction, acquittal, or other final disposition. The Director of Naval Intelligence (CNO (N2)) is to be included on the reports when the case involves SCI information or intelligence information. Specific requirements for the report are detailed in JAGMAN § 0126i.

F. Reports to OJAG (Code 17) for All Classified Information Cases. In all cases where a violation of the UCMJ involves classified information, regardless of whether or not it is a designated national security case, OJAG (Code 17) is to be notified at least once every 30 days or whenever a major development in the case or investigation occurs, including contemplation of criminal prosecution. Although this section broadly tasks the “command, convening authority, or judge advocate” with the responsibilities, the command will typically rely on the staff judge advocate or trial counsel, if one has been assigned. A judge advocate involved in one of these cases should consider this to be his or her responsibility.

G. Coordination with Intelligence Community (IC). All classified information has an owner, the original classification authority (OCA). The OCA has equities in the court-martial process when the court-martial process includes classified information within the OCA’s purview. Judge advocates, especially staff judge advocates and trial counsel, must keep the IC’s interests in mind as the case proceeds through the process. Coordination with the IC, early and often, is recommended. Code 17 can support this coordination effort.

FOR OFFICIAL USE ONLY

This page intentionally left blank

APPENDIX 3-A

Reporting Checklist

IMMEDIATE REPORT (SECNAVINST 5510.36 § 12-2)

___ Local NCIS Office

72-HOUR REPORT, SENT VIA P.I.**

All incidents, send PI to:

(See SECNAVINST 5510.36, § 12-4)

___ Next superior in administrative chain of command (ISIC)

___ CNO (N09N2)

___ Originator of the classified information

___ Original Classification Authority (OCA)

___ Local NCIS Office

In addition, if incident involves:

(See SECNAVINST 5510.36, § 12-8)

___ DoD SAPS, send to ODUSD(PS) via CNO (N09N2)

___ SIOP/SIOP-ESI, send to JCS and USCINSTRAT by “quickest means”

___ COMSEC info or Keying material, send to controlling authority (e.g., NSA)

___ SCI, send to ONI-522 or COMNAVSECGRU, as applicable, as delegated by DNI in
Navy Supplement to DoDINST S-5105.21.M-1

___ Intelligence sources and methods, send to DNI

___ Non-DoD information, send to DoD Principal Director, Security and Information
Operations (ODASD(S&IO))

___ NATO classified information, send to ODUSD(PS) via CNO (N09N2)

___ Foreign Government Information (FGI), send to ODUSD(PS) via CNO (N09N2)

**Do not send PI if it concludes that a loss or compromise did not occur, or that the possibility of compromise is “remote” due to multiple security controls within the command. See SECNAVINST 5510.36, § 12-7.

FOR OFFICIAL USE ONLY

This page intentionally left blank

CHAPTER 4

National Security Cases

“National Security Cases” are a unique subset of cases that involve classified information. In fact, only a relatively small number of cases that involve classified information are designated as national security cases. Such designation is an administrative designation only within the Navy and Marine Corps and such designation does not supersede or modify the Uniform Code of Military Justice or the Manual for Courts-Martial. The potential for qualification as a national security case is an important determination, because only an officer designated as a National Security Case Disposition Authority (NSCDA) may initially dispose of such cases. Additionally, Navy Legal Service Command has assigned a limited number of commands to maintain special national security counsel available for worldwide assignment to such cases.¹ Once designated as a national security case, the case is subject to special procedural requirements with respect to pretrial agreements, immunity and post-trial processing. In addition, the security and litigation issues applicable to all cases involving classified information, and discussed throughout this Primer, apply to these cases as well.

A. National Security Case Disposition Authority (NSCDA). The limitation on initial disposition authority is pursuant to R.C.M. 306 and JAGMAN § 0126c. JAGMAN § 0126c limits the initial disposition authority for such cases to listed officers. The list is made up of very senior commanders, typically 3-star and 4-star admirals and generals. The following officers are currently designated NSCDAs:

- Chief of Naval Operations;
- Commandant of the Marine Corps;
- Vice Chief of Naval Operations;
- Assistant Commandant of the Marine Corps;
- Commanders, Fleet Forces Command, U.S. Pacific Fleet, U.S. Naval Forces Europe, U.S. Naval Forces Central Command;
- Commander, U.S. Marine Corps Forces Command;
- Commander, U.S. Marine Corps Forces, Pacific;
- Commanders, Sixth and Seventh Fleets;
- Commanding General, Marine Expeditionary Forces;
- Commanders, Naval Air Force, Submarine, and Surface Forces;
- Commander, Naval Education and Training Command;
- Commanding General, Marine Corps Combat Development Command, Quantico, VA;
- Commanding General, Marine Corps Bases, Japan;
- Commanding Generals, Marine Corps Installations East and West;
- Commander, U.S. Marine Forces, Reserve; and
- Commander, Naval Special Warfare Command

¹ The designated commands are NLSO Mid-Atlantic and RLSO Mid-Atlantic in Norfolk, Virginia, and NLSO Southwest and RLSO Southwest located in San Diego, California. See COMNAVLEGSVCCCOMINST 5800.1E, paragraph 1005. In practice, a designated national security case is likely to be tried in one of those two locations as the necessary infrastructure support is located there, as well as military judges specially designated by the trial judiciary.

An officer who is a convening authority, but not an NSCDA, must forward a potential national security case to the first NSCDA in the administrative chain-of-command. The NSCDA may then dispose of the case by any method authorized under R.C.M. 306, to include returning the case to the original convening authority for disposition.



Practice Pointer. In certain cases the NSCDA may designate a case as a national security case but return the case to another commander to serve as the convening authority. This may be done for the pragmatic reason that the other commander may regularly convene general courts-martial and may have the staff experience and processes in place to most expeditiously handle the case. If the NSCDA passes the case to another convening authority, the NSCDA retains overall reporting responsibility and is in the administrative chain of command to the Secretary of the Navy but may not, pursuant to R.C.M. 401(c)(2)(B) and 407(a)(2), direct specific action on disposition of the charges in the case.

B. Identification of a National Security Case. A significant amount of discretion is involved in designating a case as a national security case, and that discretion is vested in the NSCDA. This discretion is contained in the definition of a National Security Case. According to JAGMAN § 0126a, a "National Security Case" is one which:

to any serious degree, involves the compromise of a military or defense advantage over any foreign nation or terrorist group; involves an allegation of willful compromise of classified information, affects our military or defense capability to successfully resist hostile or destructive action, overt or covert; or involves an act of terrorism.

Eligible offenses include an attempt or conspiracy to commit such offenses, as well as conduct aiding and abetting in the commission of such offenses or subsequent unlawful assisting.

Examples of offenses which may be designated as national security cases include, but are not limited to, UCMJ Articles 81, 92 (for violations of SECNAV M-5510.36, "Department of the Navy Information Security Program, June 2006" and U.S. Navy Regulations, 104, 106, 106a, 107, 131, and 134; and provisions of the U.S. Code, such as 18 U.S.C. § 792, 793, 798, 1001, 2151-56, 2331-39b, 2381-85, 2388-90; 42 U.S.C. § 2272-77; and 50 U.S.C. 783. See Chapter 8 of this Primer for a more detailed discussion of charges.

Designation of a case as a national security case requires the NSCDA to weigh many objective and subjective factors. Even a case that involves a charge under 18 U.S.C. § 793, the federal espionage statute, may not be a national security case if no actual compromise occurred or if the offense is not of a "serious degree." Likewise, even if an actual compromise did occur, it might not be a national security case if the unauthorized recipient was, for example, another U.S. government employee who simply happened not to have a clearance or a need to know the particular information. On the other hand, if no actual compromise occurred and the case did not involve an unauthorized recipient, it still could be a national security case if the accused had the

intent to give the information to a foreign agent. For instance, the *Lessenthien* court-martial in 1996 involved a sailor who provided classified information to an FBI agent whom the accused thought was an agent of a foreign power.

The factors which the NSCDA must consider include whether an actual compromise occurred, the status of the recipient, the intent of the accused, the type of information involved, and the gravity of the risk created by the accused. Because designation of a case as a national security case involves a significant amount of discretion and the consequences of such a designation are significant, a command that has a potential national security case should forward the case to an NSCDA for review.



Practice Pointer. The staff judge advocate should consult with both OJAG Code 17 and the staff judge advocate of the NSCDA in the chain of command when the staff judge advocate believes the command may have a potential national security case. There is no stigma attached to seeking an NSCDA opinion on national security case designation at an appropriate time early in the process. A good rule of thumb is that the command should forward a case if it meets any of the listed criteria (e.g., actual compromise, allegation of willful compromise), and then let the NSCDA determine if it rises to a “serious degree.” The NSCDA bases its decision on the facts developed during the investigation. Therefore, while “early and often” contact and coordination is recommended, there is little value added for the NSCDA to review a case if the investigation has not progressed to an appropriate stage. Additional evidence uncovered after an NSCDA has reviewed a case may warrant a new NSCDA determination.

Quick Quiz: Which of the following scenarios could result in designation of the matter as a National Security Case?

1. Sailor apprehended in NCIS sting operation as he tries to sell information related to the Naval nuclear propulsion system.
2. Marine being investigated for leaving laptop containing classified information in a Dubai hotel room safe.
3. Sailor who posted on his blog unclassified information about his ship’s inport security arrangements to show his buddies the “cool machine gun” he was assigned to.
4. Naval officer who uses unclassified e-mail to send logistics information for a ship preparing for a port visit in Aqaba, Jordan “because the SIPRNET computer was down and they needed the information right away!”
5. All of the above.
6. None of the above.

Answer: You simply don’t know without more information! It could be any, all, or none of the above scenarios, depending on the facts developed and the objective and subjective analysis of the NSCDA. While all may be chargeable, not all may be national security cases.

C. Identification of NSCDA and Convening Authority. In most cases, the accused's commanding officer will not be an NSCDA. Thus, the first step is to determine the appropriate NSCDA. The rules are no different than those for determining the appropriate special court-martial convening authority (SPCMCA) or general court-martial convening authority (GCMCA) when the accused's commanding officer does not have such authority. JAGMAN § 0126e clarifies that if the commander has separate operational and administrative chains of command with NSCDAs in each chain, the NSCDA in the administrative chain of command is the primary NSCDA. If there is a specific reason to later change this designation to the operational chain of command NSCDA or another NSCDA, substitution is permissible as discussed below.

If the CO does not have the proper level of authority, he simply forwards the case up his administrative chain of command to the first officer with the proper authority. The only significant difference from the usual GCMCA determination is that the NSCDA may be several levels higher up the chain of command. For this reason also, the cognizant NSCDA may be geographically remote from the local command. In some cases, it may be advisable for the local command and the cognizant NSCDA to request that an alternate NSCDA act on the case. Substitution of NSCDAs should only be done on a case-by-case basis and with coordination between the legal staffs of both NSCDAs and Code 17. Factors to consider are geographic location, availability of secure facilities, and the caseload and legal resources of the NSCDAs.

After the appropriate NSCDA has determined whether a case is a national security case, the next step is to identify who will act as convening authority. The NSCDA may retain the case and act as convening authority, or may forward the case to any other competent convening authority. If the case is not a national security case, normally it will be returned to the original command for processing, although this is not required. If the case is a national security case, the NSCDA will, most commonly, either retain it or forward it to a GCMCA better equipped for convening courts-martial, such as an area coordinator. Often, the NSCDA is senior enough that subordinate commanders and area coordinators handle most military justice matters, including general courts-martial. As discussed above in a Practice Pointer, it is not required that an NSCDA act as convening authority in a national security case, as long as an NSCDA has made the designation and sent the case to a competent convening authority. Remember that regardless of designation as a national security case, the procedures for handling classified evidence, discussed throughout this Primer, must be followed.

D. Special Requirements – Pretrial Agreements and Immunity.

1. Pretrial Agreements. One of the most significant special requirements in a national security case is that the government may not enter into a pretrial agreement without the approval of the Secretary of the Navy.² In accordance with JAGMAN § 0137c, the NSCDA must request permission from the Secretary of the Navy before actually executing a pretrial agreement. The request is sent from the convening authority (who

² In *United States v. Allen*, 31 M.J. 572 (N-M.C.M.R. 1990), the Navy-Marine Corps Court of Military Review ruled that such Secretarial control and involvement in the court-martial process did not constitute unlawful command influence. Essentially, the Manual for Courts-Martial specifically permits the Secretary to withhold authority in a type of case and provides specific authority for the Secretary to issue regulations on the handling of national security cases. See R.C.M. 306(d) and R.C.M. 407(b).

may or may not be the NSCDA) directly to the Secretary of the Navy, with information copies provided to OJAG (Code 17) and the Chief of Naval Operations or Commandant of the Marine Corps, as appropriate. In addition to the text of the proposed pretrial agreement, the convening authority's request must provide the factual background of the case, summarize the available evidence that could be introduced by either the government or defense on the merits and during sentencing, and summarize the factors warranting acceptance of the pretrial agreement. See JAGMAN § 0137c. A careful review of the strengths and weaknesses of the government's case is necessary to ensure that the Secretary is well-equipped to make this decision, especially in cases where the proposed terms are much less than the statutory maximums. Code 17 can assist in preparing the package to the Secretary of the Navy. It is important to note that while the approval of the Secretary of the Navy is required before entering into a pretrial agreement, other decisions by the NSCDA are not subject to secretarial approval, such as identification of an appropriate convening authority or the decision to dispose of the case at a particular forum (e.g., NJP, SPCM).

2. Immunity. If the government intends to grant immunity to any witness in a National Security Case, it must first consult with the Department of Justice, per the "Memorandum of Understanding Between the Departments of Justice and Defense Relating to the Investigation and Prosecution of Certain Crimes." This Memorandum of Understanding requires consultation with DoJ for a proposed grant of immunity in a case involving espionage, subversion, aiding the enemy, sabotage, spying, or violation of rules or statutes concerning classified information or the foreign relations of the United States. (DoD Instruction 5525.07, recently reissued on 18 June 2007, implements this MOU. See Annex E) JAGMAN § 0138d also requires consultation with DoJ in all cases involving national security or foreign relations of the United States. DoJ must also be consulted when an accused is given post-trial immunity as part of a pretrial agreement when he has agreed to be debriefed, including a polygraph. Chapter 11 provides further discussion on pretrial agreements and grants of immunity.

E. Special Requirements - Post-Trial.

1. Supplemental Clemency. If a case has been designated as a national security case, the Secretary of the Navy has reserved "supplemental clemency." This reservation of authority is found in JAGMAN § 0159 and correlates to the requirement that the Secretary of the Navy must approve any proposed pretrial agreement in a National Security Case. JAGMAN § 0159 provides that "[n]o official of the DON, other than the Secretary of the Navy, may remit or suspend, pursuant to article 74(a), UCMJ, and R.C.M. 1107, MCM, any part or amount of the approved sentence in any case designated as a national security case in accordance with section 0126." (Emphasis added.) It is important to remember that the convening authority can still exercise clemency pursuant to UCMJ Article 60 when the convening authority takes initial action approving the findings and sentence. The Secretary of the Navy has only reserved "supplemental clemency" authority in national security cases. U.S. v. Allen, 31 M.J. 572 (1990)

2. Record of Trial. If any part of the record of trial contains classified information, it must be protected just like any other classified document. The overall record of trial should be kept unclassified to the greatest extent possible, and the classified portions removed and placed under separate cover. The classified portion must be handled and stored in accordance with SECNAV M- 5510.36, “Department of the Navy Information Security Program,” June 2006. Before forwarding a record of trial that contains any classified portions, contact Code 17 to coordinate transfer and storage.

Further discussion of post-trial matters can be found in Chapter 13.



Practice Pointer. A command may have the need to explain the rationale for, and impact of, designating a case as a national security case. Code 17 has prepared a summary and talking points that may be adapted by the command for use in working with the public affairs staff on media issues. Those documents are appended to this chapter.

Key Elements of National Security Case Definition

In the opinion of the NSCDA, a case which “to any **SERIOUS DEGREE**” involves:

- **COMPROMISE** of military or defense advantage over any foreign nation or terrorist group;
- Allegation of **WILLFUL** compromise of classified information;
- Affects military or defense **CAPABILITY** to successfully resist hostile or destructive action; or
- Involves an act of **TERRORISM**.

APPENDIX 4-A

Information Paper on National Security Cases

In military justice, the term “national security” is defined as “the national defense and foreign relations of the United States.” Military Rule of Evidence 505(b)(2). A court-martial case may be designated a “National Security Case” by certain Navy and Marine Corps Flag and General officers pursuant to the Manual of the Judge Advocate General (JAGMAN) section 0126. These designated officers are called National Security Case Disposition Authorities (NSCDA’s).

A National Security Case is defined as a case, which, in the opinion of a designated NSCDA, "to any serious degree, involves the compromise of a military or defense advantage over any foreign nation or terrorist group; involves an allegation of willful compromise of classified information; affects our military or defense capability to successfully resist hostile or destructive action, overt or covert; or involves an act of terrorism." JAGMAN section 0126a. The JAGMAN provides an extensive list of potential violations of the Uniform Code of Military Justice (UCMJ) that might be present in a National Security Case. Since the JAGMAN’s list is by no means exclusive, any violation of the UCMJ could be present in a National Security Case once all the factors surrounding the case have been considered.

The test for designation is a combination of objective criteria, *i . e .* , the circumstances are one of the four listed in the section, and the subjective evaluation of seriousness of the activity by the NSCDA. Since not all cases involving matters or information related to national security will rise to the level of requiring the designation of a National Security Case, the JAGMAN’s key phrase is “to a serious degree.” A variety of factors will need to be considered such as whether an actual compromise of classified information occurred. If, in fact, information was passed, it will be necessary to determine who may have received the classified information. The sensitivity of the information can affect the potential designation as a national security case as can the accused’s intent. Certainly, a willful intent to harm the nation’s security by passing highly classified sensitive compartmented information will weigh more heavily than a negligent or inadvertent compromise.

JAGMAN section 0126 directs special procedures for the investigation, review, and referral of cases that may qualify for designation as National Security Cases. It also mandates certain periodic and recurring reporting obligations in such cases. Other than these special procedures, the case is handled in the same manner as any other court-martial.

The designation of a case as a National Security case does not in any way limit the rights of an accused during the court-martial process. If an NSCDA designates a case as a National Security Case it triggers certain special reporting mechanisms within the Department of the Navy, and mandates the Secretary of the Navy approval of pre-trial agreements, immunity requests, and post-trial relief. Other procedural requirements for protection of classified information are the same as for any case involving classified information. These can include closure of portions of the Article 32, UCMJ, investigation and subsequent court-martial to members of the public, including the media, pursuant to the provisions of Military Rule of Evidence 505.

FOR OFFICIAL USE ONLY

This page intentionally left blank

APPENDIX 4-B

Talking Points on National Security Cases

Q1. What is a National Security Case?

A1. This is a court-martial that has been specifically designated as such because the case involves, to a serious degree, the compromise of a military or defense advantage over any foreign nation or terrorist group; involves an allegation of willful compromise of classified information; affects our military or defense capability to successfully resist hostile or destructive action, overt or covert; or involves an act of terrorism.

Q2. Are all courts-martial involving national security designated as National Security Cases?

A2. No, only those cases of a serious enough nature to require the designation should be so designated. A case may involve national security matters, such as an inadvertent disclosure of classified information, but does not rise to the level of requiring such a designation and the additional procedural requirements that accompany the designation.

Q3. Who makes this determination and how do they do so?

A3. The JAGMAN lists the National Security Case Disposition Authorities at Section 0126(f). They are high level Officers within the Department of Navy chain of command. The JAGMAN tasks the NSCDA with looking at the facts of the case to determine whether they fall within the category of a National Security Case and whether the facts and circumstances are of a serious degree to warrant such a designation.

Q4. Is a National Security Case different than a typical court-martial?

A4. A National Security Case involves the application of special procedures to the regular court-martial process for cases designated pursuant to JAGMAN section 0126. These procedures do not impact the rights of the accused or change the court-martial process. These procedures are intended to ensure that the Navy's senior leadership is involved in such critical matters as approval of a pre-trial agreement, granting immunity to a witness, or making a determination that an accused deserves clemency following a conviction.

Q5. Why does the Navy designate cases as National Security Cases? Do the other Services have similar designations?

A5. The Department of the Navy established this designation for certain serious cases to ensure that the Secretary of the Navy was actively involved in specific critical decisions in a case. One reason is that these cases often involve information from sources outside of the Navy or outside of the Department of Defense. The Secretary or his designee can ensure that the interests of those organizations are properly considered in rendering certain decisions in the case, though the final decision rests with the Secretary or his designee. This designation only applies to Navy and

Marine Corps cases. No other Service has such a designation though they may have special procedures for certain types of courts-martial.

Q6. Does designation as a National Security Case pre-determine that the accused is guilty of committing serious offenses endangering national security?

A6. No. Just as the decision to send a case to a general court-martial does not pre-judge an accused's guilt, the decision to designate a case as a National Security Case does not change the presumption of innocence nor does it change the Government's burden to establish the accused's guilt beyond a reasonable doubt. It is simply a procedural mechanism to ensure that senior Navy and Marine officers are supervising the case, and that the Secretary of the Navy makes certain decisions in the case if those decisions are necessary in the case. While the facts and circumstances known to the NSCDA may indicate that the case "involves the compromise of a military or defense advantage over any foreign nation or terrorist group; involves an allegation of willful compromise of classified information; affects our military or defense capability to successfully resist hostile or destructive action, overt or covert; or involves an act of terrorism," the Government must still prove the charges at court-martial beyond a reasonable doubt.

Q7. Doesn't the involvement of the Secretary of the Navy constitute unlawful command influence in a case?

A7. No. The Secretary is not involved in the court-martial process except to render certain decisions for which intra-DoD or interagency coordination may be required. The NSCDA is a general court-martial convening authority and makes all of the decisions in the case as to charges, appointment of an investigating officer, review of the case following investigation for referral to a court-martial, and assignment of court-martial members, among other routine court-martial responsibilities.

The Secretary is notified of the designation of the case as a National Security Case but takes no action unless and until a pre-trial agreement proposal, whose terms are mutually agreeable to both the accused and the convening authority, is presented for approval [JAGMAN section 0137c], or a request for immunity is submitted which must be coordinated with the Attorney General [JAGMAN section 0138d].

Q8. Does a National Security Case have to involve classified information?

A8. No. The definition of a National Security Case in JAGMAN section 0126a specifies only one of the four general types of qualifying cases as involving classified information. Most if not all designated National Security cases do involve classified information to some degree but that it not a requirement for designation.

CHAPTER 5

Other Cases Involving Classified Information

As discussed in Chapter 4, “National Security Cases” are a unique subset of cases that involve classified information. However, only a relatively small number of cases that involve classified information will actually be designated as national security case. Therefore, the odds are that a judge advocate assigned to a case involving classified information will in fact have a non-national security designated case. The general rules and procedures for handling and securing classified information are essentially the same for any case involving classified information as they are for national security designated cases.

These more routine cases involving classified information are less complicated because they do not involve the complicating factor of a National Security Case Disposition Authority (NSCDA) as the disposition authority in the case. In non-national security designated cases, the command follows the normal process for convening a court-martial. There is also no requirement for SECNAV approval of pretrial agreements and certain post-trial actions. However, grants of immunity still need to be coordinated with the Department of Justice in accordance with JAGMAN § 0138. This is especially crucial if the accused agrees to a polygraph as part of a pretrial agreement, which is often the case in a court-martial involving classified information. Again, the “ordinary” rules apply to this type of case in addition to the application of M.R.E. 505 (detailed in Chapters 9 and 10), coordination with Code 17, security requirements, and other specific issues discussed in this Primer.

A. Types of Cases Likely to be Seen. Non-national security designated cases generally fall into one of two categories: mishandling cases and cases where the classified information is not directly relevant to an element of an offense. The latter category of cases has seen a dramatic increase because the ongoing military operations in Iraq and Afghanistan have resulted in a significant increase in courts-martial involving classified information. Both categories are discussed more fully below.

1. Mishandling Cases. Mishandling cases generally involve an individual either intentionally or negligently failing to properly safeguard classified information in accordance with applicable regulations. Such cases may result in actual loss of classified information or even compromise to someone without a clearance, but for various reasons are not designated national security cases. For instance, they may not meet the “serious degree” requirement of JAGMAN § 0126a or there may not be sufficient evidence that an actual loss or compromise occurred.

(a) Negligent Handling. Negligent failure to properly follow security regulations that results in classified information exposed to possible loss or compromise is a common mishandling case. Often such cases do not result in court-martial, but are resolved at non-judicial punishment and usually result in a review of security procedures and increased training. Negligent mishandling cases that go to court-martial are often the result of repeated incidents and warnings. More often than not, negligent mishandling charges are charges added to other, more serious,

offenses that do not involve classified information. Another consideration that may lead to a negligent mishandling case being referred to a court-martial is the amount or level of classified information negligently lost or mishandled. In other words, the seriousness of the potential loss or compromise. Conversely, Code 17 is aware of one recent case where a large amount of extremely sensitive material was lost through what can only be described as gross negligence given the controls in place for that level of material. Nonetheless, the case was not referred to court-martial precisely because of the extreme sensitivity of the material that was lost.

(b) Intentional Mishandling. This type of mishandling case results from a willful and knowing disregard of security regulations by the accused. In these cases, the accused is well aware of the requirements of the regulations, but chooses to ignore them because he did not want to be subject to such constraints. This type of case is often characterized as a “self-help” case. The most common types of self-help cases are:

“I needed some extra study time before my qualification exam.” This excuse is especially prevalent in ratings that routinely use classified information and will be tested on various items on their rating exams. This leads to removal of study texts or notes from the command, which are often found and turned over to the authorities either by a disgruntled spouse or ex-roommate.

“I needed to cut a few corners in order to get the mission accomplished!” This excuse is most commonly used by those who view the classification regulations as impediments to their ability to do their jobs effectively or efficiently. A common scenario is taking classified information from one job to the next, but doing so by improperly copying information to CDs, thumb drives, and personal laptops. It is very possible to accomplish the same end using the security regulations (see Chapter 2 on transportation and transmission of classified information), but rather than do so, the individual takes the easy way out and knowingly violates the regulations.

“There was no time to get to the base so I secured the material in my room.” Laziness or poor planning is a common component of mishandling cases. Such cases often evolve into more egregious cases because after the initial failure to safeguard, the perpetrator is usually in no hurry to return the material reasoning that the harm has already occurred. However, the longer the material remains outside proper controls the greater the possibility of loss or inadvertent compromise. In addition, after the first instance of failing to safeguard classified information properly, it becomes easier for the course of conduct to continue.

“Everyone knew this report was not properly classified as Secret so I went ahead and took off the markings.” This excuse is not seen in courts-martial as often as the others are, but the first part of the statement is a common sentiment in many intelligence circles. Most of those who work in the field, however,

understand that just because something has been published by the media does not mean it is no longer classified. Information remains classified until it is formally declassified by proper authority.

While compelling, and often creative, such excuses rarely amount to a legal defense or justification to dereliction of duty or orders violation charges, but may be persuasive as to forum or disposition. Especially when the use was designed by the accused to benefit the Navy, such excuses are often used in the defense extenuation and mitigation case. Additionally, a self-help case on a battlefield, e.g., sharing classified information with a coalition partner that does not have the appropriate clearance, could contain significant facts to support a relatively lenient command response.

2. Operational Cases. In cases arising from the Global War on Terror, the classified information generally does not form the basis for the charges, but rather is relevant in some way to the allegations in the case. For example, in the cases of the Marines charged with murdering an Iraqi man in Hamdania, Iraq, the defense sought to use classified information to characterize the victim as one of the “bad guys.” The defendants in the Hamdania cases were all alleged to have taken an active role in the planning, abduction, and murder of the victim. These “shooter” cases generally involve the use of classified information such as the Rules of Engagement (ROE) in place at the time of the killing, the use of force rules, operations orders, battle updates, and intelligence briefings. The average Marine or soldier, such as those involved in the Hamdania cases, will not have direct knowledge of the latter two categories of information. It is possible, though, that they will have a very good idea of the results of the update and intelligence briefings, e.g., who the targets are and other information needed to complete the intelligence picture. Thus, in the Hamdania cases some of that material was found to be relevant and admissible to the accused’s state of mind regarding the threat faced by the Marines in their operations area.

A second category of cases involve “non-shooter” cases, i.e., senior personnel in the chain-of-command charged with offenses such as dereliction of duty for failing to investigate possible war crimes, obstruction of justice, false official statement and other “non-shooter” offenses. In the Haditha cases, the battalion commander, his staff judge advocate, Human Exploitation Team Leader, and the platoon commander were all charged with dereliction of duty for failing to investigate the deaths of 24 Iraqis, including women and children, following the explosion of an improvised explosive device that killed a Marine and wounded two others. In this type of case, the classified information is relevant to proving or defending against the charges because there is often a great deal of SIPR-net email traffic and classified briefing slides prepared before, during, and/or after the operation at issue. ROE are less important to these types of charges because the actions of the shooters are not as relevant as actions taken by the chain-of-command. Operation orders containing information on Commander’s Critical Information Requirements and watch logs are also very important to understand the requirement for reports on various topics, as well as a historical record of what reports were actually made.

B. Military Commissions. The Military Commission detainee cases represent another group of cases involving classified information. Although the applicability of the Military Commission rules is very narrow, they bear mentioning because of the fact that Military Commission Rule of Evidence (M.C.R.E.) 505 is drawn directly in many respects from M.R.E. 505. As a result, much of the discussion contained in this guide on M.R.E. 505 is directly relevant to commission practice. Those working on the commission cases are encouraged to conduct a thorough comparison of the two rules so that they are aware of the subtle differences between them. A full understanding of M.R.E. 505 coupled with the unique features of M.C.R.E. 505 allow counsel to both appreciate and take advantage of the gaps, advantages, and opportunities present in M.C.R.E. 505.

CHAPTER 6

Security Requirements

The Navy maintains two security programs that have a direct impact on the conduct of courts-martial involving classified information: the personnel security program and the information security program. The personnel security program deals with the administration of security clearances and provides the adjudicative criteria used to determine whether or not someone will be granted a clearance and subsequent access to classified information. This program is important because all of the counsel (including civilian counsel), members, bailiff, and court personnel (including the military judge) involved with a classified information case must have a security clearance. The information security program deals with the security of classified information itself, providing all the standards for storage and handling of classified information, whether in document form or electronic media.

A. Personnel Security. The Navy's Personnel Security Program is contained in SECNAV M-5510.30.. The personnel security rules for Sensitive Compartmented Information are found in Director of Central Intelligence Directive (DCID) 6/4. Personnel security pertains to the policies, rules, and procedures for security clearances.

1. Department of the Navy Central Adjudication Facility (DONCAF). The single authority for granting security clearances for the Navy is the Department of the Navy Central Adjudication Facility (DoNCAF). DoNCAF determines eligibility for all Confidential, Secret and Top Secret clearances. The adjudicative decision is based on the results of a security investigation that has been conducted on the person's background based on the submission of a personnel security questionnaire (SF-86). A person is eligible for a security clearance only after a finding that, based on all available information, the person's loyalty, reliability and trustworthiness are such that entrusting him or her with classified information is clearly consistent with the interests of national security. DoNCAF does not grant access to specific classified information, nor does it grant access to sensitive compartmented information. Once a person has been declared eligible for access to a specified level of information, it is the individual's command that actually grants him or her access to classified information. Generally, access is based on a "need to know" the information in the performance of official duties.

DoNCAF's determination that a person does or does not meet the loyalty, reliability, and trustworthiness criteria for clearance eligibility is not subject to judicial review. *Department of Navy v. Egan*, 484 U.S. 518 (1988). Courts are authorized, however, to ensure that agencies follow their own regulations in making the determination and the regulations regarding the individual's ability to appeal adverse security determinations.

2. Security Clearances in Navy Courts-Martial. All personnel who will handle classified material during a case that involves classified information will be

required to hold a proper security clearance. This typically includes the Article 32 investigating officer, military judge, all defense counsel (including civilians), all trial counsel, court reporters, bailiffs, brig chasers, some witnesses, members, the investigation security officer, and the court security officer. The current policy of the Commander, Naval Legal Service Command, is to require three military judges, two government counsel, and two defense (one on each coast) to maintain security clearances at the Top Secret/Sensitive Compartmented Information level so that they are ready to handle national security cases, regardless of the classification level of information involved. As all officers are required to maintain eligibility for a Secret clearance, any JAG can normally handle the average mishandling case that is limited to Secret information. When defense counsel representation could conceivably involve classified information, defense counsel must immediately ensure that they understand the highest possible level of classified information involved. Defense counsel must ask their client this question at the beginning of their initial meeting to ensure that defense counsel has the appropriate clearance. This will help avoid delays that might be encountered if the accused forms an attorney-client relationship with a defense counsel without the appropriate clearance and ensures that defense counsel establish a firm foundation for competent representation.

(a) Civilian Defense Counsel. Civilian defense counsel also require the appropriate clearances. In the event the accused retains civilian defense counsel, the convening authority should immediately direct in writing that the civilian counsel apply for security clearances. This is often done via the protective order, but can also be done in a letter from the convening authority. Paragraph 9-11 of SECNAV M-5510.30 describes the procedures for civilian counsel to receive access to classified information. The request, usually sent by the detailed defense counsel, is sent to CNO (N09N2), via the Office of the Judge Advocate General (Code 17), along with a completed personnel security investigation request form (SF-86). A sample letter is provided at Appendix 6-A. Code 17 will conduct an initial review of the SF-86 to ensure it is properly completed. The Code 17 endorsement on the request will certify the counsel's need for access. Code 17 will also normally ask for interim access for the civilian counsel. If interim access is requested, CNO (N09N2) will conduct a formal adjudicative review of the SF-86 and if it contains no adverse matters, will issue the interim access. The SF-86 will then be submitted to Office of Personnel Management (OPM) for formal investigation and eventual final adjudication by DoNCAF. If the case involves Special Access Program material or Sensitive Compartmented Information then, in addition to CNO (N09N2), the Navy's Special Security Officer will be involved in the access decision. Code 17 will forward such requests as appropriate, providing the information required by SECNAV M-5510.30, paragraph 9-11.

If the civilian defense counsel wants to represent an accused in a court-martial involving classified information, civilian defense counsel must cooperate with the process to obtain a clearance. In *United States v. Jolliff*, a case tried under CIPA, the defense counsel was reluctant to submit to a security clearance process. The court stated: "Although the Sixth Amendment grants an accused an absolute right to have assistance of counsel, it does not follow that his right to a particular counsel is absolute." *Jolliff*, 548 F.Supp. 227 (D. Md. 1981). This was a warning that counsel's failure to cooperate in obtaining a security clearance can lead to disqualification and dismissal from the case by the trial judge. See also *United States v. Pruner*, 33 M.J. 272 (CMA 1991); *United States v. King*, 2000 CAAF Lexis 472 (2000) (ordering stay of proceedings until defense granted clearance or Government demonstrates defense counsel have not promptly provided necessary information for clearances).

(b) Access for the Accused. In espionage and mishandling cases, the accused's access to classified information will usually be suspended upon the initiation of the preliminary inquiry by the command. Once charges are preferred to court-martial and defense counsel is assigned, the accused will usually need access to the classified information at issue in the case. In the past, a request for access by an accused followed a process similar to that for civilian counsel. However, CNO (N09N2) no longer make access determinations for an accused in courts-martial. Such determinations are properly made by the convening authority who can balance the accused's Sixth Amendment confrontation right with the needs of national security. The convening authority, as does any commander, has the authority to grant such limited access under the provisions of SECNAV M-5510.30 and M.R.E. 505(d)(4) (stating that upon a request by the accused for classified information, the convening authority may "[p]rovide the document subject to conditions that will guard against the compromise of the information disclosed to the accused"). A sample letter from a convening authority granting limited access to the classified information necessary for his case is provided at Appendix 6-B. Prior to receiving access to the information, the accused will have to complete a Non-Disclosure Agreement (SF-312), regardless of whether the accused has previously completed one.

B. Information Security. The Navy's Information Security Program is contained in SECNAV M-5510.36. Information security pertains to the policies, rules, and procedures for classifying, safeguarding, transmitting, and destroying classified information. Chapter Two of this Primer summarizes the basic security concepts and regulations that counsel handling a classified information case must know. Beyond the basic handling and safety precautions for all classified information, specific issues that arise in courts-martial are discussed below.

1. Document Security. All parties to the court-martial are responsible for the security of classified documents. However, the investigation security officer and

court security officer will have primary responsibility once they are appointed. If adequate facilities are available to provide the appropriate level of protection, it is recommended that trial and defense counsel maintain their own files of classified evidence. This will often be difficult with Sensitive Compartmented Information, which must be kept in a Sensitive Compartmented Information Facility (SCIF). In such cases, one option is to designate specific storage areas, e.g., one drawer in a safe for each side's Sensitive Compartmented Information and Special Access Program material. During a court-martial where classified information will be in the court room, the court security officer bears primary responsibility for ensuring that all material is appropriately protected (watched by someone with proper clearance) or stored during breaks in the proceedings. In cases involving Sensitive Compartmented Information or Special Access Program material, all parties must be aware of any special handling procedures for this material.

2. Computer Security. Any documents produced by the military judge, government counsel, or defense counsel that contain classified information must be prepared on a computer designated for classified material. The command security manager or special security officer can provide laptop computers capable of classified word processing. Desktop computers approved for classified word processing must have a removable hard-drive. The laptop computer or removable hard-drive must be maintained and stored in an approved safe (or a SCIF for Sensitive Compartmented Information or Special Access Program material) when not in use. Any computer disks used to store information must be labeled to reflect the appropriate level of classification. If documents at the Top Secret/Sensitive Compartmented Information level are produced, then the appropriate intelligence agency and/or program office must approve use of the computer. At the conclusion of the proceeding, the classified information must be removed from the laptop computer or the removable hard drive and transferred to a floppy disk. The disk will then be inventoried and stored with the original transcript or record of trial. The hard drives should then be sanitized in accordance with applicable security procedures.

3. Court Recording Equipment. The military judge, court reporter and the court security officer must devise a system to record classified (closed) sessions that maintains security for the classified information discussed. Any media storage device, such as a hard drive or cassette tape that is used to record classified sessions becomes classified at the same level as its contents. The method of recording must be examined carefully to ensure that there is no risk of compromise of the classified information. This may be as simple as ensuring that separate cassette tapes are used for classified sessions than the unclassified ones. In any event, it is strongly recommended that the classified media be well-marked before the classified session. This way, the classified portions can be stored separately and transcribed by a court reporter with the requisite security clearance. The unclassified portions may still be contracted out for transcription.

C. Protective Order. A protective order should always be issued when classified information is going to be disclosed to the defense. If that disclosure will occur before referral, for example, before the Article 32 proceeding, then the protective order will be issued by the convening authority. Once the case is referred to trial, the government should always file a motion under M.R.E. 505(g)(1) to have the military judge issue a new protective order now that he has jurisdiction over the case. In both cases, the purpose of the protective order is to guard against the compromise of the classified material. The protective order will generally serve as the security procedure guide for the case. It can include a wide range of terms and conditions for the proper handling of classified material at the proceeding(s). Generally speaking, the protective order requires storage of classified materials in a manner consistent with the classification level of the documents, mandates that all persons required to obtain security clearances must cooperate with background investigators in obtaining clearances, and regulates the making and handling of notes derived from classified material. In addition, the protective order appoints an investigation security officer for an Article 32 investigation or a court security officer for a court-martial. If desired, the convening authority and/or military judge may appoint both the investigation security officer and the court security officer in a document separate from the protective order.

Among other things, the protective order will require the accused and any civilian counsel in the case to enter into a Memorandum of Understanding (MOU) with the convening authority that protects the classified information to be disclosed. The military judge may choose to adopt the protective order that was in effect prior to referral. A protective order may be issued regardless of whether the classified information privilege under M.R.E. 505 has been invoked. *See* R.C.M. 405(g)(6). A sample protective order and MOU are in Appendix 6-C.

D. Role of the Investigation Security Officer and the Court Security Officer. As stated above, the protective order will appoint an investigation security officer and/or court security officer who is charged with safeguarding classified material during the proceeding. Both the investigation security officer and court security officer are neutral and serve as the security advisor to the Article 32 investigating officer or military judge and serve as experts on protecting classified information. The investigation security officer and court security officer should have considerable familiarity with the material relevant to the proceeding so that they can best advise the investigating officer or military judge with regard to what information is classified and the required handling procedures for the specific classified information at issue. If specific programs or special access material is at issue in a particular session (open or closed), it may be necessary to have a subject matter expert serve as a security officer to assist in signaling the investigating officer or military judge when a question calls for classified information or testimony inadvertently strays into classified matters.

It is paramount to remember that none of the security officers is a member of the prosecution or defense team. Rather, all security officers are primarily responsible to the investigating officer or the military judge for providing security guidance and assistance to the proceeding, including, as necessary, the government and defense teams. The

security officers are there to prevent the military judge and the government and defense teams from committing security violations. They advise the investigation or court from a security perspective, not from a legal perspective. The defense should request an expert in security issues from the convening authority should they feel the need, based on the facts of the case, to receive privileged advice on those issues.

Security officers should be experienced military members with a broad background in information, personnel, and physical security. Convening authority staff judge advocates, working with the local security managers and special security officers, should identify a pool of individuals with requisite backgrounds.. These individuals must be cleared for the material that will be at issue in the proceeding. This means that if the proceeding involves classified material from a Special Access Program (SAP) or at the level of Top Secret/Sensitive Compartmented Information, then the security officers must be "read in" and cleared to handle that particular information. It is incumbent upon the staff judge advocate to ensure that an investigation security officer is assigned to the case at the outset. This is usually done by naming the investigation security officer in the Article 32 appointing order or in the protective order.

The security officers also ensure that all the necessary parties have the requisite security clearances and accesses. They also generate an access list that contains the names of the personnel authorized to be in the courtroom during classified sessions. The bailiff or a door sentry may use this list to prevent unauthorized access to the courtroom.

E. Physical Security. The security officers are also tasked with ensuring that the physical security requirements are met and that the courtroom is secure in the event the military judge allows classified evidence or testimony to be presented. Both government and defense counsel should have dedicated safes where they can store classified material. No attempts, however reasonable, should be made to allow the government counsel and defense counsel to share a safe unless the drawers have separate combination locks.

If the evidence in the proceeding involves material classified at the Top Secret/Sensitive Compartmented Information level, then that evidence can only be discussed or presented within a specially designed Sensitive Compartmented Information Facility (SCIF). The SCIF must meet certain construction requirements -- including approved locks and alarms -- outlined in Director of Central Intelligence Directive 6/9. Top Secret/SCI material can only be stored inside a SCIF that has been accredited by a special security officer. It is important to remember different intelligence agencies may have differing physical security protocols. Therefore, Top Secret/Sensitive Compartmented Information and Special Access Program material may be of such a nature that a particular intelligence agency or program office may have additional approval/accreditation requirements. The information security officer and court security officer are tasked with obtaining the additional approval/accreditation that might be required.

Accredited SCIFs are not plentiful. Those that are available are typically in high demand. As soon as the convening authority's staff judge advocate and the government counsel become aware that material requiring a SCIF might be at issue in a case, they must take

immediate action to reserve adequate facilities for the handling of this material. Ideally, one SCIF should be reasonably dedicated to the exclusive use of the defense counsel and another for government counsel for the duration of the case. This would allow each side to work, store documents, and hold meetings at the Top Secret/Sensitive Compartmented Information or Special Access Program level. However, this is usually not practical, so alternative arrangements must be made that protect both the security of the material and the attorney work product of each side, e.g., one drawer in a safe for each side's material.

FOR OFFICIAL USE ONLY

This page intentionally left blank

APPENDIX 6-A

Attorney Access Authorization Request

5510
23 Nov 04

From:

To: Chief of Naval Operations (N09N2)

Via: Office of the Judge Advocate General (Code 17)

Subj: REQUEST FOR ACCESS AUTHORIZATION FOR ATTORNEY NAME, SSN

Ref: (a) SECNAVINST 5510.30A

1. In accordance with reference (a), limited access authorization is requested for the following individual:

- a. NAME, SSN
U.S. citizen
- b. Date and Place of Birth:
- c. Security Clearance: None
- d. Military Experience: None
- e. Level requested: (Choose one) Secret / Top Secret
- f. Duration of Access: until legal proceedings have concluded, approx. 1 yr

2. Mr. X has been retained as civilian defense counsel for PO ACCUSED, USN, ACC's SSN, a Navy member undergoing court-martial proceedings for (summary of charges). The case requires access to classified material at the SECRET level at a minimum, and potentially at the TOP SECRET level. The Accused's Court Martial is scheduled for DATE.

3. Access for Mr. X is necessary in order for the Accused to receive due process and a fair trial. Denial of access would impede the Accused's defense and prevent full discussion with the Accused. Therefore, expedited access is requested as soon as possible.

4. Please contact me at # if you have any questions in this matter.

Very respectfully,

FOR OFFICIAL USE ONLY

This page intentionally left blank

6-A-2
FOR OFFICIAL USE ONLY

APPENDIX 6-B

Accused Access Request

5510
Ser ___/
[Date]

From: Commander, Network Warfare Command
To: [Accused]
Via: [Detailed Defense Counsel]

Subj: ACCESS AUTHORIZATION FOR LCDR I. M. SMART, USN

Ref: (a) [Defense Counsel] ltr of _____
(b) M.R.E. 505, Manual for Courts-Martial (2005)
(c) SECNAV M-5510.30

1. For the purposes stated in reference (a), you are authorized access to national security information classified up to and including Secret.
2. Your access is limited to [matters related to preparation of your defense to the charges preferred on (DATE)] [discussion of the classified statement you provided to NCIS with your detailed and properly cleared defense counsel]. I reserve the right, in consultation with applicable original classification authorities, to limit your access in accordance with paragraph (d) of reference (b).
3. Physical custody and retention of classified material is not authorized. You are to comply with all rules and regulations regarding handling and safeguarding classified material. [Specifically, you are reminded of the terms of my previously issued protective order in this case, reference (c). **(NOTE: Should use this language and a protective order for post-preferral access; not necessary for limited, pre-preferral access)**]
4. You must complete the Classified Information Nondisclosure Agreement (SF-312) required by paragraph 9-4 of reference (d[c]) prior to receiving access to any classified information. Copies will be provided to my Staff Judge Advocate, trial counsel, the Office of the Judge Advocate General (Code 17), and, if applicable, the designated Investigation/Court Security Officer.

I. C. Onvene

FOR OFFICIAL USE ONLY

This page intentionally left blank

6-B-2

FOR OFFICIAL USE ONLY

APPENDIX 6-C

Sample Protective Order and MOU

5 Nov 05

From: Convening Authority
To: (1) Detailed Trial Counsel
(2) Detailed Defense Counsel
(3) Retained Civilian Defense Counsel
(4) Accused
(5) Investigation Security Officer(s)

Subj: PROTECTIVE ORDER FOR THE PROTECTION OF CLASSIFIED
INFORMATION DURING ARTICLE 32 AND COURT-MARTIAL
PROCEEDINGS ICO U.S. V. CTA1 MAXWELL SMART, USN

Ref: (a) M.R.E. 505
(b) SECNAVINST 5510.36
(c) TSO Security Manager ltr of 12 Oct 04

1. The purpose of this Protective Order is to prevent the unauthorized disclosure or dissemination of classified national security information in the subject named case pursuant to references (a) and (b). This Protective Order covers documents previously made available to the accused in the course of his employment with the United States Government or which have been, or will be, reviewed or made available to the accused and defense counsel in this case.

2. In order to protect the national security and pursuant to relevant executive orders of the President of the United States; regulations of the Departments of Defense and of the Navy; and the general supervisory authority as the Convening Authority; it is hereby ORDERED:

a. That the procedures set forth in this Protective Order and the security procedures referred to above will apply to all Article 32 investigation, pretrial, trial, post trial and appellate matters concerning the subject named case.

b. As used herein, the term "classified national security information or document" refers to:

1. Any classified document (or information contained therein);

2. Information known or that reasonably should be known by the accused or defense counsel to be classified. If the accused or defense counsel are uncertain as to whether the information is classified they must confirm whether the information is classified;

FOR OFFICIAL USE ONLY

3. Classified documents (or information contained therein) disclosed to the accused or defense counsel as part of the proceedings in this case;

4. Classified documents and information which have otherwise been made known to the accused or defense counsel and which have been marked or described as: "Confidential," "Secret," or "Top Secret."

c. All such classified documents and information contained therein shall remain classified unless they bear clear indication that they have been declassified by the agency or department of government (hereinafter referred to as "original classification authority") that originated the document or the information contained therein.

d. The words "documents" or "associated materials" as used in this Order include, but are not limited to, all written or printed matter of any kind, formal or informal, including the originals and all non-identical copies, whether different from the original by reason of any notation made on such copies or otherwise, including, without limitation, papers, correspondence, memoranda, notes, letters, telegrams, reports, summaries, inter-office and intra-office communications, notations of any sort bulletins, teletypes, telefax, invoices, worksheets, and all drafts, alterations, modifications, changes and amendment of any kind to the foregoing, graphic or aural records or representations of any kind, including, without limitation, photographs, charts, graphs, microfiche, microfilm, video tapes, sound recordings of any kind, motion pictures, any electronic; mechanical or electric records or representations of any kind, including, without limitation, tapes, cassettes, discs, recording, films, typewriter ribbons and word processor discs or tapes.

e. The word "or" should be interpreted as including "and," and vice versa; "he" should be interpreted as including "she," and vice versa.

(f) Those named herein are advised that direct or indirect unauthorized disclosure, retention, or negligent handling of classified information could cause serious and, in some cases, exceptionally grave damage to the national security of the United States, or may be used to the advantage of a foreign nation against the interests of the United States. The security procedures in this Protective Order are to insure that persons subject to this Order will never divulge the classified information disclosed to them to anyone who is not authorized to receive it, without prior written authorization from the original classification authority and in conformity with these procedures.

e. Persons subject to this Order are admonished that they are obligated by law and regulation not to disclose any classified national security information in an unauthorized fashion.

f. Persons subject to this Order are admonished that any breach of the security procedures in this Order may result in the termination of their access to classified information. In addition, they are admonished that any unauthorized disclosure or possession of classified information may constitute violations of United States criminal laws, including but not limited to, the provisions of Sections 641, 793, 794, 798 and 952, Title 18,

FOR OFFICIAL USE ONLY

United States Code, and Sections 421 and 783(b), Title 50, United States Code. In addition, for all persons who are attorneys, violations of this Order will be filed with their State Bar Association.

3. Prior to any Article 32 or court-martial proceeding, a Court Security Officer will be appointed in writing and served with a copy of this protective order.

4. Personnel Security Investigations and Clearances

a. This case may involve classified national security information or documents, the storage, handling and control of which requires special security precautions mandated by statute, executive orders and regulations, and access to which requires a security clearance.

b. Pursuant to reference (c), the Convening Authority was advised that all detailed trial and defense counsel have executed non-disclosure agreements (SF 312) and have the requisite security clearances to have access to material classified Secret and below. Once a party obtains a security clearance that party is to have unfettered access to that classified information which is relevant and necessary to prepare for this case, subject to the requirement in paragraph 4.e, below.

c. As a condition of receiving classified information, any retained civilian defense counsel will agree to the conditions specified herein and execute all necessary forms so that the Department of the Navy may complete the necessary personnel security investigation to make a determination whether to grant a Access Authorization. Any retained civilian defense counsel will also sign the statement in paragraph 4.d. Upon the execution and filing of the statements set forth in paragraph 4.d by any retained civilian defense counsel requiring access to classified information and upon that retained civilian defense counsel's completion and submission of any necessary personnel security investigation forms, the government shall undertake, as expeditiously as possible, the required inquiries to ascertain the retained civilian defense counsel's eligibility for access to classified information.

d. There are three conditions precedent to obtaining access to the classified information at issue in this case. A) All individuals, other than the law enforcement agents, trial and military defense counsels and personnel of the original classification authority, can obtain access only after having provided the necessary information required for, and having been granted, a security clearance or Access Authorization by the Department of the Navy; B) Any retained civilian defense counsel shall also sign a standard form nondisclosure agreement (SF 312) as a condition of access to classified information; and (C) Each person, other than the Department of Navy employees named herein and personnel of the original classification authority, before being granted access to classified information must also sign a sworn statement which states:

FOR OFFICIAL USE ONLY

Any retained civilian defense counsel's Memorandum of Understanding shall include a statement expressing his understanding that the failure to abide by the terms of this Protective Order will result in a report to his State Bar Association.

e. In addition to the Memorandum of Understanding contained in paragraph 4.d, any person who as a result of this case gains access to information contained in any Department of the Navy Special Access Program, as that term is defined in Executive Order 12958, or to Sensitive Compartmented Information (SCI), shall sign any nondisclosure agreement which is specific to that Special Access Program or to that Sensitive Compartmented Information.

f. All other requests for clearances for access to classified information in this case for persons not named in this Order or for clearances to a higher level of classification, shall be made to the Court Security Officer, who, after notifying trial counsel, shall promptly process the requested security clearance applications for them. If trial counsel objects to such requests for access or for clearances to a higher level of classification, the matter will be brought to the attention of the Convening Authority for resolution.

g. Before any person subject to this Protective Order, other than law enforcement agents, trial counsel and military defense counsel and personnel of the original classification authority who have appropriate level security clearances, receives access to any classified information, that person shall be served with a copy of these Procedures and shall execute the written agreement set for in paragraph 4.d.

h. The security procedures contained in this Order shall apply to any civilian defense counsel retained by the accused, and to any other persons who may later receive classified information from the U.S. Department of the Navy in connection with this case.

5. Preparation and Filing of Mil. R. Evid. 505(h) Notice and other Pleadings.

a. The accused and defense counsel shall prepare forthwith, but in no event later than ____ business days before any court and/or Article 32 proceeding, a brief written description of any information known or believed to be classified, which the accused reasonably expects to disclose or cause to be disclosed in any pre-trial motion or proceeding, or at trial of this case (hereinafter referred to as "the Accused's Disclosure Notice"), as required under Mil. R. Evid. 505(h).

b. For the purposes of preparing the Accused's Disclosure Notice, defense counsel, subject to compliance with the applicable provisions of this Order, shall be allowed to discuss, communicate and receive information from the accused concerning any matter believed by the accused to contain, involve or relate to classified information, and believed by the accused to relate to this case. Any retained civilian defense counsel shall also comply with the provisions of this Order before having access to said classified information.

FOR OFFICIAL USE ONLY

c. The accused, through counsel, shall advise the Convening Authority, and the trial counsel when he has prepared or possesses the Accused's Disclosure Notice or any other material which the accused or counsel believes contains classified information, which he intends to offer at the Article 32 investigation, file in court or use in court, and shall then deliver to the Court Security Officer directly, or by means of a courier designated by the Court Security Officer, the Accused's Disclosure Notice and all copies thereof, or any other pleadings. All associated materials and other documents of any kind or description containing any of the information in the Accused's Disclosure Notice shall be stored under conditions prescribed by the Court Security Officer.

d. Until further Order of this Court, the Accused's Disclosure Notice and all other written pleadings shall be delivered to the Court Security Officer. The time of delivery to the Court Security Officer shall be considered the date of filing. The Court Security Officer shall promptly review such pleadings and shall determine with the assistance and consultation of the attorney for the government and any personnel from any agency necessary to make such determination, whether any of the material submitted is classified, and the level of classification of any such material. If the pleading or information does not contain any classified information, the Court Security Officer shall forward it immediately to the Article 32 Investigating Officer or Court for routine filing. If the pleading does contain classified information, or information which might lead to or cause the disclosure of classified information, the Court Security Officer shall, after consultation with the trial counsel and original classification authority:

- (1) mark it appropriately
- (2) give a marked copy to the trial counsel;
- (3) have the original filed under seal and stored under appropriate security conditions.

In this way, any documents containing classified information (or information believed to be classified and which must undergo a classification determination) which are filed shall be sealed by order of the Convening Authority.

6. Handling and Protection of Classified Information

a. Defense Counsel shall seek guidance from the Court Security Officer with regard to appropriate storage and handling of classified information.

b. Classified information and documents related to this case can be stored by the Security Manager at Naval Legal Service Office, _____. If the Security Manager at Naval Legal Service Office, _____ takes custody of classified information and documents related to this case, the Court Security Officer or Trial Counsel shall ensure that the appropriate storage facilities and procedures for such material are being employed. The Accused's Disclosure Notice and associated materials prepared by the defense shall be maintained by the Court Security Officer in a separate sealed envelope to which only the defense counsel shall have access.

c. If the defense requires custody of defense generated documents, appropriate physical security protection (which is approved by the Court Security Officer as meeting the required standards) shall be provided for any materials prepared or compiled by them, or by any person in relation to the preparation of the accused's defense or submissions under Mil. R. Evid. 505. The

FOR OFFICIAL USE ONLY

materials and documents (defined above) requiring physical security include, without limitation, any notes, carbon papers, letters, photographs, drafts, discarded drafts, memoranda, typewriter ribbons, computer diskette, magnetic recording, or other documents or any kind or description.

d. Classified national security documents and information, or information believed to be classified, shall only be discussed in an area approved by the Court Security Officer, and in which persons not authorized to possess such information cannot overhear such discussions.

e. No one shall discuss any of the classified information over any standard commercial telephone instrument or any inter-office communication system, or in the presence of any person who is not authorized to possess such information.

f. Written materials prepared for this case by the accused or defense counsel shall be transcribed, recorded, typed, duplicated, copied or prepared only by persons who have received access to classified information pursuant to the security procedures contained in this Order.

g. All mechanical devices of any kind used in the preparation or transmission of classified information in this case may be used only with the approval of the Court Security Officer and in accordance with instructions he shall issue.

h. Upon reasonable advance notice to the Convening Authority or the Court Security Officer, defense counsel shall be given access during normal business hours and at other times on reasonable request, to classified national security documents which the government is required to make available to defense counsel but elects to keep in its possession. Persons permitted to inspect classified national security documents by this Order may make written notes of the documents and their contents. Notes of any classified portions of these documents, however, shall not be disseminated or disclosed in any manner or form to any person not subject to this Order. Such notes will be secured in accordance with the terms of this Order. Persons permitted to have access to the documents will be allowed to view their notes within an area designated by the Court Security Officer. No person permitted to inspect classified national security documents by this Order, including defense counsel, shall copy or reproduce any part of said documents or their contents in any manner or form, except as provided by the Court Security Officer, after he has consulted with the trial counsel and the Court.

i. Without prior authorization of the Department of the Navy, there shall be no disclosure to anyone not named in this Order by persons who may later receive a security clearance or approval from the Department of the Navy in connection with this case (except to or from government employees acting in the course of their official duties) of any classified national security information or national security document (or information contained therein) until such time, if ever, that such documents or information are admitted into evidence in an open session of court in this case.

FOR OFFICIAL USE ONLY

- j. The defense shall not disclose the contents of any classified documents or information to any person not named herein, except the members of this court-martial, if any, and the judge advocates for the United States identified by the Court Security Officer as having the appropriate clearances, and a need to know.
 - k. All persons given access to classified information pursuant to this Order are advised that all information to which they obtain access by the Order is now and will forever remain the property of the United States Government. They shall return all materials which may have come into their possession, or for which they are responsible because of such access, upon demand by the Court Security Officer.
 - l. A copy of this Order shall issue forthwith to defense counsel named herein, with a further order that said defense counsel advise the accused named herein of the contents of this Order, and furnish him a copy. The accused, through defense counsel, shall forthwith sign the statements set forth in paragraph 4.d of this Order, and counsel shall forthwith file an original with the Convening Authority and provide an original each to the Court Security Officer and the trial counsel. The signing and filing of this statement by the accused is a condition precedent to the disclosure of any classified information to the accused.
7. Nothing contained in these procedures shall be construed as a waiver of any right of the accused.

/S/

MEMORANDUM OF UNDERSTANDING

1. I, _____, understand that I may be the recipient of information and intelligence that concerns the present and future security of the United States and that belongs to the United States. This information and intelligence, together with the methods of collecting and handling it, are classified according to security standards set by the U.S. Government. I have read and understand the provisions of the espionage laws (sections 793, 794, and 798 of Title 18, United States Code) concerning the disclosure of information relating to the national defense and the provisions of the Intelligence Identities Protection Act (section 421 of Title 50, United States Code) and I am familiar with the penalties for the violation thereof. I have also read and understand the provisions of SECNAV Instruction 5510.36, concerning safeguarding, disseminating, transmitting and transporting, storage and destruction, and loss or compromise of classified information.
2. I have been advised that the unauthorized disclosure, unauthorized retention, and negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation or enemy of the United States. I hereby agree that I will never divulge classified information to anyone unless (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive classified information; or (b) I have been given prior written notice of the authorization of the United States Government Department or Agency responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted; or (c) as ordered by the Convening Authority. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose the information, except as provided in (a), (b) or (c), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information. I have been advised and understand that any breach of this agreement may result in the termination of any access to classified information. I recognize that this agreement including its provision for the termination of access to classified information does not constitute a waiver of the United States' right to prosecute me for any statutory violation.
3. I understand that this agreement will remain binding on me after the conclusion of proceedings in _____.
4. I have received, read and understand the Protective Order entered by the Convening Authority on _____ 2004, in the case of _____, relating to classified information, and I agree to comply with the provisions thereof.
5. I understand that noncompliance with this Order will be reported to any State Bar where I am admitted to practice law.

Signature Date

Witnessed, sworn and subscribed to before me this ____ day of _____, 2004

Signature of Witness

CHAPTER 7

Classification Reviews

Classification reviews represent a critical litigation support tool in a military justice case involving classified information. A classification review provides an official determination on the classification level of the material at issue, both for evidentiary reasons and for procedural reasons, as explained below.

A. Definition. “Classification Review” is a term of art most commonly used by the Navy and Marine Corps in the information security context. When the Department of the Navy is the Original Classification Authority (OCA), the authority to conduct a classification review and its procedures are contained in SECNAV M-5510.36, Chapter 12, “Loss or Compromise of Classified Information.” Army and Air Force regulations apply a similar concept in their information security programs.¹ Terminology differences exist among the Armed Services. This Primer adopts “classification review” as understood in the Navy and Marine Corps as the term that describes the process introduced in this chapter.

1. Distinction. The “classification review” must be distinguished from other analytical processes such as the “damage assessment” and “declassification review.” It is neither a damage assessment nor a declassification review. The failure to properly understand and distinguish this difference frequently results in confusion, lost time, delay, and faulty products. “Classification review” was once defined and distinguished from these other processes in DODI 5240.11, “Damage Assessments” (Issued on 23 December 1991, and cancelled on 1 June 2005). While this instruction was cancelled without replacement, it remains informative on this issue, and is consistent with current language found in SECNAVINST 5510.36.² Enclosure (1) of DODI 5240.11 defined a classification review as “[a] formal finding that information subjected to loss or compromise is (was) legally classified at the time of compromise. The review usually includes an assessment of the probability (risk) of damage to national security resulting from disclosure of this information or material to an unauthorized person. A classification review is obtained in all national security cases and is necessary when a determination must be made on the use of classified information as trial evidence under the Classified Information Procedures Act or Military Rule of Evidence 505.” While originally required only in “national security cases,” classification reviews should be obtained in *all* cases involving classified information.

(a) **Damage Assessment.** DODI 5240.11 defined “damage assessment” as a “multidisciplinary analysis to determine the effect of a compromise of classified information on the national security. [It is] normally a long-term, *post*-prosecution effort to determine in great detail the practical effects of an

¹ AR 380-5, § 10-5: “reevaluation and damage assessment”; AFI31-401, §9.10: “damage assessment”

² SECNAV M-5510.36, paragraph 12-16 describes classification reviews which include:

- a. [v]erification of the current security classification level and its duration.
- b. [t]he security classification level of the information when it was subjected to compromise.
- c. [w]hether further review is required by another DON or DOD activity, or Executive Branch agency.
- d. [a] general description of the impact on the affected operations.

espionage-related compromise.” (Emphasis added) A classification review, in contrast, is performed *in support of* litigation.

(b) Declassification Review. Executive Order 12958 § 6.1(k) defines “declassification” as “the authorized change in the status of information from classified information to unclassified information.” Executive Order 12958 § 6.1(w) defines “mandatory declassification review” as “the review for declassification of classified information in response to a request for declassification” in accordance with Executive Order 12958 § 3.5. A “declassification review” is an administrative process that examines whether classified information can be declassified as a result of a request for declassification. Requests for mandatory declassification reviews are similar to Freedom of Information Act requests and are commonly submitted by researchers seeking classified information (often historical) for their books and projects. A classification review, in contrast, does not request declassification of the information. Instead, it asks the reviewer to verify and re-evaluate the classification level of the information.

2. Documentation of the Classification Review. The result of the classification review should be documented in an affidavit. The affidavit is most often prepared by a subject matter expert that works in the agency that originally classified the information. If the OCA does not prepare the affidavit, then the OCA certifies the result of the classification review affidavit by letter. The OCA agency must complete the classification review because only the OCA has first-hand knowledge as to why the information was classified and the expected harm to national defense resulting from its disclosure. A derivative classifier does not have such personal knowledge and would only be stating hearsay if he completed an affidavit that essentially stated “the document is classified because Agency X classified it as SECRET.” In order to assert the classified information privilege and comply with M.R.E. 505(i)(3), the affidavit “shall demonstrate that disclosure of the information reasonably could be expected to cause damage to the national security in the degree required to warrant classification under the applicable executive order, statute, or regulation.” Without a proper classification review, counsel and the court have no assurances that the information is correctly classified and properly marked. Furthermore, a classification review must be completed before any material can be offered as “evidence” in any proceeding. Any classified information offered without having undergone a classification review is subject to challenge by the opposing party. Executive Order. 12958 § 1.8, Classification Challenges, details the process a party must follow if the party believes, in good faith, that the documents are improperly classified.

B. Components of a Classification Review Package.

1. Affidavit. Generally the classification review affidavit is unclassified, although it may have classified attachments, such as the classified information itself. It is usually drafted by a subject matter expert on the OCA’s staff, although it may be drafted by the OCA himself in some cases. A sample classification review affidavit is provided at Appendix 7-A. Customarily, the affidavit has the following sections:

(a) Background. The drafter states his identity, employment, position and experience in the field.

(b) General Information. The drafter identifies the case name and announces the references used to assist in their analysis. It also outlines the general provisions of classified information, demonstrating compliance with Executive Order 12958 § 1.4.

(c) Classification of the Material Reviewed. This key section states whether the information is or was classified at the time of the loss or compromise, confirms the current classification, and determines whether the protections of M.R.E. 505 need to be invoked.

(d) Damage to National Security. The drafter indicates the level of damage that would be caused to national security if the information was disclosed and should include more detail as to why it would be harmful for unauthorized persons to gain access to the information.

2. OCA Cover letter. If the affidavit is not prepared personally by the OCA, the OCA will sign a cover letter. The OCA letter addresses whether permission to access the information and use the information in the legal proceedings is authorized or not. In the cover letter, the OCA will also endorse the subject matter expert's classification review findings. The OCA may also add conditions of access and use, such as limiting use to a redacted version. In most of the national-level intelligence agencies, there are many OCAs within each agency. A sample cover letter is provided at Appendix 7-B.

3. M.R.E. 505 Letter by the "Head of Agency". The OCA cover letter and affidavit are then forwarded to the Head of Agency or Military Department because only he can claim the classified information privilege under M.R.E. 505. The classified information at issue is usually included as part of the package because the Head of Agency or Military Department can only claim the privilege "after actual personal consideration by that officer." *United States v. Reynolds*, 345 U.S. 1, 8 (1953); see also *id.* at n.20. The Head of Agency or Military Department letter typically authorizes the trial counsel to invoke the privilege on the Agency or Military Department's behalf. The Secretaries of the Navy, Army, and Air Force are the head of their respective military departments. The Secretary of Defense is the head of military department for Department of Defense information that did not originate within one of the services, e.g., Combatant Commanders and the Joint Chiefs of Staff.



Practice Pointer: Although the National Security Agency (NSA) is a DoD member of the Intelligence Community, the Secretary of Defense is not the Head of Agency for NSA. The Director, NSA is the Head of Agency and asserts the classified information privilege on behalf of NSA.

C. Role of the Affidavit at Trial. The classification review package has three distinct purposes. Procedurally, it is required under M.R.E. 505 to assert the privilege and prevent the use of classified information at trial. The classification review also demonstrates that information is properly classified. This allows the government the opportunity to argue for a closed session during *Grunden* hearings. Finally, the classification review addresses an element of one or more charged offense because it sets forth the classification level of the information at the time of the offense³ and describes the harm to national security⁴ that would result from compromise of the information. Thus, the classification review is a critical part of pretrial proceedings and the trial itself.

1. Privilege & Procedure. M.R.E. 505 (c) is structured to protect *currently* classified information, regardless of its previous status. It states that the Head of Agency may claim the classified information privilege over information upon “a finding that the information *is* properly classified and that disclosure *would be* detrimental to the national security.” (Emphasis added.) When the information is to be withheld from the accused, the Head of Agency relies upon the classification review affidavit to claim the privilege. The procedure for reviewing the privilege assertion is contained in M.R.E. 505(i). The classification review satisfies the predicate showing in M.R.E. 505 (i)(3) to “demonstrate that disclosure of the information reasonably could be expected to cause damage to the national security in the degree required to warrant classification under the applicable executive order, statute, or regulation.” The M.R.E. 505(i) procedure is also used to test the sufficiency of any proposed summary, substitute, or alternative to the actual classified information. In that instance, the classification review identifies the classified information that the summary, substitute, or alternative replaces.

2. Closure of the Courtroom. The classification review is also the usual method of demonstrating the “overriding interest” that will be prejudiced if the proceedings remain open. The classification review describes the harm to national security that would result from disclosure to the public. The classification review is not the only method of demonstrating this interest during the closure proceeding. The overriding interest may also be demonstrated by testimony, or, under R.C.M. 806, the military judge may make the finding based on his own review of the information, even without a classification review. This is most likely to occur when a large amount of classified information has been turned over to the defense team and the parties are litigating the relevance of some of that information based on M.R.E. 401 prior to the completion, or even the initiation, of a classification review.

3. Evidence on an Element. As noted in the DoDI 5240.11 definition of “classification review” and in SECNAVINST 5510.36, a classification review determines whether a piece of classified information was properly classified *at the time of compromise*. The classification review examines the classification level of the information at the time of

³ The fact that the information was classified is particularly important to Article 92, orders violation offenses that are predicated on the Information Security Program Manual, SECNAV M-5510.36, Chapter 10.

⁴ Charges under 18 U.S.C. § 793 are not based on the classification of the material, but rather turn upon whether the information relates to “national defense.”

the offense and helps establish the evidentiary requirements of certain offenses. A properly prepared classification review will provide notice that at least some of the elements of the offenses may be easily proven. Although the classification review is likely to be an appellate exhibit because of pretrial motions, it may also be offered on the merits as proof of that element. However, introducing the classification review is vulnerable to a hearsay objection. Counsel must be prepared to introduce witness testimony to actually prove the element of the offense at trial. If no element of an offense requires classified information, the classification review may still be relevant and admitted into evidence. For example, Article 106a, Espionage (non-capital), only requires that the communicated information “relate to the national defense.”⁵ The information does not have to be classified, although its classified markings could have probative value in proving that the accused has intent or reason to believe that the disclosure would injure the U.S. or provide an advantage to a foreign nation. Additionally, the classified status of the information will have a bearing on the amount of damage caused to the national defense and the United States by the loss or compromise of the information. Further discussion on potential charges and sample specifications is contained in Chapter 8 and Appendix 8-A, respectively. Appendix 11-B contains a breakdown of the elements of 18 U.S.C. § 793.



Practice Pointer: Testimonial Evidence. When a classification review is completed on a classified document, testimony based on the information contained in the document is also covered by the classification review. Testimony about classified information that has not been the subject of a previous classification review will need a separate classification review. The proponent of the testimony must coordinate with Code 17 and the OCA to obtain an affidavit that will cover the expected testimony. Otherwise the court will not have the necessary tool to close the courtroom to the public in accordance with R.C.M. 806(b)(2).

BOTTOM LINE: ALL classified information to be used at trial needs to be reviewed! This requires a great deal of forethought and planning on the part of each of the parties.

D. Procedures for Requesting a Classification Review. CNO (N09N2) is the Department of the Navy office officially tasked with initiating a classification review in cases of loss or compromise of classified information.⁶ As a practical matter, CNO (N09N2) coordinates classification reviews of all material originated within the Department of the Navy. Code 17 coordinates classification reviews with most non-Navy OCAs, especially the national level members of the Intelligence Community (IC). The convening authority and government counsel must ensure that classification reviews are initiated, either by CNO (N09N2) or Code 17, as early

⁵ Also see *U.S. v. Richardson*, 33 MJ 127 (CMA 1991).

⁶ Army and Air Force do not designate any particular organization with this role. Instead, AR 380-5 and AFI31-401 state that the OCA will conduct their review upon notification of a loss or compromise of classified information. None of the Service regulations address the situation of a non-loss/compromise case where classified evidence will be necessary in a court proceeding. However, as a matter of policy and practice, Code 17 has adopted the same procedures for all cases involving classified information, not just loss/compromise cases.

as possible in the court-martial case. For more information on CNO (N09N2), refer to its website at www.navysecurity.navy.mil.

All potentially relevant documents must be sent to the experts with cognizance over the classified information in those documents. Classified documents containing information belonging to more than one OCA, as often occurs in derivatively classified documents, must be reviewed by each of those OCAs. It is the responsibility of the trial counsel to receive the results of those multiple classification reviews and ensure that they are consistent with each other. The analysis of evidence must occur before charges are brought under the UCMJ and the classification reviews should occur before the Article 32 hearing and other court-martial proceedings. It is recommended that classification reviews occur before copies of classified or potentially classified documents are provided to the accused or defense counsel. However, given the length of time to conduct such reviews, the pressure to move cases, and the pressure to provide full and complete discovery as early as possible, OCAs often do not complete all required classification reviews prior to discovery. At a minimum, trial counsel need to ensure that they have the OCA's permission to turn over non-DoD information in discovery to the defense team and all counsel have the appropriate clearances to view the information. Code 17 can prepare and coordinate documents for the Secretary of the Navy, or any other Head of Agency or Military Department, to assert the M.R.E. 505 claim of privilege.

E. Speedy Trial Issues. Historically, classification reviews take a great deal of time to complete, especially when lengthy documents involving multiple agencies are involved. Because classification reviews take so much time, it is recommended that convening authorities do not prefer charges until after the majority of classification reviews have been completed. Convening authorities should carefully examine the need for pretrial confinement in classified information cases, given the unusual complexity of investigations involving classified information and the length of time for classification reviews. The National Security Case Commission, in its review of the *King* case, even went so far as to suggest that convening authorities consider removing an accused from confinement in order to relieve speedy trial pressure. Due diligence in securing classification reviews is required in all cases, but especially in those involving pretrial confinement. Trial counsel should request excludable delay from the convening authority, citing and documenting the numerous reasons that apply in these cases (e.g., further investigation, obtaining security clearances, completion of classification reviews). In the *Weinmann* case, trial counsel did not request a blanket authorization for delay, but rather submitted excludable delay requests every 30 days to the convening authority, providing updates each time on the status of all the issues justifying the request for delay. By the time of the guilty plea, more than six months after Weinmann's arrest, not a single day had elapsed from the 120-day clock.



Practice Pointer: Electronic media, such as CDs and thumb drives, may contain hundreds or even thousands of documents requiring forensic computer analysis by NCIS. Trial counsel and staff judge advocates should ensure that classified computer media are fast-tracked through the NCIS computer forensic process. When necessary, outside agencies with information at issue may be able to provide technical assistance. Code 17 can facilitate such requests through the appropriate agency counsel.

APPENDIX 7-A

Sample Classification Review Affidavit

Declaration

I, LCDR _____, USN, declare and state:

BACKGROUND

I am a Naval officer with ____ years of experience. My current position is Anti-Submarine Warfare (ASW) Sensors Requirements Officer in the Office of the Chief of Naval Operations (N780) which office is responsible for all matters pertaining to Maritime Surveillance policy. I report to _____, Head, Aviation Plans and Requirements Division. I have held my current position for ____ years, and have over ____ years of experience in Maritime Surveillance, ASW operations as a pilot, ASW Operator, staff officer.

PURPOSE OF DECLARATION

This declaration is submitted in the matter of United States v. _____ to demonstrate, to the best of my knowledge and belief, that disclosure of the information identified below reasonably could be expected to cause damage, serious damage or exceptionally grave damage to the national security of the United States. In making the following statement regarding the classified information in this case, I rely on my personal knowledge and experience, **Department of the Navy Security Classification Guides – OPNAVINST C5513.2B, Air Warfare Programs and S5513.5B, Undersea Warfare Programs**, and additional information available to me in my official capacity.

I have deliberately structured this declaration in an unclassified form to facilitate its handling and use during any judicial proceeding.

DESIGNATION OF INFORMATION

Information which requires protection in the interest of national security of the United States is designated CLASSIFIED NATIONAL SECURITY INFORMATION per Executive Order 12958 signed by President Clinton on April 20, 1995, as amended by President George W. Bush on March 25, 2003. Information is classified in levels commensurate with the assessment that unauthorized disclosure could cause the following expected damage to national security:

- a. Top Secret information – exceptionally grave damage
- b. Secret information – serious damage
- c. Confidential information – damage

Unclassified information does not require a security clearance for access, but nonetheless may be of a sensitive nature.

FOR OFFICIAL USE ONLY

PROTECTION OF INFORMATION

Within the Department of Defense, classified information is handled in accordance with the Information and Personnel Security Program Directives, 5200.1-R and 5200.2-R. Classified information should be handled and examined only under such conditions as are adequate to prevent unauthorized persons from gaining access. Classified material may not be removed from designated work areas, except in the performance of official duties and under special conditions which provide protection for the classified material.

CLASSIFICATION DETERMINATION

I have reviewed the material related to this case, which was provided by [Name] at [Organization]. The item in question is an official message from Commander Task Group (CTG) 12.0; subject: "Anti-Submarine Warfare Exercise (ASWEX) 96-2 Post Prosecution Report." The message is classified SECRET. The message was appropriately classified SECRET at the time it was generated, and at no time has it been declassified. **It is currently and properly classified SECRET.** It describes the ASWEX including objectives, forces involved, times, locations, environmental data, tactics employed, the effectiveness of those tactics, and lessons learned.

IMPACT ON NATIONAL SECURITY IF INFORMATION RELEASED

Unauthorized disclosure of the classified material specified above would:

- a. Impair U.S. Anti-Submarine Warfare (ASW) effectiveness -. In the Navy's mission of power projection, ASW is a core naval capability. Access to U.S. ASW tactics and their effectiveness will enable potential adversaries to develop their own **"counter"** taking maximum advantage of our relative weaknesses.
- b. Increase U.S. submarine vulnerability to hostile ASW forces. Access to environmental data tactics, exercise information, and lessons learned will assist potential adversaries in developing their own ASW capabilities, placing U.S. forces at risk.

Pursuant to 28 U.S.C. 1746, I declare under penalty of perjury that the information provided herein is true and correct to the best of my knowledge.

LCDR USN
OPNAV N78
ASW Sensors Requirements Officer

Executed this ____ day of _____ 2006.

FOR OFFICIAL USE ONLY

APPENDIX 7-B

Sample OCA Cover Letter

SECRET (UNCLASSIFIED upon removal of Enclosure (2))

From: Original Classification Authority

To: Convening Authority

Subj: CLASSIFICATION REVIEW ICO UNITED STATES VS. PO2 NAME, SSN, USN

Ref: (a) Your ltr 5510 Ser x of 14 Oct 04, w/o encl

(b) Military Rule of Evidence 505, Manual for Courts-Martial, 2005

Encl: (1) Affidavit of LCDR X of 14 Oct 04

(2) Classified document in question

1. In response to reference (a), enclosure (1) is forwarded to you. As Commander, Naval Command, I am an Original Classification Authority for information up to and including SECRET. The information in enclosure (2), the subject of the classification review, is within my responsibility. I have reviewed enclosure (1) and I concur with LCDR X's assessment that enclosure (2) is properly classified and disclosure would be detrimental to the national security of the United States.

2. I hereby request that the Secretary of the Navy authorize the trial counsels in the subject case to assert the classified information privilege under reference (b).

3. Additionally, personnel involved in the subject proceedings, including civilian defense counsel, may access the information if the Convening Authority or Military Judge determines that they have a need-to-know and have the appropriate security clearance.

4. The point of contact in this matter is LCDR X at xxx-xxx-xxxx.

OCA

7-B-1

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

This page intentionally left blank

7-B-2

FOR OFFICIAL USE ONLY

Chapter 8

Charges in Classified Information and National Security Cases

As in any court-martial, how the charges are drafted in classified information cases affects the shape of the case from discovery through trial, whether contested or by plea. There are a number of considerations that need to be taken into account prior to drafting charges in any case involving classified information. Most importantly, the authority to use classified information as evidence at trial. Other concerns are the amount and classification level of the information, as well as issues that arise due to the presence of classified information on electronic media. Those considerations are discussed in section A. Sections B and C discuss the specific non-capital and capital offenses that are most commonly charged in cases involving classified information, including those federal offenses that are charged under Clause 3 of Article 134, UCMJ (Crimes and Offenses Not Capital).

A. Charging Considerations.

1. Permission to Use the Classified Information. The most important question to be considered at the early stage of any classified information court-martial is what classified information the government will be able to use as evidence in the case. It should NOT be assumed that simply because the accused is alleged to have committed a crime, even the crime of espionage, that the classified information will be available for use at trial. This is especially true for information that originates outside the Department of Defense. The intelligence community's first priority is protection of its sources and methods, not prosecution. This colors their approach to these cases. The presence of civilian counsel representing the accused heightens these concerns. Members of the intelligence community, and the National Security Agency (NSA) in particular, have been known to refuse to allow their information to be turned over in discovery, much less used at trial. Alternatively, it is not uncommon for an agency such as NSA to place limits on the material that may be used, such as only allowing Secret or non-Sensitive Compartmented Information to be used.

It is important for the staff judge advocate to develop a full understanding of the quantity and quality of classified information as early as possible. To that end, NCIS should complete all forensic examinations as soon as possible. It is critical that trial counsel review all potential evidence prior to drafting charges.¹ The charges should not be drafted until counsel has a full and complete understanding

¹ This is a lesson learned from the King case, where trial counsel was not cleared to review all of the evidence prior to the preferral of charges. The fact that Petty Officer King was in pre-trial confinement drove the sense of urgency behind preferring charges against him so early in the investigation.

of what evidence will be available² and what restrictions, if any, the intelligence community places on the use of the classified information as evidence.

2. Amount of Classified Information. The amount of classified material present is an important consideration in any case because large amount of classified material require more classification reviews. It is possible to write a broadly worded charge that implicates all of the classified information, but then pick only certain documents to use as evidence at trial and just have those documents undergo a classification review. In such a case, the defense will often ask for a bill of particulars because the broadly worded charge does not provide sufficient detail as to what actual information was lost, mishandled, or compromised. Even if the government cherry picks particular documents to use as evidence, some or all of the remaining documents may still be discoverable. After all, the defense counsel has the obligation to test any characterization that the government makes about the remaining documents or about the overall group of documents. In cases involving large amounts of classified information, especially when the Original Classification Authority (OCA) has placed use restrictions on some of the information, trial counsel should consider listing specific classified documents in the specification in order to minimize potential discovery and evidence necessary for the trial. Therefore, everything not listed in the specification is not relevant to the case and effectively “fenced off” from discovery.³ Such a charging strategy can assist any use limits imposed by OCAs and address and drastically limit the number of classification reviews required. It also provides for a more focused case, however, the full scope of the accused’s misconduct may be obscured from the finder of fact.

3. Classification Level. The classification level of the material in the case needs to be considered prior to drafting charges. The higher the classification level, or if there is Sensitive Compartmented Information or Special Access Program material present in the case, the more complicated the case becomes, both from an evidentiary and logistical standpoint. Both types of information can only be discussed in a Sensitive Compartmented Information Facility (SCIF), which means that all closed pre-trial and trial sessions would have to be held in such a location. Other extra security precautions immeasurably complicates the case. This is especially true in mishandling cases where there is no allegation of espionage or willful compromise. Serious consideration should be given to charging in such a way as to NOT implicate these two types of information. This can be done by enumerating specific documents in the specification, as discussed in the last section, or by putting a specific classification level into the specification. For instance, charging the accused with mishandling “information

² The convening authority staff judge advocate and trial counsel need to have the proper clearance to review the evidence in the case and should apply for any required upgrades in clearance level as early in the process as possible.

³ Of course, trial counsel could not then refer in any way to the greater body of classified documents/information. The enumerated documents could not be characterized as being “representative,” or a “sampling” in any way of the entirety of the classified information.

classified at the Secret level” rather than the more generic “classified information.” However, it should be emphasized that charging in such a manner carries a risk if the classification review does not confirm the classification level. This risk can be dramatically reduced by having good, thorough classification reviews completed prior to charging or ensuring that multiple Secret documents are charged and then reviewed. When the evidence in a case does not go above the Secret level, then the more conservative approach is to simply charge loss of “classified information.”

4. Electronic Media. The cases involving the largest quantities of highly classified information are usually cases where the classified information was located on electronic media such as laptop hard drives, CDs, or thumb drives. Electronic media should not be charged in the specification, especially if efforts are being made to fence off amounts or levels of classified information. The electronic media is not the classified information. It is merely the holder of the classified information, much like a file folder of classified information found at someone’s house. It is the classified information inside the folder that is charged, not the folder. Case law and the facts of each case need to be carefully examined to determine whether or not the entire forensic examination is subject to discovery, especially in cases where efforts have been made to limit the scope of the material at issue. In such cases, when a decision is made to provide the entirety of the forensic examination, the titles of the non-relevant documents/files on the electronic media should be carefully screened to ensure that classified subject lines are not mistakenly provided in discovery.

B. Non-Capital Offenses.

1. Article 92 – Failure to Obey Order or Regulation. Article 92 violations are the most commonly charged UCMJ offenses in classified information cases. It is often the only charge available in mishandling cases. Article 92 can also be charged in espionage and willful compromise cases as such conduct also violates the safeguarding and handling regulations.

The applicable regulation is SECNAV M-5510.36, the Department of the Navy Information Security Regulation.⁴ It is important to note that, although the instruction is expressly punitive, most of the affirmative duties are placed on commanding officers. Only a few provisions place affirmative duties on service members generally. The facts of each case need to be carefully evaluated to determine if they constitute a specific violation of SECNAV M-5510.36. Judge advocates should become familiar with provisions in chapters 7 (Safeguarding), 10 (Storage and Destruction), and 12 (Loss or Compromise of Classified Information) as these chapters are the most likely to support an orders violation charge. In Chapter 7, the regulation requires the Commanding Officer to set administrative procedures for controlling the various levels of classified information. Individuals must take care to properly log classified materials,

⁴ Army: AR 380-5; USAF: AFI31-401

conduct end-of-the-day security checks, and take care when discussing classified information. While Chapter 10 places much of the burden on commanding officers to establish proper procedures for the storage and destruction of classified information, be aware of situations involving unauthorized storage at residences or within workspaces by individuals. Chapter 12 places an affirmative burden on individuals to notify their security manager and commanding officer upon discovering a loss or compromise of classified information.

Another option for trial counsel is to charge a violation of the Classified Information Executive Order. Section 4.2(c) of Executive Order (E.O.) 12958 states that classified information may not be removed from official premises without proper authorization. This is a prohibition that applies to everyone, not just COs, and would seem to be specific enough to support a charge of disobedience of a general order. Section 5.7(b) of E. O. 12958 also contains language that simply and clearly prohibits unauthorized disclosures of classified information.

Trial counsel can also use Article 92 to charge a dereliction of duty. The principle is that all service members have a duty to safeguard classified information. This duty is a long-standing custom of the service and is known, or should be known, because it is discussed in several regulations, including SECNAV M-5510.36 and E.O. 12958. In many cases, the service member was indoctrinated upon being granted a clearance and signed a non-disclosure agreement (SF-312) or other form. Copies of the SF-312 are usually available in the service member's service record. SECNAV M-5510.36 can be used to establish certain duties pertaining to classified information. A failure to safeguard information marked as classified would constitute a dereliction of this duty and, depending on the facts, could be charged either as willful or negligent.

2. Article 134 - The General Article. Article 134, clause 3 permits the assimilation of non-capital crimes and offenses under the United States Code that are not otherwise specifically contained in the UCMJ. Article 134's preemption doctrine prohibits the assimilation of offenses specified under the U.S. Code if the conduct is already covered by Articles 80-132 of the UCMJ. There are several federal statutes that prohibit conduct not already covered under standard UCMJ articles. These are frequently charged in national security cases and cases involving classified information. JAGMAN § 0126 lists some of the federal statutes that relate to national security. Sample specifications are provided in Appendix 8-A. Note, however, that 18 U.S.C. § 794 cannot be charged under Article 134 because it is a capital offense.

When charging Article 134 violations, remember that the applicable statute of limitations is Article 43, UCMJ, which provides for a five year period for most violations. If, however, the offense is punishable by death, there is no statute of limitations.

(a) 18 U.S.C. § 793. 18 U.S.C. § 793 is one of the primary federal espionage statutes. Section 793 is titled “Gathering, transmitting, or losing defense information,” and is subdivided into six separate offenses. Each offense carries a maximum sentence of 10 years confinement. Section 793 does not require any intent or attempt to give the information to a foreign entity, unlike Article 106a, discussed below in section C. Section 793 is not preempted by Article 134 because it is, in effect, a lesser offense of Article 106a, and is aimed at preventing the possession of national defense information by any person who is not authorized to possess it, not just foreigners. Just as with Article 106a, Section 793 does not specifically require that the information be classified. It only requires that the information be related to the national defense. Each subsection differs slightly with respect to the manner in which the accused comes into possession of the information and other minor details. See Appendix 11-B for a detailed breakdown of the elements of the various subsections of 18 U.S.C. § 793.

(b) 18 U.S.C. § 1924. Section 1924 is titled “Unauthorized removal and retention of classified documents or material.” This section is appropriately charged when the evidence indicates mishandling of classified information, but does not suggest the accused made any attempt or had any intent to give the information to an unauthorized person. It is a misdemeanor and carries a maximum sentence of one year of confinement. This offense, by itself, would not likely be a national security case, because it does not involve a compromise. However, it often is charged in conjunction with other offenses in a national security case. The main focus of section 1924 is to prevent unauthorized handling of classified information by persons who might otherwise be authorized to possess the information. In contrast, the focus of section 793 is to prevent unauthorized people from possessing classified information. Section 1924 also differs from section 793 in that it does specifically require that the information be classified.

(c) Other Federal Statutes. Titles 18, 42, and 50 describe several additional offenses which may be applicable in cases involving classified information. Within title 18, counsel should consider section 792 (harboring or concealing persons), section 795 (photographing defense installations), section 798 (disclosure of classified information), and section 1001 (false statements when the falsification or concealment concerns any actual, prospective, or attempted commission of a crime against national security). In addition, sections 2151 through 2156 of title 18 (chapter 105) describe offenses of sabotage, and sections 2331-2339B of title 18 (chapter 113B) describe offenses of terrorism. Other title 18 offenses include sections 2381 (treason), 2382 (misprision of treason), 2383 (rebellion or insurrection), 2384 (seditious conspiracy), 2385 (advocating overthrow of Government), 2388 (activities affecting armed forces during war), 2389

(recruiting for service against the United States), and 2390 (enlistment to serve against the United States).

Title 42 and title 50 describe offenses that may be chargeable in national security cases for specific categories of evidence. If the case involves restricted data, counsel should consult title 42. Offenses under title 42 include sections 2272 (violation of specific sections), 2273 (violation of sections generally), 2274 (communication of restricted data), 2275 (receipt of restricted data), 2276 (tampering with restricted data), and 2277 (disclosure of restricted data). If the case involves classified information, counsel should consult title 50. Within title 50, section 783 makes it a crime to communicate classified information, or conspire to do so, to any person whom one knows or has reason to believe to be an agent of a foreign government. 50 U.S.C. § 421, the Intelligence Identities Protection Action prohibits the unauthorized disclosure of information identifying certain U.S. intelligence officers, agents, informants, or sources.

3. Miscellaneous Articles. One should not overlook traditional offenses when drafting a charge sheet involving classified information. Judges and counsel are generally more familiar with traditional UCMJ violations than federally assimilated statutes. There is usually established military case law applicable as well. Furthermore, traditional charges may be less difficult to prove and may not require the use of classified information during the presentation of evidence. Some possible charges include Articles 81 (Conspiracy), 107 (False Official Statement), and 131 (Perjury). Cases involving the taking or removal of classified information from a workplace or command can be charged under Articles 108 (military property) and 121 (larceny) because classified information is property of the United States, according to SECNAV M-5510.36, Section 7-1.

C. Death penalty eligible charges

1. Art 104 – Aiding the enemy (if referred capital). Any person who aids, or attempts to aid, the enemy with arms, ammunition, supplies, money, or other things, is guilty of aiding the enemy. Further, any person who, without proper authority, harbors, protects or gives intelligence to or communicates or corresponds with the enemy, either directly or indirectly, is guilty of this offense. “Enemy” is defined in Part IV, paragraph 23c.(1)(b) of the MCM and includes organized forces of the enemy in the time of war, any hostile body that our forces may be opposing, and includes civilians as well as members of hostile military establishments. For the offense of aiding the enemy, either a court-martial or a military commission may award the death penalty. This is the most applicable of the death penalty offenses to instances of a service member assisting a terrorist organization such as Al Qaeda.

2. Art 106 – Spies (mandatory). Any person, regardless of nationality or status, who, in time of war, is found to be acting clandestinely or under false pretenses

and collecting or attempting to collect certain information, with the intent to convey this information to the enemy, is guilty of this offense. The phrase “time of war” is defined in R.C.M. 103(1) as either a period of war declared by Congress, or the factual determination by the President that the existence of hostilities warrants a finding that a “time of war” exists for purposes of R.C.M. 1004(c)(6) and Parts IV and V of the MCM. The accused shall be tried by general court-martial or military commission and, if convicted under this Article shall be punished by death. There is no lesser-included offense.

3. Art 106a – Espionage (if referred capital). Article 106a was created in 1985 to establish a peacetime espionage offense. Prior to its enactment, espionage and espionage-like acts could only be punished, if committed in a time of war, under Article 106, Spies. Article 106a was modeled after 18 U.S.C. § 794, the Federal Espionage Act. This particular section of the federal code could not be assimilated under Article 134 since it is a capital offense and Article 134 prohibits the assimilation of capital offenses. Congress responded to this deficiency by creating Article 106a. Article 106a may be used to charge an individual, who communicates, delivers or transmits or attempts to communicate, deliver or transmit any “thing” relating to the national defense to an entity or agent of what is best described generically as a “foreign power.” A terrorist organization, such as Al Qaeda, does not fit neatly within the definitions of “entity” contained within the definitions of this section. Trial counsel must prove that the accused acted with intent or with reason to believe that “thing” at issue would be used to the injury of the United States or to the advantage of a foreign nation. “Thing” is a defined term which, in its broadest term, includes “information relating to the national defense,” which parallels the language used in the pertinent sections of Title 18 of the U.S. Code.

Transmission of certain types of information may be punishable by death. Article 106a states that the information warranting a capital charge is anything that directly concerns nuclear weaponry, military spacecraft or satellites, war plans, communications intelligence and or any other major weapons system or major element of defense strategy.

Trial counsel must be able to show the subject did, or did attempt to, transmit, deliver, or communicate, national defense information to a specified entity, such as a foreign government; a faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the U.S.; or a representative, officer, agent, employee, subject, or citizen of such a government, faction, party or force. It is important to note that the information does not have to be classified. It only needs to relate to the national defense. In circumstances where the information is not classified,⁵ the trial counsel must show the accused acted in bad faith, without lawful authority with respect to information that is not

⁵ The Department of Justice, as a matter of policy and practice, does not prosecute cases under 18 U.S.C. §§ 793 and 794 unless the information was, in fact, classified. Code 17 recommends that convening authorities follow DoJ’s lead on this issue.

lawfully accessible to the public, and that the accused did so with the intent or reason to believe that the information would be used to the injury of the U.S., or to the advantage of a foreign nation.

When Article 106a is charged as a capital offense, the court martial must find unanimously and beyond a reasonable doubt one or more of the following aggravating factors: the accused has been convicted of another offense involving espionage or treason for which the sentence of death or imprisonment for life was authorized by statute; the accused knowingly created a grave risk of substantial damage to the national security in the commission of the offense; the accused knowingly created a grave risk of death to another person in the commission of the offense; or any other factor that may be prescribed by the President pursuant to Article 36 of the UCMJ. As already stated, only information which directly concerns nuclear weaponry, military spacecraft or satellites, war plans, communications intelligence and or any other major weapons system or major element of defense strategy, has the potential to satisfy this requirement.

As a final note, *attempted* espionage is not charged under Article 80 like most other attempted crimes under the UCMJ. Attempted espionage is charged under Article 106a. Sample specifications are provided in the Appendix.

4. Aggravating Factors. For the death penalty to be imposed for the foregoing offenses, the members must find, beyond a reasonable doubt, one or more of R.C.M. 1004 aggravating factors are present. While trial counsel should plead the element that makes the charge capital when seeking a capital referral, it is not required to plead the aggravating factors. It is imperative for counsel to be certified for capital litigation before litigating a national security case which has been referred capital.

APPENDIX 8-A

Sample Specifications

§ 793(b):

Specification: In that _____, on active duty, did, on board _____, from on or about _____ to on or about _____, for the purpose of obtaining information respecting the national defense of the United States of America, with intent or reason to believe that the said information was to be used to the injury of the United States or to the advantage of a foreign nation, violate Title 18, United States Code, Section 793(b), by knowingly and willfully [taking photographs or equipment; making a writing; containing information] connected with the national defense.

§ 793(e):

Specification: In that _____, on active duty, did, at or near _____, on or about _____, having unauthorized possession of information relating to the national defense of the United States of America, which information the said _____ had reason to believe could be used to the injury of the United States or to the advantage of a foreign nation, violate Title 18, United States Code, Section 793(e), by knowingly and willfully [communicating; delivering] information relative to the national defense to persons not entitled to receive said information.

§ 793(f):

Specification: In that _____, on active duty, did, at or near _____, on or about _____ violate Title 18, United States Code, Section 793(f), by permitting, through gross negligence, a computer disk containing information pertaining to the national defense, of which he had lawful control, to be removed from its proper place of custody on board _____ and ultimately to his private residence.

§ 795(a):

Specification: In that _____, on active duty, did, on board _____, from on or about _____ to on or about _____, violate Title 18, United States Code, Section 795(a), by unlawfully making photographs of vital naval equipment, relating to the national defense and requiring protection against general dissemination, without first obtaining permission from the naval command concerned and submitting said photographs to such command for censorship or such other action as deemed appropriate.

§ 1924:

FOR OFFICIAL USE ONLY

Specification: In that _____, on active duty, did, on board _____, from on or about _____ to on or about _____, violate Title 18, United States Code, Section 1924, by becoming possessed, by virtue of his office, of materials containing classified information of the United States and knowingly removing such materials without authority and with the intent to retain such materials at an unauthorized location.

ADDITIONAL SAMPLE CHARGES AND SPECIFICATIONS

Charge: Violation of the UCMJ, Article 81

Specification: In that _____, on active duty, did, at or near _____, on or about _____, conspire with Mr. and Mrs. Bin Laden, to commit an offense under the Uniform Code of Military Justice, to wit: espionage, in violation of Article 106a, and in order to effect the object of the conspiracy, _____ did deliver documents titled "Super Secret Squirrel" to Mr. Bin Laden.

Charge: Violation of the UCMJ, Article 92

Specification 1: In that _____, on active duty, did, at or near _____, on or about _____, violate a lawful general regulation, to wit: Paragraph X of SECNAV M-5510.36, by wrongfully disclosing documents titled "Super Secret Squirrel", classified SECRET and TOP SECRET, in his possession and under his control, to persons not authorized to receive said classified information.

Specification 2: In that _____, on active duty, did, at or near _____, on or about _____, violate a lawful general regulation, to wit: Paragraphs X of SECNAV M-5510.36, by wrongfully failing to properly safeguard and store documents titled "Super Secret Squirrel", classified SECRET and TOP SECRET, in his possession, Paragraph X of SECNAV M-5510.36, by wrongfully possessing and storing said classified information at locations not authorized for such storage, and Paragraphs X of SECNAV M-5510.36, dated 23 Jan 01, by wrongfully reproducing SECRET and TOP SECRET classified material without authorization.

Specification 3: In that _____, on active duty, did, at or near _____, on or about _____, having knowledge of his duties concerning the proper handling of classified material, was derelict in the performance of those duties by having, without proper authority, wrongfully and negligently removed classified material, to wit: documents titled "Super Secret Squirrel".

Charge: Violation of the UCMJ, Article 104

Specification: In that _____, on active duty, did, at or near _____, on or about _____, attempt to, without proper authority, knowingly give intelligence to the enemy, by providing documents concerning SIGINT operations.

FOR OFFICIAL USE ONLY

Specification: In that _____, on active duty, did, at or near _____, on or about _____, aid the enemy with maps of Naval installations, by furnishing and delivering said maps to members of al Qaida.

Charge: Violation of the UCMJ, Article 106a

Specification: In that _____, on active duty, did, at or near _____, on or about _____, with the intent or reason to believe that it would be used to the injury of the United States or to the advantage of a foreign nation, attempt to deliver classified SECRET and TOP SECRET information, to wit: documents titled "Super Secret Squirrel", relating to the national defense to a representative of a foreign government.

Charge: Violation of the UCMJ, Article 108

Specification: In that _____, on active duty, did, at or near _____, on or about _____, without proper authority, sell to Mr. Bin Laden, documents titled "Super Secret Squirrel", of some value, military property of the United States.

Charge: Violation of the UCMJ, Article 121

Specification: In that _____, on active duty, did, at or near _____, on or about _____, steal documents classified SECRET, of some value, the military property of the United States.

FOR OFFICIAL USE ONLY

This page intentionally left blank

8-A-4
FOR OFFICIAL USE ONLY

CHAPTER 9

Military Rule of Evidence 505

Unlike the other rules of privilege contained in the Manual for Courts-Martial, Military Rule of Evidence (M.R.E.) 505 is a rule of both privilege and procedure. M.R.E. 505 was created prior to the promulgation of the Rules for Courts-Martial (R.C.M.) in 1984. Thus, extensive procedural requirements were included in M.R.E. 505 to aid with the application of the classified information privilege.¹ The actual text of M.R.E. 505 is drawn from the House version of the Classified Information Procedures Act (CIPA), which was the version that did not make it into law. It is important to understand M.R.E. 505's genesis when considering the intent and operation of various sections of the Rule, especially the procedure under 505(i). Most importantly, the procedural portions are effective and in operation even if there is no assertion of the classified information privilege.

The procedural overlay of M.R.E. 505 is complex and not easy to understand. This is especially true when you consider the interplay of the various sections of M.R.E. 505 with the later-promulgated R. C. M. (especially the provisions on discovery, Article 32 investigations, exculpatory evidence, and courtroom closure). Closing the courtroom is the subject of the next chapter. The remainder of this chapter will explore and explain the operation of the classified information privilege contained in M.R.E. 505 on the discovery and use of classified evidence in Article 32 investigations and trials.

A. Classified Discovery. One of the most important and critical practice differences in cases involving classified information is that trial counsel cannot permit "open file" discovery. The government cannot provide the defense with copies of, or access to, the classified information in the investigative file in order to simply avoid litigation over discovery. In fact, even a cursory reading of M.R.E. 505 reveals that the rule explicitly contemplates extensive litigation over classified information discovery.

Certainly, one of the restrictions on "open file" discovery is the requirement that the recipient have a "need-to-know" the classified information. The fact remains, though, that "need-to-know" is an ill-defined, broad concept under which it is very easy to articulate a need, especially if you are defending a client charged with a serious crime involving that same classified information. Instead, by far the biggest discovery restriction in classified information cases is the need to get the permission of the originator/owner of the information prior to disclosing that information to the defense. As has been stated before in this Primer, this is most critical in cases involving Sensitive Compartmented Information from national-level members of the Intelligence Community, specifically the National Security Agency and the Central Intelligence Agency .

¹ The Military Rules of Evidence were drafted in 1979-80. For those interested in more information on the development and promulgation of the Military Rules of Evidence, the best source is an article by Professor Fredric I. Lederer, THE MILITARY RULES OF EVIDENCE: ORIGINS AND JUDICIAL IMPLEMENTATION, *130 Mil. L. Rev.* 5, Fall 1990.

Under M.R.E. 505(d), the convening authority is in control of the discovery process before referral. While the investigating officer may at times have to apply the provisions of M.R.E. 505 during the course of the investigation, the investigating officer has limited ability to control discovery since the investigating officer does not have the full authority vested in a military judge after referral. After referral, the military judge is responsible for overseeing the bulk of the M.R.E. 505 procedures that relate to discovery and use of the classified information, as well as any assertion of privilege to prevent disclosure of information. When the case is before the military judge, the defense can object to the convening authority's prior handling of discovery.²

Because of the length of time needed to complete classification reviews and the requirement to get Original Classification Authority (OCA) approval before providing classified discovery, convening authorities should forego or dismiss charges that would unnecessarily bring classified information into the case. Further, trial counsel should carefully select case-in-chief evidence to avoid having to introduce or provide discovery of any more classified information than is necessary to meet the government's burden. While every trial counsel wants to present overwhelming evidence on every charge and specification, trial counsel must resist that urge with respect to classified evidence.

B. Actions Prior to Disclosure to Defense. Whenever possible, before beginning classified discovery, trial counsel *should* ensure that:

- The classification review of the material to be produced has been completed;
- Improperly marked documents have been corrected with proper markings; and
- Classified information no longer warranting protection in the interests of national security has been declassified.

In other words, trial counsel must be sure that the classified document is properly classified before providing discovery of any classified document. While the proper classification of a

² While M.R.E. 505(d) does provide that “[a]ny objection by the accused to the withholding of information or to the conditions of disclosure shall be raised through a motion for appropriate relief at a pretrial session,” counsel should be aware that the some objections may be made and resolved at the Article 32 by the investigating officer and/or the convening authority. Like M.R.E. 412, M.R.E. 505 speaks of the military judge as the decision-maker. Despite that wording, R.C.M. 405(i) provides that rules of privilege in Section V of the M.C.M., like M.R.E. 412, apply to the Article 32. The obvious tension between rules that seem to provide for application by the investigating officer despite the fact that the investigating officer lacks any real authority to invoke the sanctions of a military judge has not been resolved. At a minimum, the investigating officer should have the authority to perform those tasks that clearly impact the conduct of the Article 32, such as issuance of a protective order, ordering compliance with the notice provisions of M.R.E. 505(h), and following the procedures within M.R.E. 505(i) when the government has made the classified material available to the hearing. Where the original classification authority or the convening authority do not make classified information available, there may be little the investigating officer can do. As with litigation over the failure of an investigating officer to employ M.R.E. 412 correctly at an Article 32, the likely remedy for failure to provide classified information at the Article 32 where required would be reopening the hearing, ordering a new Article 32, or simply ordering disclosure to the defense for use at trial. Note that an objection by the government on grounds of privilege, rather than a simple withholding of the documents by the convening authority under M.R.E. 505(d)(5), will result in an *in camera* proceeding under M.R.E. 505(i).

document may be irrelevant to the elements of an offense, it is necessary for invoking the protections of M.R.E. 505.

While the formal protections of M.R.E. 505 privilege assertion are not yet available at this juncture, i.e., pre-referral, the convening authority can, through the protective order (see Section D, below), permit discovery of information with OCA approval. While the classification of the information may later be modified as a result of the classification review, the convening authority, again with OCA approval, can permit discovery with presumptive classification markings that will ensure protection of the possibly classified information.



Practice Pointer. It is possible for multiple versions of the same classified information to be present in a case! In addition, different OCAs may view the classification of the same document (containing information from both OCAs) differently. The trial counsel must resolve these conflicts with the OCAs prior to using the information in any proceeding.

One suggestion is to limit discovery, at least at the outset, to a viewing in a secure space, rather than allowing physical custody by the defense. This will serve the dual purpose of ensuring security over the classified information and facilitating substitution of the properly marked information when the classification review is completed. These measures must not be unduly restrictive of the defense's rights of access. Incorporation of the discovery "rules of engagement" in the convening authority's protective order is highly encouraged (see Section D below).

C. Pre-Referral Discovery. During the early stages of a classified information case, the convening authority controls the pace and amount of classified information turned over in discovery. Effectively, it is the trial counsel that manages this process and coordinates these efforts with the OCAs. Code 17 is always available to assist coordination efforts with intelligence agencies. It is not unusual for an extensive amount of classified information to be turned over to the defense in order to properly prepare for the Article 32 process. M.R.E. 505(d)(4) gives the convening authority this authority. The information can be provided in other formats and trial counsel should be aware that these alternatives are available to avoid actual disclosure of classified information, in discovery, and later, at trial.

1. Classified Information Alternatives. The permissible alternatives are:

(a) Redaction. The first alternative--redacting the classified information out of the document--is the preferred alternative when the classified information is not relevant to the case. In other cases, the fact that a document contains classified information is relevant, but the substance of the classified information and the propriety of the classification are irrelevant. Examples of such offenses include

violations of 18 USC §§ 798³ and 1924, and 50 USC § 783(b),⁴ all of which can be assimilated under Art. 134. In addition, violations of general orders for handling classified information do not require a showing that the classified information at issue was properly classified, but rather that the information was marked as classified and was handled contrary to the governing orders. In such cases, trial counsel might redact all of the classified information from the document and leave the classification markings. In cases in which the government must prove either that the information was properly classified or related to the national defense, trial counsel could select a limited amount of classified information to use as evidence for such purposes and redact the rest of the classified information from the document.

(b) Substitution. The next alternative is to replace the classified information with a substitute. A portion of the document may be replaced with language that either lowers the overall classification of the document (e.g., from SCI to Secret) or may make the entire document unclassified (for instance, if only limited portions are classified). Many times, information may be rewritten to be more general or eliminate or obscure specific sources and methods, yet still keep much of the substance of the information at a lower or unclassified level. The second type of substitution contemplated by the rule is a summary. Especially useful for larger amounts of classified information contained in documents, an unclassified summary of the information may be substituted for the classified information, or for the entire document, as appropriate. These options will require extensive coordination with the owner of the classified information to ensure that the proposed substitutes are, in fact, unclassified. All of the intelligence agencies are familiar with these methods of substitution because they prepare them on a routine basis for cases that the Department of Justice prosecutes using CIPA. Remember, the origins of M.R.E. 505 lie in CIPA and these alternatives should be the trial counsel's first option for introducing evidence at trial rather than immediately succumbing to the lure of a closed session, with its attendant procedural complications (i.e., *Grunden* hearing) and opportunities to introduce appellate error. Substitutions are also an excellent method of dealing with information that will be referred to routinely throughout the trial. A coded

³ "Under section 798, the propriety of the classification is irrelevant. The fact of classification of a document or documents is enough to satisfy the classification element of the offense." *United States v. Boyce*, 594 F.2d 1246, 1251 (9th Cir. 1979), cert. denied 444 U.S. 855 (1979).

⁴ "There is no suggestion in the language of Section 783(b), by specific requirement or otherwise, that the information must properly have been classified as affecting the security of the United States. The essence of the offense described by Section 783(b) is the communication--by a United States employee to agents of a foreign government--of information of a kind which has been classified by designated officials as affecting the security of the United States, knowing or having reason to know that it has been so classified. The important elements for present purposes are the security classification of the material by an official authorized to do so and the transmission of the classified material by the employee with the knowledge that the material has been so classified. Indeed, we think that the inclusion of the requirement for scienter on the part of the employee is a clear indication of the congressional intent to make the superior's classification binding on the employee, once he knows of it." *Scarbeck v. United States*, 317 F.2d 546, 558-59 (D.C. Cir. 1963), cert. denied 374 U.S. 856 (1963).

substitution is often used to avoid the necessity of going into closed session to prevent inadvertent disclosure to the public. An example might be the name of a covert intelligence agency employee. In such a case, the Government might substitute "CIA employee 1" or "John Doe" in place of the real name.

Pseudonyms were used in such a way for certain witnesses in the SEAL detainee abuse trial, *United States v. Ledford*. In the Weinmann case, the name of the country that received the classified information from the accused was, and remains, classified. In place of the country name, "Country X" was used during the plea and sentencing, thus avoiding the need for closed sessions.

(c) Stipulation. The third alternative to the disclosure of classified information in discovery, or the use of classified information at trial, is a statement admitting the relevant facts the classified information would tend to prove. This usually takes the form of a stipulation between the parties. This is a very effective method to protect classified information and have the Article 32 investigation and court-martial as open to the public as possible. It is a method that is used often in federal trials under CIPA and one that deserves much more consideration in courts-martial involving classified information. Stipulations may be helpful to both sides to narrow the issues to be litigated at trial and assist in shaping the case. Given the requirement of R.C.M. 806(b)(2) that reasonable alternatives to closing the court-martial must be considered, the stipulation admitting relevant facts that the classified information would tend to prove is an important alternative to consider. As an example, assume the defense wants to introduce classified operational and intelligence information to show the extent of the threat/violence faced by a unit in a particular area. Rather than introducing all of the classified details, a stipulation of fact acknowledging the level of threat and providing an unclassified description of the conditions faced by the unit would likely suffice.



Practice Pointer. The defense team may find that the stipulation alternative is the most beneficial alternative for the accused. By definition, a stipulation must be agreed to by the parties and the accused. This creates opportunities for creative drafting and is another opportunity for advocacy on behalf of the client. *See, e.g., Turning The Tables: Using The Government's Secrecy And Security Arsenal For The Benefit Of The Client In Terrorism Prosecutions*, Sam A. Schmidt and Joshua L. Dratel, 48 *N.Y.L. Sch. L. Rev.* 69, 84.

These alternatives are designed to minimize the release of classified information and have as open a court-martial as possible, but they do not necessarily mean less work for trial counsel. The redaction of classified information by itself is straightforward and a classification review is not necessary to perform a simple redaction (this assumes, of course, that the material was properly portion-marked and it is easy to tell what paragraphs are classified). However, if the defense is not willing to stipulate that the redacted material is not relevant to the case, or contests the redaction (depending on the

purpose of the redaction), the government must assert the classified information privilege over the redacted information. Likewise, when unclassified substitutes are proposed in lieu of the actual classified information, and the defense objects, classification reviews are required because classified information is being withheld. As for unclassified stipulations, the need for a classification review will depend on the particular facts and circumstances of each case. The stipulation itself may need to be reviewed to ensure that it does not contain any classified information.

2. Protective Orders. During the pre-referral stage, if the Government agrees to produce classified discovery to the defense, the convening authority may disclose it “subject to conditions that will guard against the compromise of the information.” M.R.E. 505(d)(4) (emphasis added.). One type of condition that could be used is a protective order, which is specifically referred to in Rule for Courts-Martial 405(g)(6). Although R.C.M 405(g)(6) does not require the entry of a protective order, the convening authority should, at a minimum, enter a protective order when classified information is disclosed to the defense. The protective order should contain all the provisions of M.R.E. 505(g). Sample protective orders are included in this guide as appendixes to Chapter Six. However, it should be noted that the only specific suggestion of a pre-referral protective order comes in R.C.M 405(g)(6). The language used in M.R.E. 505(d)(4) is “conditions,” a much broader term which means the convening authority is only limited by his imagination and the Constitution in developing conditions designed to ensure the protection of classified information. Some “conditions” that would not be considered unusual, but are certainly NOT required in a classified information case are: requiring the defense to have a GSA-approved safe prior to storing classified material in government defense spaces; using a “reading room” as a central point of storage for all classified information, thereby providing access to the material, but not providing copies; and requiring the accused to be in the presence of his counsel or a cleared member of the defense team when the accused is reviewing classified information in the case.

While not specifically provided for under the R.C.M. or the M.R.E., the defense may object to the terms of the protective order imposed by the convening authority if the defense believes the terms are unduly restrictive or otherwise interfere with the rights of the accused. *See United States v. King*, No. 00-8007/NA, 2000 CAAF LEXIS 472 (C.A.A.F May 8, 2000) (finding that the convening authority’s appointment of an Investigation Security Officer to monitor conversations between defense counsel and the accused does not “appear” to be the “least restrictive means of providing appropriate protection of classified information.”) In a recent non-espionage case, defense objections to the protection order terms and “special instructions” issued by the convening authority were the subject of an extraordinary writ that, again, made it all the way to the Court of Appeals for the Armed Forces. *See Doe v. Commander, Naval Special Warfare Command*, 61 M.J. 14 (C.A.A.F. 2005). In this case, the convening authority’s initial Article 32 convening order had not permitted the introduction of classified information. After an extraordinary writ was filed with the Navy-Marine Corps Court of Criminal Appeals, a revised order was issued directing the investigating officer to inform the convening authority if it appeared that there was classified information requested by the defense that the investigating officer thought was relevant to the case. Although the

second order effectively mooted the extraordinary writ, CAAF specifically stated that the accused could file a further petition for extraordinary relief upon a showing that the convening authority “did and continues to refuse to permit the investigating officer to consider classified information in the hearing that the investigating officer deems relevant to the investigation.” *Id.*

3. Article 32 Proceedings. Article 32 proceedings, like courts-martial, are open to the public. This means that Article 32 investigations may only be closed in accordance with the procedures discussed in the next chapter. Under M.R.E. 505, the assertion of the classified information privilege may not occur at the Article 32 stage of the court-martial proceeding. Instead, under M.R.E. 505(d)(5), the convening authority may choose to withhold disclosure of the information, if disclosure would cause identifiable damage to the national security. Where the information is withheld, the investigating officer does not hold a hearing under M.R.E. 505(i) to determine the classified information’s relevance and necessity to an element of an offense. Those provisions all apply post-referral, in front of the military judge. If the convening authority provided classified information to the defense in discovery, it is entirely possible that classified information will be introduced during the Article 32 proceeding, by one of the parties or through witness testimony, without substantive discussion of their contents. This is most commonly referred to as the “silent witness” rule. Alternatively, the parties may decide to introduce the evidence in a closed session. When that happens, the IO will need to conduct a closure hearing under R.C.M. 806(b)(2), as discussed in Chapter Ten.

Convening authorities should seriously consider avoiding convening orders that bar the introduction of classified information at Article 32 proceedings or that order the entire proceeding to be held either in a closed or open forum. Barring the introduction of classified information and ordering an entirely open proceeding may deprive the accused of the opportunity to effectively represent himself and unconstitutionally restrict his presentation of evidence in his defense.⁵ By ordering an entire Article 32 proceeding to be held in closed session, a convening authority is going to violate the accused’s and public’s right to an open trial. *United States v. Grunden*, 2 M.J. 116 (C.M.A. 1977). Because there may be cases in which the government does not foresee a defense request for discovery of classified information, the investigating officer may have to notify the convening authority “as soon as practicable” upon receipt of such a request. R.C.M. 405(g)(1)(B).

(a). Reasonably Available? Upon receiving a defense request for discovery of classified information or permission to use classified information in the proceeding, the investigating officer (beyond notifying the convening authority) must make an initial determination whether the information requested is “reasonably available.” R.C.M. 405(g)(3)(C). “Evidence is reasonably available if its significance outweighs the difficulty, expense, delay, and effect on military

⁵ See the discussion of *Doe v. Commander, Naval Special Warfare Command*, 61 M.J. 14 (C.A.A.F. 2005) under subsection 2 on protective orders for an example of a case in which a convening authority attempted to restrict the introduction of classified information at an Article 32 proceeding.

operations of obtaining the evidence." R.C.M. 405(g)(1)(B). The determination of whether classified evidence is reasonably available would rest on the normal factors for determining whether information must be produced; this is, whether the requested information is relevant to the investigation, not cumulative, and was requested in a timely manner. *Id.*

If the investigating officer finds classified information requested by the defense to be reasonably available, the investigating officer must request the "custodian of the evidence" to produce it. If the custodian of the evidence determines the classified evidence is not reasonably available, the investigating officer and the accused are bound by that determination. R.C.M. 405(g)(2)(c). With respect to classified information, the "custodian of evidence" may include both the OCA and the convening authority. The originator is a custodian of the evidence because it may be the only agency with physical custody of the evidence and it may bar another holder of the evidence from releasing it without the originator's approval. The convening authority may also be a custodian of the evidence if it has physical custody of the evidence. However, unless the convening authority is also the OCA for the classified information, the convening authority lacks the authority to release the classified information.

If the defense objects to a determination that classified evidence is not reasonably available, the investigating officer must include a statement of the reasons for that determination in the record of investigation. R.C.M. 405(g)(2)(D). The government, therefore, should be prepared to assist the investigating officer in making a full and articulate record of the reasons relied upon by the OCA and the convening authority -- if both have determined the classified evidence is not reasonably available. A good record on this determination will be important since, if the case is referred to a general court-martial, the accused is permitted under R.C.M. 906(b)(3) to move the military judge to review the determination during a pretrial session. Unless the defense request was wholly frivolous, the defense should file such a motion as soon after referral of charges as possible.

(b) Defense Duty of Notification. Although M.R.E. 505 reads as if the notice provisions only apply at trial, recall that R.C.M. 405(i) makes Part V of the M.R.E.'s apply at the Article 32. Therefore, the M.R.E. 505(h) requirement that the defense notify the government of any possible use of classified information appears to apply at the Article 32. Regardless, the convening authority should place a requirement on the defense in the Article 32 convening order. The intent of the M.R.E. 505(h) notice requirement is to allow the government time to complete any necessary classification reviews and to decide whether or not to invoke the privilege. It is also intended to allow the hearing to accommodate classified information without compromise. Although privilege may be a non-issue at the Article 32 stage, the need to get classification reviews and be prepared to address potential closure issues is very important. The convening authority should require the defense to provide this notice well in advance of the date of the Article 32 proceeding, even if this means delaying the Article 32 longer than

would occur in a non-classified information case. In short, the convening order should order the defense to comply with the notice requirements of M.R.E. 505(h), discussed more fully below.

D. Post-Referral Discovery. M.R.E. 505(e) places the post-referral processes squarely in the lap of the military judge, who is to set the timing of requests for discovery, the defense notice obligation under subsection (h), and the *in camera* review hearings of subsection (i). The convening authority's role is now confined to responding, on behalf of the government (including the intelligence community), to the rulings of the military judge. *See* M.R.E. 505(f).

1. Protective Orders. When the government has previously disclosed classified information to the defense, or has agreed to do so post-referral, the onus is on the government, under M.R.E. 505(g), to request an appropriate protective order from the military judge. Trial counsel should ALWAYS request such a protective order in classified information cases. The order previously issued by the convening authority is arguably no longer effective now that the military judge is in control of the litigation. Of course, the defense counsel and accused's duty to safeguard classified information as embodied in the non-disclosure agreement they already signed does not go away. Still, the protective order issued by the military judge ensures that all the parties are aware of the military judge's requirements and expectations with respect to classified information. At a minimum, the protective order proposed by the government for the military judge should include all of the provisions discussed in subsections M.R.E. 505 (g)(1)(A) through (G).

2. Alternatives to Full Disclosure. After referral, under M.R.E. 505(g)(2) the military judge, like the convening authority before him, is authorized to approve the same alternatives to full disclosure or use: redaction, substitution, and admissions of relevant facts. The same considerations as discussed above with regard to those alternatives also apply post-referral. Under this section, however, the military judge is required to consider whether disclosure of the classified information is required to allow the defense "to prepare for trial." Note that a finding that certain information is necessary to "prepare" for trial does not guarantee that the information will be allowed to be used at trial, or used in its classified form. Any motion by the government for using these alternatives are to be considered by the judge *in camera*, which utilizes the procedures contained in subsection (i) of M.R.E. 505, the operation of which is discussed more fully below.

3. Brady Material. Notwithstanding the number of methods and opportunities the government has to avoid full disclosure of classified information, defense counsel are likely to assume that potentially exculpatory information regarding the accused must be disclosed under the principles of *Brady v. Maryland* and R.C.M. 701. However, this assumption may be erroneous when the information at issue is classified. The typical practice in courts-martial is for the government counsel to disclose, per R.C.M. 701(a)(6), "the existence of evidence known to the trial counsel which reasonably tends to: (A) negate the guilt of the accused of an offense charged; (B) reduce the degree of guilt of the accused of an offense charged; or (C) reduce the punishment." This is the codification of

the constitutionally required test set forth by the Supreme Court in *Brady v. Maryland*, 373 U.S. 83 (1963) and *Giglio v. U.S.*, 405 U.S. 150 (1972).

The major factor complicating the discovery of classified information is that regardless of the defense's need-to-know, the Government may not disclose classified information to the defense without the consent of the agency originating that information. "An agency shall not disclose information originally classified by another agency without its authorization." E.O. 12958, § 4.4(b). If the OCA refuses to release exculpatory material, then the exculpatory material cannot be provided to the defense. Of course, from the defense standpoint, this is not all bad as the failure to provide exculpatory material would require the military judge to impose one of the sanctions listed in M.R.E. 505(i)(4)(E) because exculpatory information certainly meets the heightened discovery standard for classified information of "relevant and necessary to an element of the offense or a legally cognizable defense." M.R.E. 505(i)(4)(B) and 505(f).

The biggest hurdle in classified information is simply determining whether any potential *Brady* information even exists, especially when intelligence agencies are involved in the case. Because most military lawyers are not familiar with the operation of intelligence community agencies, neither trial nor defense counsel may even know what to ask for. One possible solution is for counsel to look to the Department of Justice procedures for classified information in federal criminal cases for some good rules of thumb.

Section 2052 of the U.S. Attorney's Manual, Title 9 Criminal Resource Manual ("Manual"),⁶ sets forth DoJ procedures for "Contacts with the Intelligence Community Regarding Criminal Investigations or Prosecutions." The guidance discusses the concept of a "prudential search" of Intelligence Community (IC) files, generally before charges are brought, if the government has "objective articulable facts justifying the conclusion" that IC files "probably contain classified information that may have an impact" on charging and other decisions. Of course, one means by which a prosecutor can come to this conclusion is by a detailed proffer in a discovery request by the defense for information known or believed by the accused to be in the IC files. This certainly makes the government's obligation to conduct a prudential search that much more compelling!

Along those lines, Section 2052 of the Manual also details when a prosecutor is compelled to search for discovery material within IC files. Because we recommend to counsel that they read the Manual we will not repeat the Manual's content *in toto* here. However, the relevant sections may be summarized as follows:

[The] prosecutor's affirmative obligation to search the IC files for *Brady* material is not triggered merely by the defendant's (or the prosecutor's) speculation that such files contain discoverable information. Nor is the government required to search the files of every intelligence agency that conceivably may have exculpatory information...On the other hand, where there is an explicit request for discovery that has been approved by the court, the scope of the search may have

⁶ Available at http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm02052.htm.

to be broadened. It may not reasonably be confined to merely the prosecution team if there are known facts that support the possible existence elsewhere of the requested information... If the prosecutor has actual or implied knowledge that the IC files contain ... Jencks [or] *Brady* materials, the prosecutor must search the IC files.

Manual, Sections 2052(2)(a)(2), 2052(2)(b).

The bottom line is that there are no fishing expeditions for classified material. The intelligence community and its litigation attorneys will not tolerate such forays. However, they will respond to court orders based on non-speculative defense requests. Defense counsel will best serve their client by making such requests as specific as possible. By doing so it is much easier to locate the information among the vast amounts of data held by the intelligence community and it is harder for the government to deny the request.

4. Disclosure of *Brady* Information. Determining the existence of potential *Brady* material does not completely answer the question of whether it has to be disclosed to the defense. There is a limited amount of military case law on this topic. However, *United States v. Lonetree*, 31 M.J. 849 (N-M.C.C.A. 1990), which applies a CIPA analysis to the discovery of potentially exculpatory information at a court-martial, is particularly helpful. The standard the court used is set forth in *U.S. v. Roviato*, 353 U.S. 53 (1957). At its essence, the standard is a 3-part test on relevance; the existence of a colorable privilege; and whether the information is "helpful to the defense" or "is essential to a fair determination of a cause." See e.g., *United States v. Yunis*, 867 F.2d 617 (DC Cir. 1989); *United States v. Moussaoui*, 382 F.3d. 453 (4th Cir. 2004).

5. Jencks Act/R.C.M. 914 Prior Statements. R.C.M. 914 codifies for military courts-martial the provisions of the Jencks Act (18 U.S.C. §3500), which relates to prior statements of a witness available in discovery to the opposing side following that witness's testimony. The usual R.C.M. 914 rules do not apply, however, when the witness's prior statement is classified in accordance with Executive Order 12958, as amended. When the privilege against disclosure is invoked over such statements because of their classified nature, the military judge must conduct an *in camera* review of the material to determine whether the classified statement is consistent or inconsistent with the witness's testimony. If the statement is consistent, then the judge will excise the consistent classified portion from the prior statement and deliver the redacted statement to the defense. If the statement is inconsistent, then the military judge must give the government an opportunity to invoke 505(i) proceeding. Essentially, there is no harm in not disclosing prior consistent statements to the defense. However, the onus of making that determination is placed on the military judge. If the military judge finds that the statement is inconsistent, but the government still refuses to permit disclosure to the defense, this, again, presents an opportunity for the defense to get the military judge to invoke one or more of the sanctions of M.R.E. 505(i)(4)(E) against the government.

If there are prior statements of witnesses that are classified, those statements will need to undergo a classification review just like any other potential classified evidence to be used at trial. Trial counsel and staff judge advocates need to plan accordingly, well in advance of trial, so that delays will not derail the court-martial process. The defense is also obligated to notify the government under M.R.E. 505(h) if they are aware of any prior statements by defense witnesses that may be classified. This will permit the government the time to have a classification review completed and determine whether or not it will invoke the classified information privilege over the material.

6. Defense Duty of Notification. M.R.E. 505(h) imposes a mandatory requirement on the defense to notify the government of any classified information that it “reasonably expects to disclose,” or cause to be disclosed, in the defense case. It should be noted upfront that there is no reciprocal notice requirement within M.R.E. 505(h) imposed on the government. This is very different from most other R.C.M. notice provisions, which generally impose reciprocal notification requirements on the government. Despite the lack of reciprocal notice, where the government does intend or expect to disclose information at trial, the defense will get notice either at the evidentiary stage under M.R.E. 505(i), or at the closure stage under R.C.M. 806(b)(2), as the government will have to move the court for authority to conduct a closed session for purposes of taking classified evidence. Since notice will occur anyway, defense counsel should consider a motion requesting reciprocal notice from the government at the same time defense notice is due. After all, if there is any case where the military judge and the parties want to avoid trial by surprise, it is a case involving classified information. The court must know this evidence is coming in order to adequately prepare for the hearing.

The M.R.E. 505(h) defense notice must be served on trial counsel and the military judge within the time frame specified by the military judge or, if no time has been specified, prior to arraignment. M.R.E. 505(h)(1). This notification obligation is a continuing duty and the defense must notify the trial counsel and military judge “as soon as possible” after learning of the reasonable expectation to disclose information for which notice was not previously given. M.R.E. 505(h)(2). The notice must include a brief description of the classified information but must be “more than a mere general statement of the areas about which the evidence may be introduced.” M.R.E. 505(h)(3). Rather the notice “must state, with particularity, which items of classified information he reasonably expects will be revealed by his defense.” *Id.* This provision is in keeping with the idea that fishing expeditions for classified information are not allowed. The defense must list the particular items of classified information that will be used at trial.

Although “particularity” refers to identification of the classified information to the extent possible, and not the intended use of that information, it may not be entirely possible for the defense to avoid sharing the purpose for which it intends to use the information. Under the procedures of M.R.E. 505(i), discussed in the next section, if the government objects to information contained in the defense notice on classified privilege grounds or proposes an alternative to the requested defense information, the defense will need to argue why the information itself is relevant and necessary to the defense’s case. Likewise, there may be situations in which the government argues that the classified

information sought by the defense is not relevant under the standard of R.C.M. 401 (discussed in section E below). In such an instance, the defense will also need to reveal to the government and the military judge the intended use that makes the information relevant to the case.



Practice Pointer. Defense counsel should note that the notice requirement encompasses information that the defense will “cause the disclosure” of, for instance on cross-examination of witnesses during the government’s case-in-chief! Defense counsel must carefully plan out all aspects of their case well in advance to ensure that they are not foreclosed from pursuing a classified line of questioning. See M.R.E. 505(j)(4) (permitting government objection to any line of inquiry not previously found to be relevant and necessary to the defense).

7. The *In Camera* Proceeding. The evidentiary hearing to which all M.R.E. 505 roads lead⁷ is the *in camera* proceeding under M.R.E. 505(i). The primary purpose of the *in camera* proceeding is to litigate the government’s assertion of privilege over classified information. As it is rare that information is withheld from disclosure to the accused,⁸ the secondary purpose of the *in camera* proceeding is evidentiary, i.e., the consideration and approval of classified information alternatives and substitutes. The *in camera* proceeding is separate from the hearing used to close the courtroom. A hearing to close the courtroom has traditionally been called a *Grunden* hearing, but is actually best thought of as a hearing under R.C.M. 806(b)(2) and is discussed in the next chapter.

M.R.E. 505(i)(2) places the burden of moving for an *in camera* proceeding on the government, after all, it is the government’s privilege. The government needs to provide the classified information at issue and an affidavit to the military judge, who examines the material *ex parte*. The affidavit must demonstrate that the disclosure of the information could cause damage to the national security in the degree required to warrant classification under the applicable Executive Orders and regulations. The classification review completed by the subject matter expert and endorsed by the Original Classification Authority fulfills this requirement. The military judge does not review the propriety of the classification, but does ensure that the information has been classified in accordance with the Executive Order. As discussed in Chapter 7, every properly prepared classification review will describe the damage to national security in the term

⁷ The other sections that refer to the *in camera* proceeding are: (e), (g)(2), (g)(3)(B), and (h)(4).

⁸ One of the rare instances was the case of *United States v. Lonetree*, 31 M.J. 849 (N-M.C.M.R. 1990), aff’d 35 M.J. 396 (C.M.A. 1992). In *Lonetree*, the government withheld the name and background information of a government agent who was called to testify about facts that would corroborate Lonetree’s confession. The agent was to testify that a known Soviet agent appeared at a time and place indicated by Lonetree as the location he was to meet this known Soviet agent. The trial judge agreed with the government’s motion and allowed the agent to testify under the pseudonym John Doe, without his real name and background known to the accused and his counsel. The Navy-Marine Corps Court of Military Review and the Court of Appeals for the Armed Forces both determined that withholding the information did not violate the accused’s Sixth Amendment confrontation right because the accused had all that was needed to place the witness “in his proper setting” and to provide the context for the testimony. *Lonetree*, 35 M.J. at 42-43.

concomitant with the requisite level of classification: damage for Confidential; serious damage for Secret; and extremely grave damage for Top Secret. Once the military judge reviews the properly prepared classification review affidavit, he will conduct an *in camera* proceeding.

Interestingly, although there are repeated references to this as an *in camera* proceeding, the defense has a role to play. The government is required to give the accused notice of the information that is the subject of the *in camera* proceeding. This is to allow the defense the opportunity to prepare an argument to be presented to the military judge regarding the material that is the subject of the proceeding. If the classified information has never been made available to the accused in conjunction with pretrial proceedings, then the government may provide a generic description of the material to the defense team. This generic description must be approved by the military judge. If the classified information has previously been available to the accused during the course of the proceedings, usually in discovery, then the government's notice must specifically identify the information that will be at issue in the proceeding. Thus, the more the accused knows about the information, the more information must be contained in the government's notice.

Before the military judge makes his ruling, both the government and the defense are given the opportunity to brief and argue their respective positions to the military judge, ostensibly as part of the *in camera* proceeding. If the military judge finds, in writing,⁹ that the classified information is "relevant and necessary to an element of the offense or a legally cognizable defense and is otherwise admissible in evidence," M.R.E. 505(i)(4)(B), he can then order the government to disclose the information to the accused for use at trial. The government then has the option to either produce the material, stipulate to admissible facts, or propose an alternative that the military judge finds an acceptable substitute. If the military judge finds there is no acceptable substitute or replacement for the material itself and the government still refuses to disclose the information (as is its prerogative), then the military judge "shall issue any order that the interests of justice require" pursuant to M.R.E. 505(i)(4)(E). M.R.E. 505(i)(4)(E) provides a non-exhaustive list of possible sanctions.

M.R.E. 505(i)(4)(D) makes it clear that a full discussion of evidentiary alternatives to full disclosure is a primary purpose of the *in camera* proceeding. The rule clearly contemplates situations in which the government does not contest the relevance, necessity, and admissibility of the issue. In such circumstances, the focus of the inquiry is not whether the information should be disclosed or not, but whether or not there is an acceptable alternative. "Acceptable," of course, is up to the military judge, whose decisions will be subject to appellate review as the record of the *in camera* proceeding, including the complete version of the classified information, is sealed and attached as an appellate exhibit to the record of trial.

⁹ M.R.E. 505(i)(4)(C) states that the information may not be disclosed "[u]nless the military judge makes a written determination that the information meets the standard set forth (above)." (emphasis added)

8. Consequences for Invoking the Classified Information Privilege: Sanctions

Under M.R.E. 505(i)(4)(E) and M.R.E. 505(f). Although they are phrased in a similar fashion, the sanctions of these two sections arise under very different circumstances and are imposed by two different entities. The military judge is the primary sanctioner under M.R.E. 505(i) if the government continues to refuse to disclose classified information following a fully litigated *in camera* proceeding. In such a proceeding, the military judge has had full access to the classified information at issue, thus he can take a nuanced approach to sanctioning the government. The military judge's options are greater under M.R.E. 505 (i)(4)(E) than the convening authority's are under M.R.E. 505 (f). Pursuant to M.R.E. 505(i)(4)(E), the military judge may do nothing, strike testimony, or even dismiss the charges or specifications to which the classified information relates.

Unlike the sanctions under M.R.E. 505 (i)(4)(E), the sanctions under M.R.E. 505 (f) come into play in large part because the classified information is not being made available to the court for review. M.R.E. 505(f) places the onus on the convening authority to locate classified information that is apparently relevant and necessary, even if the appearance is only due to the defense's notice under M.R.E. 505 (h). The military judge is simply not able to make the same ruling that he can under M.R.E. 505(i)(4)(E) since he has not had a chance to actually evaluate the merits of the information. The military judge is simply relying on the defense's proffer and whatever is offered by the government. But note that the military judge is not empowered to order discovery of the information. He can only place the ball back in the convening authority's court.

The convening authority is then put in the challenging position of making major decisions in the case with respect to classified information that is likely not under his control. The convening authority can "institute action to obtain the classified information for the use by the military judge in making a determination under subdivision (i)." M.R.E. 505(f)(1). This will likely include negotiating with the equity owner for disclosure of the information, at least to the military judge, to permit the more thorough review under 505(i). As discussed below, the 505(i) review may ultimately result in the information being protected from discovery or use in the case anyway, but it must be disclosed *in camera* to the military judge and be made a part of the sealed record. For particularly sensitive information that may not be a viable option. In certain cases and for certain information this negotiation may take place at the Secretary level in the inter-agency process. Code 17 is always available to assist throughout this process.

The convening authority's other options are to dismiss the charges completely or only those charges and specifications to which the information relates, M.R.E. 505(f)(2)-(3), or to "take such other action as may be required in the interests of justice." M.R.E. 505(f)(4). One possible such action is to negotiate a pre-trial agreement in order to eliminate evidentiary issues at trial or on appeal.

While the military judge cannot order discovery under this provision, he does have some tools that can be used if the convening authority does not resolve the issues. The military judge must make a determination that proceeding without the information "would materially prejudice a substantial right of the accused" and shall, "after a reasonable

period of time,” “dismiss the charges or specifications or both to which the classified information relates.” M.R.E. 505(f). Notice that the dismissal is mandatory under these circumstances if the judge finds material prejudice.

9. Extraordinary Writs. As discussed in various places throughout this Primer, counsel should not forget the many other provisions in the R.C.M. and M.R.E. just because there are special rules for classified information. The rest of a case involving classified information progresses according to the “normal” rules of practice. Consequently, in addition to the sanctions and remedies available under M.R.E. 505 for discovery limitations, defense counsel should also explore the availability of extraordinary relief at the Navy-Marine Corps Court of Criminal Appeals or even at the Court of Appeals for the Armed Forces if you meet the criteria for an Extraordinary Writ. But, as our appellate colleagues like to say, “they are called extraordinary writs for a reason!”

A court will look to see that the accused has demonstrated a “clear and indisputable right” to the relief. Among the factors that a court may consider are that there is no other means for relief, that the damage is not correctable on appeal, that the action by the military judge is clearly erroneous (*i.e.*, there is no dispute on the law), that this is an example of a recurring error (*i.e.*, continuing application will disrupt the judicial process), or that this is a new/important issue of law. As can be seen, these are difficult hurdles to overcome for the defense. *But see, Doe v. Commander, Naval Special Warfare Command San Diego*, 2004 CCA LEXIS 276 (Unpub. Op. December 15, 2004), and *Denver Post v. U.S. and Captain Robert Ayers*, ARMY MISC 20041215 (ACCA, 23 February 2005).

A major problem for defense counsel attempting to challenge withholding of *Brady* information is the fairly significant test for prejudice. As set out by the Court of Appeals for the Armed Forces, the test is first, was the information or evidence at issue subject to disclosure or discovery; and second, if not disclosed, what was the effect of that nondisclosure on the trial outcome. *U.S. v. Roberts*, 59 M.J. 323, 325 (C.A.A.F. 2004). The very presence of the second test indicates that a court may not be willing to entertain an extraordinary writ on a *Brady* disclosure issue since there is no “trial outcome” upon which to test the alleged harm. However, counsel should conduct their own research into the current state of the law as it relates to their case facts and circumstances and take appropriate action.

E. Motions in Limine Regarding Admissibility and Relevance. A recent phenomenon of cases arising from the Global War on Terror is litigation over the timing of classification reviews for classified information the defense seeks to introduce at trial. In these cases, the convening authority has made a policy decision to provide broad discovery (for instance, access to the intelligence database of a Marine command for a substantial portion of its deployment) to the defense team. The defense then properly files the notice of intent to use particular classified items under M.R.E. 505(h). Prior to undertaking the staffing and coordination required to conduct classification reviews of this material, the government contests the basic relevance of the requested material to the case. Essentially, the government argues that the defense request

requires an unnecessary and burdensome assertion of executive privilege for information that is not relevant.

This issue highlights an area of ambiguity under M.R.E. 505. However, the stronger argument is that the government can argue relevance and materiality issues prior to initiating steps to assert privilege. Of course, if the government adopts this tactic, the government may have to frantically gather classification reviews if the military judge rules that the disputed classified information is relevant. Another issue is the timing of this government effort. In the pre-referral period the convening authority may limit discovery and disclosure per M.R.E. 505(d). However, once the military judge is in control of the case the issue may become problematic for the government although having a detached final arbitrator may also help advance the government's position. The proper way to evaluate this issue is to remember that M.R.E. 505 does not exist in a vacuum in the court-martial process. Other evidentiary and procedural rules operate in conjunction with M.R.E. 505 and are not specifically superseded by the privilege unless indicated in the other rule. *See, e.g.*, R.C.M. 701(a)(6) compared with 701(f) (limits discovery of information "protected from disclosure by the Military Rules of Evidence.")

Government counsel can argue that the plain language of M.R.E. 505(e) does not require assertion of the privilege prior to preliminary R.C.M. 802 and/or Art. 39(a) sessions to discuss various issues relating to the case including the need to hold a *Grunden* closure hearing under 505(i) (*See* Chapter 10). The last paragraph of 505(e) provides that the military judge **"may consider any other matters that relate to classified information or that may promote a fair and expeditious trial."** (emphasis added) The government may want to argue that this language permits, and in fact encourages, the military judge to use this forum to rule on relevance and materiality under M.R.E. 401-403 as they might in other cases when the government seeks a Motion *in Limine* under R.C.M. 906(b)(13) and M.R.E. 104, without the need for classification review and privilege assertion. While there is nothing that prohibits such arguments early in a classified information case, there is the issue of what to do should there be a need to discuss the substance of the classified information at the motions hearing (as opposed to just discussing its legal significance). Under R.C.M. 806(b)(2), the military judge has the discretion and authority to close the proceeding, even without a classification review. This possibility is discussed in more detail in Chapter 10.

FOR OFFICIAL USE ONLY

This page intentionally left blank

CHAPTER 10

Courtroom Closures

The ability to present classified evidence to members at trial in a session closed to the public is unique to courts-martial. Closing the courtroom to present evidence to the jury is not an option under the Classified Information Procedures Act (CIPA) in federal court. With this authority to close the courtroom, however, comes the responsibility to ensure that closures are narrowly used in order to best uphold the right to a public trial that adheres not only to the accused, but also to the general public. Closed proceedings are drawing increased scrutiny from the news media.¹ The following sections discuss the history of closing courts-martial and the current procedures for doing so.

A. History. The genesis of the modern classified information privilege is the Supreme Court case of *United States v. Reynolds*, 345 U.S. 1 (1953). In *Reynolds*, an Air Force B-29 exploded in mid-air in October, 1948, in the vicinity of Waycross, Georgia. The plane was carrying a number of pieces of classified equipment and, along with its military crew, civilian scientists and technicians. The widows of the civilians sued the Air Force for damages, claiming that the plane was negligently maintained. In discovery, the widows of the civilians asked for the accident report and the statements of the surviving crew members taken as part of the investigation. The Air Force refused to produce the documents, even to the Federal District Court judge, based on Air Force regulations regarding release of accident reports and a formal claim of privilege over the information filed by the Secretary of the Air Force on national security grounds.² After the trial judge entered a finding of negligence against the government based on the refusal to disclose the documents to the court, the government appealed.

The Supreme Court held that a privilege against revealing “military secrets” does exist in the law and was validly invoked in *Reynolds*. The privilege must be invoked by the “head of the department which has control over the matter,” *id.* at 8, and the court must determine whether the claim of privilege is appropriate in the circumstances, yet do so without forcing disclosure of the information to be protected. The Supreme Court went on to hold that there is no requirement for the information to be automatically disclosed to the court for review, especially in a case where witnesses were made available to testify about the non-classified events that presumably caused or led to the plane’s crash. *Id.* at 11.³

¹ The Ariel Weinmann espionage case provides an excellent case in point. In that case, the Article 32 proceeding was held without local media in attendance. Although the proceeding was never closed, there were various military personnel coming and going throughout the proceedings. When the media learned about the Article 32 hearing, the Navy was accused of holding “secret” trials. Tim McGlone, *Silence Surrounds Navy’s Local Court System*, *Virginian Pilot*, August 4, 2006, at A1. Although the media was provided a transcript of the Article 32 proceeding, subsequent reporting contained an air of skepticism through repeated references to the earlier, “secret” proceeding.

² The Air Force did offer to make the surviving crew members available for examination by the plaintiffs with the ability to refresh their recollection from their previous statements to the Air Force, though they could not discuss classified matters. *Reynolds*, 345 U.S. at 5.

³ For a recent detailed examination of the *Reynolds* case, including a discussion of the facts contained in the accident report, which was found on the Internet by the daughter of one of the deceased civilians, see Louis Fisher, “In the Name of National Security: Unchecked Presidential Power and the *Reynolds* Case (2006).”

Significantly for court-martial practice, the Court distinguished the civil, tort case at issue in *Reynolds* from criminal cases stating that “it is unconscionable to allow [the government] to undertake prosecution and then invoke its governmental privileges to deprive the accused of anything which might be material to his defense.” *Id.* at 12. Thus, as discussed in the previous chapter, the remedies available under M.R.E. 505 for failure to disclose relevant and necessary classified information are much more favorable to the accused than to a plaintiff in a civil case.

1. *United States v. Grunden.* In court-martial practice, the seminal case for closing the courtroom to the public is *United States v. Grunden*, 2 M.J. 116 (C.M.A. 1977). At the time *Grunden* was decided, the controlling provision from the Manual for Courts-Martial stated “all spectators may be excluded from an entire trial, over the accused’s objection, only to prevent the disclosure of classified information.” M.C.M. para. 53e (1969 Rev.) (emphasis added). That provision went on to state that such authority must be “cautiously exercised” and the right to public trial is to be balanced with the public policy considerations justifying exclusion. *Id.* The trial judge proceeded to exclude the public “from virtually the entire trial as to the espionage charges.” *Grunden*, 2 M.J. at 120. Although the court’s actions were ostensibly within the plain language of the rule, the Court of Military Appeals found that the trial judge erred by “employ[ing] an ax in place of the constitutionally required scalpel.” *Id.*

The court then went on to establish a balancing test designed to ensure that the exclusion of the public is “narrowly and carefully drawn.” *Id.* at 121. The trial court is to weigh the reason for excluding the public against the possibility of a miscarriage of justice that might occur from such an exclusion. *Id.* at 121-22. In a case involving classified information, the prosecutor meets this “heavy burden” by demonstrating that the material in question has been properly classified.⁴ *Id.* at 122-23. To limit the danger of a miscarriage of justice, under *Grunden*, the military judge must carefully consider the scope of the public’s exclusion, ensuring that the exclusions are limited only to those portions of testimony involving classified information. *Id.* at 123.

In order to properly balance the competing interests in such a case, the *Grunden* court recognized that discussion of the classified information at issue may have to take place between the military judge and the parties in a preliminary hearing closed to the public. Note that the court did not impose a predicate requirement to demonstrate the classified nature of the material prior to closing the preliminary hearing. In its analysis of the error committed in *Grunden* at the trial level, the appellate court is focused on the exclusion of the public from the presentation of testimony and evidence to the members. In fact, the

⁴ The *Grunden* court makes a number of statements that appear to leave a great deal of discretion to the prosecutor as to how to prove the classified nature of the material. For instance, the court first says the trial judge must be “satisfied from all the evidence and circumstances that there is a reasonable danger” of exposing national security matters. The court then says the method used by the prosecution to carry its burden will “vary depending on the nature of materials in question and the information offered.” *Grunden*, 2 M.J. at 122. The court’s most definite statement of how to prove the reason for excluding the public is “that the material in question has been classified by the proper authorities in accordance with the appropriate regulations.” *Id.* at 123. As discussed in Chapter Seven, a properly prepared classification review will satisfy this requirement. However, it is not the only way to reach the first prong of the balancing test. The markings, content and originator of the document could be sufficient to meet the various formulations of what needs to be demonstrated to the military judge.

majority rejects the dissent's call to take into account all of the pre-trial hearings, final instructions, and sentencing phase of the trial and find no violation because over 60% of the trial was conducted in open session. *Id.* at 120, n.2. Thus, there is less concern about a miscarriage of justice due to the closed proceeding when it is a preliminary hearing outside the presence of the members and controlled by the military judge.

At the hearing, often called a *Grunden* hearing, after demonstrating the classified nature of the material at issue, the government then must delineate which portions of its case-in-chief will involve these materials. The military judge must decide on the scope of the exclusion in order to ensure that only those portions of testimony that actually involve classified information will be closed to the public. It is not sufficient that there is a fear or mere probability that there will be an unplanned spontaneous disclosure of classified information. Such speculation does not justify excluding the public from that portion of the testimony. *Id.* at 123, n.20.

2. Military Rule of Evidence 505. Three years after the *Grunden* decision, the Military Rules of Evidence (M.R.E) were promulgated. As discussed in Chapter Nine, M.R.E. 505 was derived from the House of Representatives version of CIPA (H.R. 4745). The Analysis of the Military Rules of Evidence, contained in Appendix 22 of the Manual for Courts-Martial provides a breakdown of which section of H.R. 4745 each section of M.R.E. 505 was drawn from and how the language was modified to comport with military justice practices.

With all the procedures imbedded in M.R.E. 505, there is, surprisingly, a dearth of any specific procedures on closing the courtroom. The sole reference to taking such action is contained in subsection (j)(5), which states “[t]he military judge may exclude the public during that portion of the presentation of evidence that discloses classified information.” The Analysis simply refers to the fact that subsection (j) comes from section 8 of H.R. 4745 and *Grunden*. Neither (j)(5) nor the Analysis refers to any other section of the rule that applies to the hearing required by *Grunden*.

Specifically, there is nothing to indicate that subsection (i) of M.R.E. 505 is required to be used for the *Grunden* hearing.⁵ Had the drafters intended for that to be the case, there surely would have been a cross-reference to subsection (i) in either (j)(5) or the Analysis, as there are in other sections of the Rule that point specifically to (i). While some have suggested that the in camera procedure of subsection (i) should be the *Grunden* hearing procedure, subsection (i) is actually much more than that. Subsection (i) is an evidentiary procedure related to what evidence must be disclosed in discovery and in what form that disclosure must take. Prior to 2004, it is not surprising that the differences between *Grunden*'s relatively limited closure hearing and subsection (i) were less than fully appreciated. However, the promulgation of Rule for Courts-Martial 806(b)(2), as discussed below, clarifies the distinction.

The *Grunden* hearing is used to determine what portions of the classified information disclosed under subsection (i) will actually need to be discussed in testimony during the

⁵ See Chapter Nine for a complete discussion of the operation of M.R.E. 505(i).

court-martial, requiring the exclusion of the public. The subsection (i) procedure is usually done well in advance of trial so that the parties have adequate time to prepare for trial based on the material the military judge finds to be relevant and necessary. The *Grunden* hearing should occur much closer to trial because it is concerned with the presentation of evidence, which the parties may not have planned out until close to the time of trial. As discussed below, there are ways to present classified information at trial that do not involve oral testimony or other discussion of the information, which would not require exclusion of the public from the court-martial. In summary, *Grunden's* closure hearing and, as discussed below, the R.C.M. 806(b)(2) hearing pertain to the courtroom closure process while M.R.E. 505 subsection (i) is an evidentiary procedure that focuses on what classified evidence is relevant and necessary, and, if relevant and necessary, what form of discovery is most appropriate.

3. Rule for Courts-Martial 806(b)(2). In 2004, the standards for excluding the public from a court-martial were clarified and codified in a change to Rule for Courts-Martial (R.C.M.) 806(b). Prior to the change, R.C.M. 806(b) simply said that the public could only be excluded over the accused's objection "only when expressly authorized by another provision of this Manual." R.C.M. 806(b), M.C.M. (2002). As pointed out by the Analysis of R.C.M. 806(b), this language essentially referred back to the closure language of M.R.E. 505(j)(5). The 2004 change eliminated this limiting language and broadened the circumstances under which the military judge can close the proceedings, provided that the standard contained in R.C.M. 806(b)(2) is met.

R.C.M. 806(b)(2) codified the standard of the *Grunden* line of cases as advanced by *United States v. Hershey*, 20 M.J. 433 (C.M.A. 1985) and *ABC, Inc. v. Powell*, 47 M.J. 363 (C.A.A.F. 1997). These cases, as well as R.C.M. 806(b)(2) are discussed more extensively in the next section, which covers the hearing used to close the courtroom or Article 32 proceeding.

B. The Closure Hearing. R.C.M. 806(b)(2) effectively supplanted *Grunden* as the standard for closing courts-martial, no matter the reason. See R.C.M. 806(b)(2) Discussion (stating that the Rule sets forth "the constitutional standard"). The Rule places a great deal of discretion in the hands of the military judge, particularly because it does not dictate the method of demonstrating the government's overriding interest.

The Rule's operation is relatively straightforward. The military judge can order the proceedings closed if he first finds a substantial probability that an overriding interest will be prejudiced by keeping the proceedings open. M.R.E. 806(b)(2)(1). In the case of classified information, the overriding interest is the prevention of harm to the national security. The Rule also requires that the military judge use the *Grunden* scalpel by ensuring that the "closure is no broader than necessary to protect the overriding interest." *Id.* at (b)(2)(2).

The final substantive requirement is that the military judge must consider reasonable alternatives to closure and find that they are inadequate. Certainly, the alternatives that are available under M.R.E. 505(i) would be viable alternatives to closing the courtroom. However, they are not the only alternatives available to closing the courtroom in the event that the M.R.E. 505(i)

evidentiary hearing determines there is no adequate redaction, summary, or substitution for the actual classified information being presented to the members. There are a number of alternatives to testimony for introducing the actual classified information at trial that should be considered before the military judge decides to close the courtroom. These alternatives, which are commonly used in federal court prosecutions under the Classified Information Procedures Act, are discussed in more detail below. Finally, R.C.M. 806(b)(2) requires the military judge to place his case-specific findings justifying closure on the record for later review on appeal.

1. Demonstrating the “Overriding Interest.” As stated earlier, the military judge is vested with broad discretion with respect to how the overriding interest is demonstrated. This accords with some of the broader language contained in *Grunden* as discussed in the section on that case above.

(a) Classification Review. By far the easiest method of demonstrating the government’s overriding interest where classified information is concerned is to submit a classification review. The potential harm to national security from disclosure of the information is the government’s overriding interest in the classified information. For purposes of demonstrating this interest, only the classification review itself (the Original Classification Authority (OCA) affidavit, or the subject matter expert affidavit accompanied by the OCA letter) is needed, not the assertion of privilege by the head of the military department. Classification reviews are covered extensively in Chapter Seven of this Handbook.



Practice Pointer. Again the need to consult with the originator of the classified information prior to its use is paramount. They must be consulted to determine if they want their information used in litigation before any charges are preferred and before any classified information is disclosed to the defense.

(b) No Classification Review. It is possible to demonstrate the overriding interest in the classified information without a formal classification review prepared by the OCA. This can be done, for instance, through testimony of a witness with sufficient knowledge and experience of the material that he can accurately describe to the military judge the harm to national security that would result from disclosure.⁶ As this is a pretrial matter, the witness could be a user or derivative classifier of the evidence, as long as they are familiar with the information and understand the ramifications of its disclosure. As a military judge can take hearsay evidence at pretrial proceedings, *see* M.R.E. 104(a) (stating that the

⁶ For instance, a Navy or Marine Corps intelligence officer can testify as to whether or not the document is properly marked and can testify, based on his level of knowledge, experience and training (all of which should be presented to the court) that the material fits within the categories of the executive order and describe the damage to national security that would result from disclosure. This was done for preliminary hearings in the USMC Hamdania cases arising from the war in Iraq when a classification review was not completed on a document that was the subject of a *motion in limine* to exclude the document based on M.R.E. 401.

military judge is not bound by the rules of evidence when determining preliminary questions such as the admissibility of evidence or the existence of a privilege), there is no need to have someone from the originating agency testify to demonstrate the overriding interest. This will make it easier to find local witnesses near the court-martial venue. Or the government can submit the hearsay testimony or affidavit from someone who has discussed the potential damage to national security with the originating organization in order to prove the overriding interest. Such an affidavit, of course, could not substitute for a formal classification review in support of the assertion of the classified information privilege.

2. “Reasonable Alternatives” to Closure. The military judge next must consider whether there are any alternatives that would satisfy the need for the actual classified information. It is not enough to review the classified information alone and determine that it needs to be protected. Closing the courtroom on that basis alone would be error. There must be a consideration of either alternatives to the information or alternative methods of presentation in an open session that would not disclose the classified information. Only by considering alternatives can the military judge make findings about why the proposed alternatives are inadequate for use at trial. Alternatives to the actual classified information, such as redacted versions, summaries, substitutions and stipulations were covered extensively in Chapter Nine. Those options should be reviewed early in the court-martial process with the OCA. The parties, especially the government, should also be prepared to discuss with the military judge other alternative methods of presenting the evidence without disclosing its classified substance. These alternatives are only limited by the bounds of one’s imagination. The most commonly seen alternatives for presenting classified information in open court are:

(a) **“Silent Witness” Rule.** The most commonly used method of presentation is the “silent witness” rule. Under this scenario, a classified document is introduced into evidence via a witness who testifies about all the facts, usually unclassified, needed to determine the documents relevance and hearsay exception, without discussing the substance of the document itself. After it is introduced into evidence, it is then published to the properly-cleared members to review. In many cases, the legal impact or effect of the document can then be discussed in open court without reference to any of the classified material contained in the document. With specific portions tabbed and marked, counsel can then use those references as part of their unclassified direct and cross-examinations about the damage to national security or other relevant legal arguments. Introduction of evidence via the “silent witness” rule will involve a certain amount of “talking around” the subject, so it may be necessary to have certain terms or concepts reviewed by the OCA to ensure that they may be used in an unclassified setting. It is important to understand that generally the most sensitive portion of any intelligence information is the source and method from which the information was derived. If there is need to discuss this aspect of the information, there should always be a review by the OCA of the proposed unclassified terms and phrasing.

Counsel should review current case law on the use of this method based on the facts and circumstances of the proposed use in any particular case.

(b) Use of Code Words or Special Terms. When the classified information is a discreet piece of information, such as the name of a country involved in an espionage case, code words or terms may be used in place of the actual information to prevent unnecessary closure of the courtroom. For instance, Country A and Country X, could represent two countries in a case where A is the country that received the classified information from the service member and X is the country where the transfer occurred. The substitution of terms could be used for a whole host of information such as classified program names or compartmented information. When such code words or terms are used, all those who need to know the correlation between the term and the classified information would have a key to use during questioning, testimony, and argument. The key, of course, is going to be classified at the highest level of information contained on the sheet and will always be an appellate exhibit.

(c) Use of Screens and Other Methods of Disguise. If the identity of a witness is classified, but the substance of his testimony is not, then it is possible for the witness to testify from behind a screen or in light disguise. When using a screen, it is normally arrayed so that the military judge, members and the parties can see the face of the witness, but his visage is blocked from public viewing. This issue has come up in at least one case arising from the Global War on Terror in the case of a Navy SEAL charged with abusing a detainee.

(d) Imagery. Classified imagery can be presented in open court in a number of different ways. One option is to place the poster board of the image in such a manner that only those with clearances are able to see the image, with those in the public gallery unable to see the image depicted. Then, if the details that are being described are unclassified, the public may hear the description of what occurred without seeing the graphic depiction. This method is especially effective for the photo used as a demonstrative exhibit, but would also work for a classified photograph introduced into evidence. If introduced into evidence, similar to documents, a classified photograph could be simply printed and distributed to the members and treated as any other piece of classified information. Another option to present classified imagery, or other classified information for that matter, is the use of courtroom monitors in those locations so equipped. Again, use of such technology needs to be carefully monitored and understood, especially the need for classified computer equipment rather than the standard equipment used. The screens also must not be visible to the public gallery. Finally, apart from the computer/driver combination, there must be a review to ensure that the other components of the system do not have nonvolatile memory chips, i.e., memory that retains the information temporarily stored there until the next information replaces it. Volatile memory dumps the data as soon as the component has completed using the memory.

3. Building the Record. Finally, R.C.M. 806(b)(2) requires the military judge to place his findings as to why the alternatives are not adequate on the record for review on appeal. This is especially important in any case in which the accused has consistently maintained his right to a public trial and objected to some or all closures of the proceedings.

C. Special Considerations for the Article 32 Hearing. In *ABC, Inc. v. Powell*, 43 M.J. 363 (C.A.A.F. 1997), the U.S. Court of Appeals for the Armed Forces ruled: "Today we make it clear that, absent 'cause shown that outweighs the value of openness,' the military accused is . . . entitled to a public Article 32 investigative hearing." *Powell's* holding means that the Article 32 appointing authority and pretrial investigating officer no longer have unbounded discretion to order Article 32 investigations closed to the public. It also means that the parties cannot stipulate or otherwise agree to close proceedings. The process for closing an Article 32 investigation and a court-martial is identical. There are no "shortcuts" or other means of closing an Article 32 other than the process described above under R.C.M. 806(b)(2). The investigating officer must be sure to consider reasonable alternatives to closing the hearing. He should also consider bifurcating witnesses testimony into open and closed portions, closing only that portion of a witness's testimony that contains classified information. Finally, the investigating officer, like the military judge, must be sure to put the reasons for any closure on the record. A recent case that illustrates the pitfalls of closing an Article 32 investigation improperly is *Denver Post v. U.S. and Captain Robert Ayers*, ARMY MISC 20041215 (A.C.C.A., 23 February 2005).

As discussed in Chapter Nine, it is also very problematic for a convening authority to attempt to order an Article 32 to be entirely open. Instead, the accused must be allowed to present evidence to the investigating officer. The better course is to direct the investigating officer to bring requests for classified information to the attention of the convening authority for resolution.

D. Closing the Courtroom: The Logistics. Once the military judge has determined the need for a closed session, precautions need to be taken to ensure the security of the information to be discussed in the courtroom, including the proper handling of the record of the proceeding.

Prior to entering the closed session at trial, the military judge must work closely with the courtroom security officer to ensure that the hearing room is properly secured and that all persons present have the requisite clearance and "need to know." The military judge should address these issues on the record. The military judge and courtroom security officer need to consider the circumstance of each courtroom setting in determining what measures need to be taken. Some of the most common measures that should be considered are:

1. Posting guards with proper clearance level near entrances to the courtroom if there is a possibility that the proceedings may be heard near the doors.
2. Post signs outside the courtroom stating that the court is in closed session.
3. Ensure that any security cameras or video feeds to locations outside the courtroom are shut down if classified information is visible to the cameras. Even if classified information cannot be seen on the video feed, any accompanying audio feed should always be secured because the reason for holding a closed session is to present oral testimony in court.

4. Switching the system used to record court proceedings so that there is no mixture of open and closed sessions on the same media.

At the start of the closed session, the military judge should state, or have whichever side is the proponent of the information state, the classification level for the record. Before adjourning from the closed session the military judge shall again have counsel who has introduced the classified information confirm the appropriate classification level for the record. When shifting from a closed session, the military judge should take a recess of sufficient length to permit the previously implemented security measure to be removed. Specifically, the courtroom security officer and military judge should ensure that:

1. The court reporter properly marks and secures the classified tapes or other media used to record the proceedings and any notes taken by the court reporter during the closed session.
2. Counsel or the court security officer secures any classified information, including exhibits published to the members or member notes.
3. The bailiff removes any signs placed outside the courtroom and ensures that the guards know that the courtroom has reopened.

E. Planned v. Unplanned Closures. To this point, the discussion has concerned planning for known closures where the classified information at issue has been vetted and the findings required by R.C.M. 806(b)(2) have been made in advance of the court-martial. But it may be the case that a line of questioning inadvertently contains or might cause classified information to be disclosed in open sessions. If this should occur, procedures need to be in place to prevent the accidental disclosure of classified information and to apply the standard of R.C.M. 806(b)(2). The military judge⁷ should consider spelling out the procedures to be used in a particular case in a protective order and the parties should be familiar with the order's contents and the military judge's expectations with respect to unplanned closures.

An “**unplanned closure**” will occur when counsel, the court security officer, equity owner subject matter expert, witness, or other individual informs the military judge of the need for a closed session if testimony “strays toward disclosure of classified information when testimony is given in open session.” *Denver Post Corp. v. U.S.*, Army Misc. 20041215 (23 February 2005)(Unpub. op. at 4). This may result from the person recognizing that a question contains classified information or calls for a classified answer. Often the security officer will have a pre-arranged signal or device that can be used to indicate to the judge that this danger is present. Witnesses should be advised that if they believe that an answer to a question, or the question itself, may involve classified information, to notify the military judge immediately in a discreet manner.

The military judge should then immediately halt the testimony, questioning or argument. No reason should be given on the record at that time as to the reason for halting the proceedings. The military judge should proceed to hold a conference under R.C.M. 802 with the security officer and the parties in order to determine whether there is, in fact, suspected classified

⁷ Although “military judge” is used throughout this section, it should be understood that the same procedures would apply at an Article 32 proceeding, where there is an investigating officer instead of a military judge.

information at issue. As counsel often do not have experience with the classified information at issue, it may well be that they did not intend for the question to evoke a classified answer. In such a case, a simple reminder instruction to the witness to keep his answer unclassified will usually be sufficient.

If there is, indeed, a desire on the part of one of the parties to discuss classified information that has not previously been the subject of a closure hearing under R.C.M 806(b)(2), the military judge should proceed with a 39(a) session outside the presence of the members in order to make the determinations required by R.C.M. 806(b)(2). If the 39(a) session itself is closed, the military judge should be sure to include an unclassified summary of his findings on the unclassified record. Even in the middle of trial, it is necessary to consider reasonable alternatives to the use of the classified information. Generally, it is normally possible for the witness to raise the factual level of his testimony so that the information is more generic and the source is obscured, i.e., provide unclassified testimony.

Finally, all parties at the trial should be aware of the possibility that when members pose questions during a trial that involves classified matters, a question could prompt an answer that is classified. The better practice is to have all written members questions reviewed by the court security officer before they are provided to the judge so that the court security officer can alert the judge of whether the question poses a risk in open court. This allows the judge to remind the witness to answer in an unclassified manner, and to instruct the witness to simply alert the judge if the witness needs to answer with classified information. The court security officer may be able to assist the judge in slight rewording of questions to avoid these issues all together.

CHAPTER 11

Pretrial Agreements

The rules pertaining to pretrial agreements in the military are contained in Rule for Courts-Martial (R.C.M.) 705. Section 0137 of the Manual of the Judge Advocate General (JAGMAN) provides further guidance on pretrial agreements for the Navy and Marine Corps. JAGMAN 0137c provides specific guidance on pretrial agreements in national security designated cases. In all classified information cases involving pretrial agreements, judge advocates should draft pretrial agreements as unclassified documents and strive to keep as much, if not all, of the record of trial unclassified. Even at this relatively late stage of the court-martial process, a goal is to avoid as many logistical issues involved with the handling of classified documents as possible. As with all pretrial agreements, judge advocates must ensure that pretrial agreements in cases involving classified information are clear, precise, and inclusive of all contingencies. Sub rosa agreements are prohibited.

A. Prohibited Terms or Conditions. R.C.M. 705(c)(1) prohibits the inclusion of any term or condition not freely and voluntarily agreed to by the accused. Additionally, a term or condition is not enforceable if it denies the accused of certain unwaivable rights including the right to counsel, the right to due process, the right to challenge the jurisdiction of the court-martial, the right to speedy trial, the right to complete sentencing proceedings, and the right to exercise post trial appellate rights. Although not specifically mentioned in R.C.M. 705(c), any pretrial agreement provision closing the court-martial to the public without complying with *Grunden* and R.C.M. 806(b)(2) infringes on the accused's right to, and the public's interest in, a public trial.

B. Permissible Terms or Conditions. R.C.M. 705(c)(2) discusses terms and conditions that either party may propose for inclusion in a pretrial agreement. Permissible terms or conditions include a promise to enter into a stipulation of fact, a promise to testify as a witness in the trial of another person, a promise to provide restitution, a promise to conform conduct to probation terms, and a promise to waive procedural requirements. Additionally, there are several unique provisions related to pretrial agreements in cases involving classified information. The sample pretrial agreement in Appendix 11-A contains suggested language for these special provisions. The following sections summarize pretrial agreement issues unique to cases with classified information.

1. Pre-Pleading Debrief. Prior to entering pleas, the accused may agree to take part in a debrief that normally includes cooperation during a series of interviews and polygraph examinations. In courts-martial involving classified information, the principal goal of the debrief process is normally to ascertain the extent of the loss and/or compromise and develop a full appreciation for numerous other counterintelligence issues. Provisions providing for such interviews must clearly set forth the scope of the interview, the role of the defense counsel, and the period of time for which the accused agrees to cooperate. Military Rule of Evidence (M.R.E.) 410(a)(4) protects statements made by the accused during this debrief process when the debrief occurs as part of the plea negotiation process. M.R.E. 410 prohibits the use of the accused's statements in a subsequent court-martial proceeding against the accused when the statements are made "in the course of

plea discussions with the convening authority, staff judge advocate, trial counsel or other counsel for the government which do not result in a plea of guilty or result in a plea of guilty later withdrawn.”

2. Pre-Sentencing Debrief. A second option is for the accused to take part in a debrief between the acceptance of the plea and the sentence, i.e., a pre-sentencing debrief. In this scenario, M.R.E. 410 does not protect the statements of the accused from use in a subsequent prosecution since the debrief does not occur during the course of plea discussions. Therefore, a grant of immunity is normally part of a pretrial agreement that includes a pre-sentencing debrief requirement. Except for the applicability of M.R.E. 410, the issues discussed in B.1 apply to pre-sentencing debriefs as well.

3. Post-Sentencing Debrief. A third, and most frequently used option in the court-martial process, is for the accused to take part in a debrief after the sentencing phase of the court-martial, i.e., a post-sentencing debrief. Again, in this scenario, M.R.E. 410 does not protect the statements of the accused from use in a subsequent prosecution. Therefore, a grant of immunity is also normally a part of a pretrial agreement that includes a post-sentencing debrief requirement. Except for the applicability of M.R.E. 410, the issues discussed in B.1 apply to post-sentencing debriefs as well.

4. Stipulation Concerning Classification Level of Information. The accused may stipulate that relevant evidence is classified at a particular level and agree to refrain from objecting to its admissibility at trial. The accused can also agree to refrain from introducing classified information during the court-martial. Although, neither of the above two stipulations represent an adequate substitute for the government’s responsibilities with respect to closing the court-martial pursuant to *Grunden* and R.C.M. 806, both stipulations support the government’s effort to avoid as many logistical burdens associated with a classified record of trial as possible.

5. Agreement Not to Seek Security Clearance. The accused may agree not to seek a security clearance or employment requiring a security clearance for a period of time after the court-martial concludes. See also the discussion of the Smith Amendment in Chapter 12.

C. Approval of Pretrial Agreements in National Security Cases. There is a unique requirement for a pretrial agreement in any case that is designated as a national security case pursuant to JAGMAN 0126. JAGMAN 0137c provides that the national security case designation authority (NSCDA), as the convening authority, must obtain permission from the Secretary of the Navy prior to entering into a written pretrial agreement. The NSCDA request format for permission from the Secretary of the Navy is a priority message or naval correspondence with information copies to the Chief of Naval Operations or Commandant of the Marine Corps, as appropriate, and Office of the Judge Advocate General (Code 17). The request must include the following:

1. The exact text of the proposed pretrial agreement;

2. A statement of the factual background of the offense(s);
3. Information pertaining to the identity of the accused;
4. A summary of the evidence that would be available for introduction at trial before findings or during any sentencing portion of trial by the Government; and
5. A summary of the factors that warrant entry into a pretrial agreement.

The JAGMAN requires that the Secretary of the Navy approve pretrial agreements. Each Secretary of the Navy develops their own process for approving the agreements. For example, a recent Secretary of the Navy required the convening authority to forward negotiating parameters for approval prior to entering negotiations. Code 17 recommends that convening authority staff judge advocates consult with Code 17 and the Secretary of the Navy's Special Assistant for Legal and Legislative Matters in future cases prior to entering into negotiations and inquire whether any current guidance is available on this issue.



Practice Pointer: Obtaining approval for a pretrial agreement is similar to obtaining the assertion of the privilege under M.R.E. 505 - both require personal action by the Secretary of the Navy. Early coordination with Code 17 will facilitate the process.

D. Grants of Immunity. As discussed above in paragraph B., the government has an incentive to grant the accused immunity to encourage cooperation in the pre-sentencing and post-sentencing debrief process. (The government's goal could also include the more traditional pursuit of testimony against a co-accused.) The accused's interest in a grant of immunity is self evident. Additionally, the accused's agreement to support the debrief process can lay the groundwork for a defense argument that the accused warrants a more lenient sentence due to the accused's cooperation. Pursuant to JAGMAN § 0138, "[i]n all cases involving national security or foreign relations of the U.S., the cognizant GCMCA shall forward, in the form prescribed in section 0139, any proposed grant of immunity to OJAG (Code 20, via Code 17) for the purpose of consultation with the Department of Justice." The Department of Defense Instruction that implements the Memorandum of Understanding (MOU) between the Departments of Justice and Defense regarding the investigation and prosecution of certain types of crimes, Annex E, includes a somewhat overlapping but broader consultation requirement at paragraph B.3. under "Supplemental Guidance:"

A proposed grant of immunity in a case involving espionage, subversion, aiding the enemy, sabotage, spying, or violation of rules or statutes concerning classified information or the foreign relations of the United States shall be forwarded to the General Counsel of the Department of Defense for the purpose of consultation with DoJ.

The cognizant Department of Justice Division for both of these regulatory requirements is the National Security Division, Counterespionage Section. JAGMAN §§ 138-140 and

R.C.M. 704 contain detailed discussions of grants of immunity. Contact Code 17 for substantive support and assistance in coordination with the Department of Justice and Department of Defense General Counsel whenever the convening authority is contemplating grants of immunity in a court-martial involving classified information.

E. Providency and Stipulations of Fact. As with any guilty plea, the military judge must craft questions for the accused to ensure the accused has pleaded providently in a guilty plea case with classified information. As classified information cases may involve charges alleging violations of federal statutes charged under Art. 134, UCMJ, preparation for the providence inquiry may be a bit more involved. This is not because the charges are any longer or more complicated, but simply because the federal statutes are not organized in the same manner as offenses defined in the UCMJ. For offenses specifically defined in the UCMJ, the MCM provides the text of the statute, the elements, and an explanation of terms. For federal statutes, there is no similar detail or explanation. The trial counsel, by virtue of an in-depth knowledge of the case, can assist the military judge by proposing questions that focus on the specific facts of the case relevant to each element of the offense. Defense counsel also must be able to anticipate the line of questioning in order to fully prepare clients for the providency process.

Appendix 11-B contains a proposed breakdown of elements and sample specification for assimilating 18 U.S.C. 793, the Federal Espionage Statute, under Article 134. For more discussion on charging 18 U.S.C. 793, see Chapter 8.

APPENDIX 11-A

Sample Pretrial Agreement

DEPARTMENT OF THE NAVY
(GENERAL/SPECIAL) COURT-MARTIAL
NAVY AND MARINE CORPS TRIAL JUDICIARY
() JUDICIAL CIRCUIT

U N I T E D S T A T E S

v.

(NAME OF ACCUSED)

RATE/RANK USN/USMC

MEMORANDUM
OF
PRETRIAL AGREEMENT

(Part I)

I, (Rate/Rank, Name, Service), the accused in a (general/special) court-martial, in exchange for good consideration and after thorough consultation with my defense counsel, do fully understand and agree to the following terms and conditions:

1. I agree to enter pleas of **GUILTY** as indicated below. I do so fully understanding that, unless otherwise specified in Part II of this agreement (the Maximum Sentence Limitation Appendix), the Convening Authority may approve any sentence adjudged by the court-martial, but shall order executed only that sentence which does not exceed the lesser of the sentence contained in Part II of this agreement or the sentence adjudged by this court-martial.

[Note: If the agreement is for the Convening Authority to refer the charges and specifications to a special court-martial vice a general court-martial (i.e., a "Bareback SPCM"), such agreement should be addressed in Part II (the Maximum Sentence Limitation Appendix). See sample provision in Paragraph 6 of the Sentence Limiting Appendix attached.]

2. This agreement (Parts I and II) constitutes all the conditions and understandings of both the government and myself regarding the pleas in this case. There are no other agreements, written or otherwise.

3. I understand that the convening authority in this case may approve and order executed any lawfully adjudged sentence awarded by this court-martial, or any automatic sentence or portion thereof, except as specifically limited by Part II, the sentence limitation portion of this agreement. I also understand that the sentence limitation portion of this agreement addresses, each of the following distinct parts of the sentence that may be adjudged in this case: (1) punitive discharge, (2) confinement and/or restraint, (3) forfeiture and/or fine, (4) reduction in pay grade, and (5) any other lawful punishment that may be adjudged.

FOR OFFICIAL USE ONLY

4. I am satisfied with my defense counsel in all respects and consider (him/her/them) qualified to represent me at this court-martial.

5. I am entering into this agreement freely and voluntarily. Nobody has made any attempt to force or coerce me into making this agreement or into pleading guilty.

6. I have been fully advised by my defense counsel of, and I fully understand and comprehend the meaning and effect of, my guilty pleas and all attendant effects and consequences, including the possibility that I may be processed for administrative discharge from the (United States Navy Navy/Marine Corps). I understand that such an administrative discharge could result in an other than honorable characterization of service, unless otherwise limited by this agreement, even if part or all of the sentence, including a punitive discharge, is suspended or disapproved for any reason.

[Note: If the agreement includes the accused waiving an administrative discharge board, such waiver may be addressed either here or in paragraph 15, infra, the “Specially Negotiated Provisions,” at the discretion/election of the parties. See sample provision in “Specially Negotiated Provisions” section, infra].

7. I understand that I may ask permission to withdraw any of my pleas of guilty at any time before they are actually accepted by the military judge. I also understand that I may ask to withdraw any of my pleas of guilty after they have been accepted, but before sentence is announced, and the military judge may, at his/her discretion, permit me to do so.

8. I understand that this pretrial agreement may become null and void, and the convening authority can withdraw from this agreement, in the event that any of the following occur:

(1) I fail to plead guilty as required by this agreement;

(2) The court refuses to accept any of my pleas of guilty;

(3) The court sets aside any of my pleas of guilty for whatever reason, including upon my request, before sentence is announced;

(4) I fail to satisfy any material term of this agreement; or

(5) I fail to plead guilty as required by this agreement at a rehearing should one occur.

9. I understand that if this agreement becomes null and void, then my offer to plead guilty and enter into this agreement cannot be used against me in any way in determining whether I am guilty or not guilty of the charges alleged against me at this court-martial.

10. I understand that if the approved sentence includes a punitive discharge or confinement in excess of 90 days (or 3 months), whether the sentence is suspended or not, Article 58a of the UCMJ and § 0152 of the JAGMAN require that I suffer automatic administrative reduction in pay grade to the lowest enlisted paygrade, E-1, unless the Convening Authority takes action to remit or suspend the automatic reduction.

FOR OFFICIAL USE ONLY

11. I understand that if the adjudged sentence includes either a punitive discharge and confinement, or confinement in excess of six months, whether the sentence is suspended or not, Article 58b of the UCMJ requires the automatic imposition of forfeitures of (2/3 pay per month) (all pay and allowances) due during any period of confinement awarded, unless the Convening Authority takes action to waive or defer the automatic forfeiture provision. Forfeitures, whether adjudged or automatic, take effect upon the convening authority's action in this case or 14 days after sentence is adjudged, whichever is earlier. I understand that I may request in writing that the convening authority defer execution of forfeitures until the convening authority takes action in this case. I also understand that I may request that the convening authority waive automatic forfeitures for a period up to six (6) months from the date of the convening authority's action. Finally, I understand that if I am held in confinement beyond my End of Active Obligated Service (EAOS) date, then I will not receive any pay or allowances by operation of law, regardless of the terms of this agreement.

12. I understand that should I commit any misconduct (i.e., any act or omission in violation of the UCMJ or any punitive statute of the United States Code. which constitutes a material breach of this agreement) after the signing of this pretrial agreement but before the date of trial, such misconduct may be the basis for the convening authority to unilaterally withdraw from the pretrial agreement, rendering the entire agreement null and void. I further understand that if I commit misconduct after the date of trial, but before the date of the convening authority's action, the convening authority may, after first complying with notice and hearing requirements consistent with Article 72, UCMJ and R.C.M. 1109, withdraw from the sentence limitation provisions of this agreement. Should the Convening Authority withdraw from the sentence limitation provisions of this agreement based on misconduct occurring after the date of trial but before action is taken in my case, I understand that any provisions in the pretrial agreement relating to suspension of any aspect of my sentence would become null and void in all respects, and that the entire sentence adjudged at my court-martial may be approved and imposed upon me.

13. I also understand that should I commit any misconduct after the date of the Convening Authority's action, but before I have completed serving the entire sentence (including any period of suspension or probation) as finally approved and executed, the Convening Authority may, after complying with the procedures set forth in R.C.M. 1109, vacate any periods of suspension agreed to in this pretrial agreement or as otherwise approved by the Convening Authority, and that previously suspended portion of my sentence could be imposed upon me.

14. I understand that I may be placed on appellate leave in a no pay status under the provisions of Article 76a of the UCMJ, notwithstanding any provision regarding forfeitures or fines in Part II of this agreement, if the sentence, as approved, includes an unsuspended punitive discharge. (Furthermore, I agree that, should a punitive discharge be adjudged, I will submit, within ____ days from the date of the conclusion of my trial, a written request to be placed on appellate leave without pay or allowances.)

15. Additional Provisions.

As consideration for this agreement, and after having fully discussed the issue with my defense counsel:

[Examples of Common Specially Negotiated/Alternative Provisions:]

FOR OFFICIAL USE ONLY

[**Elect trial by Military Judge alone**]

I agree to request and elect trial and sentencing by military judge alone, and waive my right to a trial by members, including enlisted members.

[**Article 32 Waiver as part of agreement/GCM only**]

I agree to waive my right to an Article 32, UCMJ, Pretrial Investigation. I fully understand the nature and purpose of an Article 32, UCMJ, Pretrial Investigation, and the rights that I would have at such a hearing. I understand that upon acceptance of this agreement, the charge(s) and specification(s) may be referred to trial by general court-martial without an Article 32, UCMJ, investigation or hearing.

[** "Bareback" Specials – The Bareback" Special provision is located (and should always be placed in) Paragraph 6 of Part II of the agreement (the Maximum Sentence Appendix) so that the military judge is not on notice of what the sentence maximum will be.]

[**Withdraw language to which accused pled Not Guilty**]

I understand and agree that, in return for my plea(s) of guilty, and following the military judge's acceptance of my plea(s) as set forth below, the convening authority will withdraw the language and/or charges and specifications to which I have pled not guilty. After announcement of the sentence by the military judge, the withdrawn language and/or charges and specifications will be dismissed by the convening authority with/without prejudice.

[**Government going forward on not guilty pleas**]

I understand and agree that the convening authority, through the assigned Trial Counsel, may go forward on the charges and/or language to which I have entered pleas of not guilty.

[**Waive Administrative Discharge Board**]

I agree to waive any administrative discharge board, that is based on any act or omission reflected in the charge(s) and specification(s) that is/are the subject of this Agreement. I understand that any administrative discharge will be characterized in accordance with service regulations, and may be under other than honorable conditions. I fully understand the nature and purpose of an Administrative Discharge Board, and the rights that I would have at such a Board.

[**RESTITUTION: Select from one of the following 3 paragraphs**]

[**1. Has means to make restitution prior to date of trial**]

I agree to make restitution by [cashier's check/money order] in the amount of \$_____, made payable to the economic victim of my misconduct, (Name(s) of Victim(s)), prior to the date of trial. I expressly represent that I will have the economic means to make restitution prior to the date of trial. The [cashier's check/money order] will be delivered to the trial counsel at least one day prior to the date of trial. I fully understand that failure on my part to meet this obligation may serve as the basis for the Convening Authority to withdraw from this agreement, rendering it null and void.

FOR OFFICIAL USE ONLY

[OR]

11-A-5

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

[**2. Will have means to make restitution prior to a certain date**]

I agree to make restitution by [cashier's check/money order] in the amount of \$_____, made payable to the economic victim of my misconduct, (Names(s) of Victim(s)) by DD Month YYYY. I expressly represent that I will have the economic means to make restitution by DD Month YYYY and understand that my paying restitution to the victim is a material term of this agreement. The [cashier's check/money order] will be delivered to the trial counsel or staff judge advocate on that date. I fully understand that failure on my part to meet this obligation may serve as the basis for the Convening Authority to withdraw from this agreement, rendering it null and void, or may serve as the basis for the Convening Authority to vacate any or all previously suspended portions of my sentence, causing me to have to serve that previously suspended sentence.

[OR]

[**3. Make restitution in installments**]

I agree to make restitution in the amount of \$_____, to the economic victim of my misconduct, (Name(s) of Victim(s)), by DD Month YYYY. I expressly represent that I will have the economic means to make full restitution by DD Month YYYY. I will provide the trial counsel or staff judge advocate with a [cashier's check/money order] made payable to (Name(s) of Victim(s)), no later than the second working day following the payday on the 1st and 15th of each month, in the amount of \$_____. These partial payments will begin on DD Month YYYY and will be completed by DD Month YYYY. I fully understand that failure on my part to meet this obligation may serve as the basis for the Convening Authority to withdraw from this agreement, rendering it null and void, or may serve as the basis for the Convening Authority to vacate any or all previously suspended portions of my sentence, causing me to have to serve that previously suspended sentence.

[**Testify W/Grant of Immunity in another case**]

If I am provided a grant of testimonial immunity, I agree to testify truthfully if called as a witness in the case of United States v. _____ pertaining to my involvement in or knowledge of _____. I further agree to fully and or any other punitive, judicial, or administrative proceeding requested of my by the Convening Authority truthfully cooperate in the court-martial process, to include interviews with appropriate law enforcement authorities and the trial and defense counsel involved in the case, as well as any other reasonable request made of me.

[**Testify W/O Grant of Immunity in another case**]

Even if I am not provided a grant of testimonial immunity, I agree to testify truthfully if called as a witness in the case of United States v. _____ or any other punitive, judicial, or administrative proceeding requested of my by the Convening Authority. I further agree to fully and truthfully cooperate in the court-martial process, to include interviews with appropriate law

FOR OFFICIAL USE ONLY

enforcement authorities and the trial and defense counsel involved in the case, as well as any other reasonable request made of me.

[**Stipulation of Fact**]

[**Stipulation is an appendix to the Agreement**]

I agree to enter into the Stipulation of Fact contained in Appendix I. I agree that the facts contained therein are true and may not be contradicted by either side. I further agree not to object to the stipulation's admission during the providence inquiry/on the merits/ and/or during the pre-sentencing proceeding.

[Stipulations of Fact are common in classified information cases. They are often used to establish the admissibility of the Classification Reviews]

[**Stipulation to be agreed upon after PTA is signed**]

I agree to enter into a stipulation of fact, which describes the facts and circumstances surrounding the offenses to which I am pleading guilty. I understand that the failure of the parties to reach a mutually agreed upon stipulation of fact may result in either side withdrawing from this agreement. I further agree not to object to the mutually agreed upon stipulation's admission during the providence inquiry/on the merits/ and/or during the pre-sentencing proceeding.

[**Witness Considerations**]

[**Call certain witnesses only**]

I intend to request the presence of _____ [as a witness/as witnesses] at my court-martial. Provided that the convening authority agrees to produce these witnesses, I will not request any other witnesses. This provision has not interfered with my selection of witnesses or in presenting a complete [defense/case in extenuation and mitigation].

[**Call no witness or call only local witnesses**]

I agree not to request, at government expense, the presence of any witness located (out of the area)(outside a 100-mile radius of _____). This provision does not interfere with my ability to present an effective and complete [defense/case in extenuation and mitigation]. I intend to use alternative means to present this material. (The government specifically agrees not to object to the admission into evidence of written statements in extenuation and mitigation from witnesses located (out of the area)(outside a 100-mile radius of _____).

[**Stipulation of Testimony**]

FOR OFFICIAL USE ONLY

I agree to stipulate to the testimony of the following witnesses:_____. I understand that the stipulation does not admit the truth of the testimony, which may be attacked, contradicted or explained in the same way as any other testimony.

[**Trial Date Consideration**]

I agree, and am fully prepared, to go to trial and offer to go to trial no later than _____. I understand that I will not be deemed to have breached this agreement if the judiciary cannot schedule my trial by this specific date.

[**Motion Consideration – the specific motions waived need to be specified – the language “all waivable motions” is unacceptable**]

I agree not to raise a motion pursuant to R.C.M. _____ to _____. I have not been compelled to waive my right to due process, the right to challenge the jurisdiction of the court-martial, the right to a speedy trial, the right to raise the issue of unlawful command influence, or any other motion that cannot be waived.

[** Agreement Not to Object to Evidence Offered **]

I (and the Government) agree not to object to [service record documents, chain-of-custody documents, lab reports, etc...] being offered into evidence on the merits (in sentencing) on the basis of (hearsay, authenticity, etc.).

[**Agreement on Admissibility of Classification Reviews**]

FOR OFFICIAL USE ONLY

I agree to the admissibility, for any and all purposes, of any and all classification reviews and related affidavits of classified information of the loss or compromise of classified information pertaining to my case. I will not object to the assertion of the classified information privilege, M.R.E. 505, over the classified information pertaining to my case. I will not object to the military judge's consideration of the classification reviews and related affidavits, when formulating an appropriate sentence in this case. My defense counsel and I have been given the opportunity to review all classification review affidavits and concur that the matters therein are appropriate matters for consideration under R.C.M. 1001. I acknowledge I have had an adequate opportunity to consult with, and have so consulted with my defense counsel, regarding the meaning and ramifications of this term of the pretrial agreement.

(Remove loss/compromise language if case does not concern the loss/compromise of classified information but yet some evidence is classified)

[Agreement to Unclassified Forum and Record of Trial**]**

I agree that I will not seek to admit into evidence any classified information during any court proceeding of my case. By this paragraph, it is the parties' intent that all sessions of the court will be conducted in an unclassified forum. Additionally, it is the parties' intent that the record of trial will contain no classified information. As used in this agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 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 Sections 1.2 and 1.3(e) of Executive Order 12958, or under any other Executive order or statute that requires protection for such information in the interest of national security. I acknowledge I have had an adequate opportunity to consult with, and have so consulted with my defense counsel, regarding the meaning and ramifications of this term of the pretrial agreement.

[Role of SECNAV in designated National Security Cases**]**

I have been fully advised by my defense counsel that my case has been designated a National Security Case under JAGMAN §0126. As required by JAGMAN §0137, the Convening Authority must request permission from the Secretary of the Navy to enter into this pretrial agreement. If the Convening Authority is unable to obtain permission from the Secretary of the Navy to enter into this pretrial agreement, then the provisions of this pretrial agreement will become null and void.

[Will not seek security clearance- Also in post-trial immunity section**]**

I also agree as further consideration for this agreement that I will not seek to obtain a national security clearance or access to classified information for a period of 10 years. I further agree that I will not seek employment requiring a national security clearance or requiring access to classified information for 10 years. As used in this agreement, classified information is marked or unmarked classified information, including oral communications, that is classified

FOR OFFICIAL USE ONLY

under the standards of Executive Order 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 Sections 1.2 and 1.3(e) of Executive Order 12958, or under any other Executive order or statute that requires protection for such information in the interest of national security. Should I attempt to seek employment requiring a national security clearance or requiring access to classified information at any time after signing this agreement, but before I have completed serving the entire sentence (including any period of suspension or probation) as finally approved and executed, the convening authority may consider this misconduct and either unilaterally withdraw from the agreement, withdraw from the sentencing limitation provisions of the agreement, or vacate the suspended portions of punishment as allowed pursuant to the relevant stage of the case when the convening authority discovers the misconduct and takes action. I acknowledge I have had an adequate opportunity to consult with, and have so consulted with my defense counsel, regarding the meaning and ramifications of this term of the pretrial agreement.

[** Conditional Plea(s) -- Only for Case Dispositive Issues **]

I agree, upon written consent of the Government and approval of the military judge, to enter a conditional plea of guilty in writing as to (list applicable Charges and Specifications), preserving the right, on further review or appeal, to review of any adverse determination on my motion (specify nature of the motion). I understand that if I prevail on further review or appeal, I will be allowed to withdraw my conditional plea(s) of guilty in accordance with Rule for Courts-Martial 910(a)(2).

[** Confessional Stipulation **]

I agree to enter into a confessional stipulation of fact in writing as to all elements of (list applicable Charge(s) and Specification(s)) to which I have entered pleas of not guilty. I understand that a confessional stipulation is tantamount to a guilty plea when it establishes directly, or by reasonable inference, every element of a charged offense, and when my counsel and I do not present any evidence to contest any potential remaining issue(s) on the merits of my case. I also understand that this confessional stipulation will relieve the Government and the trial counsel of the burden of proving my guilt beyond a reasonable doubt as to this charge and Specification (these charges and Specifications) and that I may be found guilty of this offense/these offenses based solely upon this stipulation and be subjected to the punishment(s) authorized.

[** Agreement to Cooperate with Debriefing and Polygraph Prior to Entry of Pleas (MRE 410 protection)**]

I understand that following approval of this pretrial agreement by the Convening Authority, but before I enter the guilty pleas set out in this agreement:

(1) I agree to submit to and cooperate in all debriefings, to include interviews and polygraph examinations, requested by the investigators specified by the Convening Authority, which interviews and polygraph examinations shall concern the loss or disclosure of any classified information for which I have knowledge or in any matter which my cooperation may be relevant. I understand that my cooperation shall extend to disclosing my knowledge of the actual or potential compromise of classified material or information by my or by any person or

FOR OFFICIAL USE ONLY

entity whatsoever. I also understand that these debriefings may also include questions typically asked in a polygraph examination for ascertaining if a person may continue to hold a Top Secret security clearance;

(2) I agree to answer all questions fully and completely, both orally and, where requested, in writing, to the best of my knowledge and belief. I will submit to as many debriefings, to include interviews and polygraph examinations, at such times and places as may be specified by the Convening Authority, as are necessary in the view of the Convening Authority, to ensure that I have made a full and truthful disclosure as to the above matters. I understand that my cooperation will extend for a period of 24 months from the date sentence is imposed on me;

(3) I agree to fully cooperate with investigators to resolve any issues arising from polygraph examination results indicating that I have provided deceptive or "no opinion" responses to any questions. I understand that such cooperation may extend to additional debriefings, to include interviews and polygraph examinations. I also understand that if I continue to provide deceptive or "no opinion" responses to any questions, based on the opinion of the polygraph examiner, that opinion and the responses shall be conveyed to the Convening Authority. I further understand that the Convening Authority may unilaterally withdraw from the pretrial agreement, rendering the entire agreement null and void, after considering all relevant information, including evidence uncovered by the ongoing investigation, other misconduct related to the theft, mishandling, and/or compromise of classified information that I admit during the interviews and/or polygraph examinations, and the examiner's opinion that I provided deceptive or "no opinion" responses to any questions and the basis for that opinion;

(4) I understand that any communication made by me during any debriefing, interview or polygraph examination conducted pursuant to this paragraph of this pretrial agreement are statements made in the course of plea discussions under Military Rule of Evidence 410. I understand that these statements are not admissible at court-martial, except as specifically provided for in Military Rule of Evidence 410.

(5) I agree to complete the polygraph rights waiver form pursuant to DoD Directive 5210.48 and DoD Regulation 5210.48-R prior to taking a polygraph examination referred to above. Although my only obligation under this provision is to complete the polygraph rights waiver form, I understand that should I not give my consent to the polygraph on the rights waiver form, my failure to cooperate may permit the Convening Authority to unilaterally withdraw from this pretrial agreement.

(6) I understand that my defense counsel shall be provided notice and a reasonable opportunity to be present during interviews and at the time of polygraph examinations required by this agreement, but will not be in the examination room during the polygraph examinations referred to above.

[**Agreement to Cooperate with Debriefing and Polygraph After Entry of Pleas, but Before Sentencing (Testimonial Immunity)**]

1. I agree, along with the Government, to request that sentencing in my case be delayed for sixty (60) days after the entry of pleas in order to conduct post-provency debriefings, to include interviews and polygraph examinations. I agree that this delay will be excluded from

FOR OFFICIAL USE ONLY

government accountability for purposes of a speedy trial. I further understand that I will be granted testimonial immunity and given an order to cooperate completely with those federal law enforcement authorities and other federal government officials as may be designated by the Convening Authority in any matter as to which my cooperation may be relevant. Following my receipt of testimonial immunity and the order by the Convening Authority referred to above:

(1) I agree to submit to and cooperate in all debriefings, to include interviews and polygraph examinations, requested by the investigators specified by the Convening Authority, which interviews and polygraph examinations shall concern the loss or disclosure of any classified information for which I have knowledge or in any matter which my cooperation may be relevant. I understand that my cooperation shall extend to disclosing my knowledge of the actual or potential compromise of classified material or information by my or by any person or entity whatsoever. I also understand that these debriefings may also include questions typically asked in a polygraph examination for ascertaining if a person may continue to hold a Top Secret security clearance;

(2) I agree to answer all questions fully and completely, both orally and, where requested, in writing, to the best of my knowledge and belief. I will submit to as many debriefings, to include interviews and polygraph examinations, at such times and places as may be specified by the Convening Authority, as are necessary in the view of the Convening Authority, to ensure that I have made a full and truthful disclosure as to the above matters;

(3) I agree to fully cooperate with investigators to resolve any issues arising from polygraph examination results indicating that I have provided deceptive or "no opinion" responses to any questions. I understand that such cooperation may extend to additional debriefings, to include interviews and polygraph examinations. I also understand that if I continue to provide deceptive or "no opinion" responses to any questions, based on the opinion of the polygraph examiner, that opinion and the responses shall be conveyed to the Convening Authority. I further understand that the Convening Authority may unilaterally withdraw from the pretrial agreement, rendering the entire agreement null and void, after considering all relevant information, including evidence uncovered by the ongoing investigation, other misconduct related to the theft, mishandling, and/or compromise of classified information admitted to by me in the interviews and/or polygraph examinations, and the examiner's opinion that I provided deceptive or "no opinion" responses to any questions and the basis of that opinion;

(4) My defense counsel shall be provided notice and a reasonable opportunity to be present for each and every interview and polygraph examination, but shall not be in the polygraph examination room itself;

(5) I understand that the Convening Authority shall provide me with a grant of testimonial immunity for any information I provide to government agents during debriefings, including interviews and polygraph examinations, conducted pursuant to this agreement;

(6) I agree to complete the polygraph rights waiver form pursuant to DoD Directive 5210.48 and DoD Regulation 5210.48-R prior to taking a polygraph examination referred to above. Although my only obligation under this provision is to complete the polygraph rights waiver form, I understand that should I not give my consent to the polygraph on the rights waiver form, I still may be found in violation of a different portion of this agreement because of my failure to cooperate. I also understand that because of the grant of immunity I will be given

FOR OFFICIAL USE ONLY

by the convening authority, I am not able to invoke the privilege against self-incrimination provided for on the polygraph rights waiver form. I understand that though I may have the right to consult with counsel as provided for on the polygraph rights waiver form, I also understand that I remain obligated under this agreement to cooperate fully and completely in answering all questions put to me during any polygraph that I am administered as part of this agreement.

[**Agreement to Cooperate with Debriefing and Polygraph After Sentencing (Testimonial Immunity)**]

1. I understand that after trial by court-martial, I will be granted testimonial immunity and given an order to cooperate completely with those federal law enforcement authorities and other federal government officials as may be designated by the Convening Authority in any matter as to which my cooperation may be relevant. Following my receipt of testimonial immunity and the order by the Convening Authority referred to above:

(1) I agree to submit to and cooperate in all debriefings, to include interviews and polygraph examinations, requested by the investigators specified by the Convening Authority, which interviews and polygraph examinations shall concern the loss or disclosure of any classified information for which I have knowledge or in any matter which my cooperation may be relevant. I understand that my cooperation shall extend to disclosing my knowledge of the actual or potential compromise of classified material or information by my or by any person or entity whatsoever. I also understand that these debriefings may also include questions typically asked in a polygraph examination for ascertaining if a person may continue to hold a Top Secret security clearance;

(2) I agree to answer all questions fully and completely, both orally and, where requested, in writing, to the best of my knowledge and belief. I will submit to as many debriefings, to include interviews and polygraph examinations, at such times and places as may be specified by the Convening Authority, as are necessary in the view of the Convening Authority, to ensure that I have made a full and truthful disclosure as to the above matters. I understand that my cooperation will extend for a period of 24 months from the date sentence is imposed on me;

(3) I agree to fully cooperate with investigators to resolve any issues arising from polygraph examination results indicating that I have provided deceptive or "no opinion" responses to any questions. I understand that such cooperation may extend to additional debriefings, to include interviews and polygraph examinations. I also understand that if I continue to provide deceptive or "no opinion" responses to any questions, based on the opinion of the polygraph examiner, that opinion and the responses shall be conveyed to the Convening Authority;

(4) I understand that if information is given to the Convening Authority indicating that I have violated the provisions of subparagraphs "(1)", "(2)", or "(3)" of paragraph "1" of this agreement after trial but prior to his having taken action on the record of trial, the Convening Authority may, after first complying with notice and hearing requirements consistent with Article 72, UCMJ and R.C.M. 1109, withdraw from the sentence limitation provisions of this agreement. I further understand that should the Convening Authority withdraw from the sentence limitation provisions of this agreement that any provisions in the pretrial agreement relating to suspension of any aspect of my sentence would become null and void in all respects,

FOR OFFICIAL USE ONLY

and that the entire sentence adjudged at my court-martial may be approved and imposed upon me;

(5) I understand that if information is given to the Convening Authority that I have violated the provisions of subparagraphs “(1)”, “(2)”, or “(3)” of paragraph “1” after the date of the Convening Authority's action, but before I have completed serving the entire sentence (including any period of suspension or probation) as finally approved and executed, the Convening Authority may, after complying with the procedures set forth in R.C.M. 1109, vacate any periods of suspension agreed to in this pretrial agreement or as otherwise approved by the Convening Authority. I understand that should the convening authority take such action, the previously suspended portion of my sentence could be imposed upon me;

(6) I understand that I will be entitled to present evidence based on a polygraph examination from an independent source if, during a hearing conducted pursuant to subparagraphs “(4)” or “(5)” of paragraph “1,” the Convening Authority wants to consider the results of polygraph examinations, including a polygraph examiner's opinion that I provided “no response” or deceptive responses and the basis for those opinions. I understand that if I elect to have such an examination, the Convening Authority has agreed to pay for one (1) alternative polygraph examination from an independent source. I also understand that the independent source polygrapher must hold, or be able to gain, the necessary security clearance in accordance with current regulations. I agree that the results and charts of any independent polygraph examination paid for by the Convening Authority will be forwarded to the Convening Authority for his review;

(7) I understand that the Convening Authority shall provide me with a grant of testimonial immunity for any information I provide to government agents during debriefings, including interviews and polygraph examinations, conducted pursuant to this agreement;

(8) I agree to complete the polygraph rights waiver form pursuant to DoD Directive 5210.48 and DoD Regulation 5210.48-R prior to taking a polygraph examination referred to above. Although my only obligation under this provision is to complete the polygraph rights waiver form, I understand that should I not give my consent to the polygraph on the rights waiver form, I still may be found in violation of a different portion of this agreement because of my failure to cooperate. I also understand that because of the grant of immunity I will be given by the convening authority, I am not able to invoke the privilege against self-incrimination provided for on the polygraph rights waiver form. I understand that though I may have the right to consult with counsel as provided for on the polygraph rights waiver form, I also understand that I remain obligated under this agreement to cooperate fully and completely in answering all questions put to me during any polygraph that I am administered as part of this agreement.

I understand that I have a continuing obligation to safeguard classified information, including the information I previously disclosed, lost, or compromised.

PLEAS OF THE ACCUSED

CHARGE

PLEAS

11-A-14

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

Charge I: Violation of Article _____ GUILTY/NOT GUILTY
Specification____: Language of Spec. GUILTY/NOT GUILTY

[** Examples of Pleas w/exceptions and substitutions**]

Spec __: Unauthorized absence terminated by apprehension. Guilty, except for the words “terminated by apprehension”; of the excepted words, Not Guilty; of the Specification as excepted, Guilty.

Spec: __: Between 22 Jun and 29 Jun 03, at an unknown location, wrongfully use cocaine. Guilty, except for the words “unknown location” substituting therefor the words “Norfolk, Virginia”; of the excepted words, Not Guilty; of the substituted words, Guilty; of the Specification as excepted and substituted, Guilty.

Charge __: Violation of Art 123a Not Guilty, but guilty of a violation of Article 134.

Spec __: Uttering checks w/out sufficient funds Not Guilty, but guilty to the LIO of dishonorable failure to maintain funds.

By my signature below I acknowledge that I have read this agreement completely, discussed it with my counsel, understand it in all respects, and am prepared to abide by its terms.

(Rate/Rank, Name, Service), Accused Date

(Rank, Name, Service), Defense Counsel Date

11-A-15

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

The foregoing pretrial agreement is approved, including the sentence limitation portion of this agreement.

_____ Date
(Rank, Name, Service of Convening Authority)
(Title of Convening Authority)

DEPARTMENT OF THE NAVY
(GENERAL/SPECIAL) COURT-MARTIAL
NAVY AND MARINE CORPS TRIAL JUDICIARY
() JUDICIAL CIRCUIT

U N I T E D S T A T E S

v.

(NAME OF ACCUSED)
RATE/RANK USN/USMC

MEMORANDUM
OF
PRETRIAL AGREEMENT:
(Part II)
SENTENCE LIMITATIONS

11-A-16

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

The convening authority in this case may approve and order executed any lawfully adjudged sentence awarded by this court-martial, or any automatic sentence or portion thereof, except as specifically limited below:

[PARAGRAPH 1. Punitive Discharge]

1. Punitive Discharge: May be approved as adjudged.

[OR – Mitigate DD to BCD – GCMs only]

1. Punitive Discharge: May be approved as adjudged. However, if a dishonorable discharge is adjudged, the convening authority agrees to approve only a bad conduct discharge.

[OR – Disapprove any punitive discharge]

1. Punitive Discharge: If adjudged, any punitive discharge will be disapproved.

[OR – Suspend the discharge for specified number of months after CA's action or other specified event]

1. Punitive Discharge: May be approved as adjudged. However, if a punitive discharge is adjudged, it will be suspended (for a period of _____ months/years from the date of trial/the convening authority's action)(until a specific date or event, such as EAOS or ADSEP completion)), at which time, unless sooner vacated, the suspended punitive discharge will be remitted without further action.

[PARAGRAPH 2: Confinement]

2. Confinement: May be approved as adjudged.

[OR – Disapprove Confinement]

2. Confinement: If adjudged, any confinement will be disapproved.

[OR – Place a cap on confinement with the excess suspended]

FOR OFFICIAL USE ONLY

2. Confinement: May be approved as adjudged. However, all confinement in excess of ____ days/months/years will be suspended for the period of _____months/years from the date of trial/date of the convening authority's action, at which time, unless sooner vacated, the suspended portion will be remitted without further action. This Agreement constitutes my request for, and the convening authority's approval of, deferment of all confinement suspended pursuant to the terms of this Agreement and deferment for the days of "good time" (as defined by SECNAVINST 1640.9B) that I might earn while in confinement prior to the convening authority taking action on the sentence. The period of deferment will run from the date of sentencing until the date the convening authority acts on the sentence.

[OR – Place a cap on confinement with the excess suspended only if a punitive discharge is awarded and accused requests appellate leave]

2. Confinement: May be approved as adjudged. However, if a punitive discharge is adjudged and I request voluntary appellate leave, all confinement in excess of ____days/months/years/time served will be suspended for a period of _____months/years from the date of trial/date of the convening authority's action, at which time, unless sooner vacated, the suspended portion will be remitted without further action. This Agreement constitutes my request for, and the convening authority's approval of, deferment of all confinement suspended pursuant to the terms of this Agreement and deferment for the days of "good time" (as defined by SECNAVINST 1640.9B) that I might earn while in confinement prior to the convening authority taking action on the sentence. The period of deferment will run from the date of sentencing until the date the convening authority acts on the sentence.

[Paragraph 3. Forfeiture and Fines]

3. Forfeiture or Fines: May be approved as adjudged.

[Or - Disapproval all adjudged and defer/waive all automatic]

a. Adjudged Forfeiture: All adjudged forfeiture will be disapproved.

b. Automatic Forfeiture: Automatic forfeiture (in the amount of \$_____ per month) will be deferred provided that the accused establishes and maintains a dependent's allotment in the total amount of the deferred forfeiture amount during the entire period of deferment. This Agreement constitutes the accused' request for, and the convening authority's approval of, deferment of automatic forfeiture (in the amount of \$_____ per month) pursuant to Article 58b(a)(1), UCMJ. The period of deferment will run from the date automatic forfeiture would otherwise become effective under Article 58b(a)(1), UCMJ, until the date the convening authority acts on the Sentence. Further, this Agreement constitutes the accused' request for, and the convening authority's approval of, waiver of automatic forfeiture (in the amount of \$ _____ per month). The period of waiver will run from the date the convening authority takes action on the sentence for six months. The deferred and waived forfeiture shall be paid to _____, who is my dependent.

11-A-18

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

c. Fines: If adjudged, the fine will be disapproved.

[OR - Suspend adjudged and defer/waive automatic]

a. Adjudged Forfeiture: May be approved as adjudged, however adjudged forfeiture (in the amount of \$_____ pay per month for _____ months) will be suspended for _____ months from the date of the convening authority's action, at which time, unless sooner vacated, all suspended adjudged forfeiture will be remitted without further action. This Agreement constitutes the accused' request for, and the convening authority's approval of, deferment of all adjudged forfeiture (in the amount of \$_____ pay per month for _____ months), which are to be suspended pursuant to the terms of this Agreement and would otherwise become effective under Article 57(a)(1), UCMJ. The period of deferment will run from the date adjudged forfeiture would otherwise become effective until the date of the convening authority's action.

b. Automatic Forfeiture: Automatic forfeiture (in the amount of \$ _____ per month) will be deferred provided that the accused establishes and maintains a dependent's allotment in the total amount of the deferred forfeiture amount during the entire period of deferment. This Agreement constitutes the accused' request for, and the convening authority's approval of, deferment of automatic forfeiture (in the amount of \$ _____ per month) pursuant to Article 58b(a)(1), UCMJ. The period of deferment will run from the date automatic forfeiture would otherwise become effective under Article 58b(a)(1), UCMJ, until the date the convening authority acts on the sentence. Further, this Agreement constitutes the accused' request for, and the convening authority's approval of, waiver of automatic forfeiture (in the amount of \$ _____ per month). The period of waiver will run from the date of the convening authority's action and shall not exceed six (6) months. The deferred and waived forfeiture shall be paid to _____, who is my dependent.

[or, Automatic Forfeiture not impacted by the agreement]

b. Automatic Forfeiture: I understand that this agreement does not affect automatic forfeiture of pay and allowances, which may be imposed in accordance with Article 58b, UCMJ.

c. Fines: May be approved as adjudged; however, the adjudged fine will be suspended for _____ months from the date of the convening authority's action, at which time, unless sooner vacated, the suspended portion of the fine will be remitted without further action.

[OR - fine will be mitigated to forfeiture]

c. Fines: May be approved as adjudged; however, the adjudged fine will be mitigated to forfeiture, which the accused shall pay in the amount of \$_____ pay per month [note: cannot be more than 2/3rds pay per month if SPCM] for _____ months (until the entire amount of the originally adjudged fine has been satisfied).

11-A-19

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

[Paragraph 4. Reduction]

4. Reduction: May be approved as adjudged.

[OR - Disapprove adjudged/remit automatic]

4. Reduction:

a. Adjudged Reduction: May be approved as adjudged, however, any adjudged reduction (below the pay grade of E-____) will be disapproved.

b. Automatic Reduction: The automatic reduction (below the pay grade of E-____) will be remitted.

[OR - Suspend adjudged and automatic]

4. Reduction:

a. Adjudged Reduction: May be approved as adjudged; however, any adjudged reduction (below pay grade ____) will be suspended for _____ months from the date of the convening authority's action, at which time, unless sooner vacated, the suspended reduction will be remitted without further action. This Agreement constitutes the accused' request for, and the convening authority's approval of, deferment of that adjudged reduction which is to be suspended pursuant to the terms of this Agreement and would otherwise become effective under Article 57(a)(1), UCMJ. The period of deferment will run from the date the adjudged reduction would otherwise become effective until the date of the convening authority's action.

FOR OFFICIAL USE ONLY

b. Automatic Reduction: The automatic reduction in pay grade (below pay-grade ____) will be suspended for _____ months from the date of the convening authority's action, at which time, unless sooner vacated, the suspended automatic reduction will be remitted without further action.

[OR - Automatic Reduction not impacted by agreement]

b. Automatic Reduction: I understand that this agreement does not affect automatic reduction in pay grade, which may be imposed in accordance with Article 58a, UCMJ, and Section 0152 of the Manual of the Judge Advocate General (JAGMAN).

[Paragraph 5. Other lawful punishments]

5. Other lawful punishments: May be approved as adjudged.

[OR – Disapprove other lawful punishments]

5. Other lawful punishments: If adjudged, any other lawful punishment will be disapproved.

[OR - Suspend other lawful punishments]

5. Other lawful punishments: May be approved as adjudged, however any [fine, restriction, hard labor without confinement, etc.] will be suspended for _____ months from the date of the convening authority's action, at which time, unless sooner vacated, the suspended portion will be remitted without further action.

[Paragraph 6. “Bareback” Special Provision – Special Courts-Martial Only]

6. I fully understand that, in return for my pleas of guilty as indicated below, the only consideration that I will receive under this agreement is the referral of the charges and specifications in my case to a special court-martial rather than a general court-martial. I also understand that in the event that I fail to plead guilty as indicated in this agreement, or fail to comply with any of the material terms of this agreement, or if the agreement becomes null and void for any reason, then the convening authority is free to convene an Article 32, UCMJ, investigation concerning these charges and, ultimately, to refer all charges and specifications for trial before a general court-martial.

I fully understand, and have discussed with my counsel, how this agreement will affect any sentence that I may be awarded by the court-martial.

FOR OFFICIAL USE ONLY

Accused: _____ Date: _____

(NAME OF ACCUSED)
RATE/RANK USN/USMC

Defense Counsel: _____ Date: _____

Name of Counsel

Rank USN/USMC

The foregoing pretrial agreement is approved.

_____ Date: _____

“by direction”) (Convening authority signature, or signature of authorized individual acting

APPENDIX 11-B

18 U.S.C. 793 Providency & Element Breakdown

Discussion. This Appendix focuses on the federal espionage statute, 18 U.S.C. § 793. Subsections (a) through (f) describe six distinct offenses, each involving the same legal principles and definitions. The text of the statute is provided in enclosure (1). It is from this text that the military judge formulates the providence inquiry.

a. Elements. The statute is rather wordy, in order to foreclose potential loopholes. For example, instead of just referring to “information,” the statute specifies several formats, such as “publication,” “code book,” “sketch,” etc. The statute is also written to expressly cover attempts. However, the text is actually very straightforward when broken down into elements. Enclosure (2) provides a useful guide as to how the text of each subsection may be parsed into elements. It is not intended to be an authoritative source. A sample specification of a section 793(e) offense is provided in Enclosure (3).

b. Definitions. Once the text of the statute is broken down and organized into elements, crafting the providence inquiry becomes a more familiar task. As with any other case, the military judge must explain to the accused the legal definitions of the terms used in the elements. Most of the terms in this statute are self-explanatory, but some require discussion. The following terms are relevant to all offenses under section 793.

(1) National Defense. The information (document, writing, etc.) must relate to the national defense. Note that the statute makes no requirement for the information to be classified. To meet the definition of national defense information, the information must relate to the national defense and not be publicly available. The first prong of the definition, “relating to the national defense,” is fairly broad. It refers to any operations of the military departments and other activities related to national preparedness. The second prong is more limiting. Information that is lawfully accessible to the public, whether or not conveniently accessible, does not meet this definition. In this context, the classification of the information can be relevant. Although not required by the statute, the fact that information is classified shows that the government has taken steps to protect it. It can also show that the accused had knowledge of the protected nature of the information. This may be helpful in the context of the providence inquiry when questioning the accused about his or her knowledge and intent. If the accused can admit that he knew the information was formally classified, and can articulate a reasonable connection to national defense, this element would be satisfied.

(2) Foreign Country. The statute is violated if the information is intended to be used, or merely could be used, to the injury of the United States or to the advantage of a foreign country. First, it should be noted that this is an either/or requirement. The element is satisfied if the information could be used to the advantage of a foreign nation, regardless of injury to the United States. The accused need not have any intent, or even reason to believe, that injury to the United States could result. Second, it is not required that the subject foreign nation be an enemy of the United States. The statute is violated even if the foreign nation is considered an ally. Under some circumstances, that may have a mitigating effect on the sentence, but it is not a defense. In

the context of the providence inquiry, this can be significant, especially in cases arising under sections 793(d) and (e). It may be easier for an accused to admit that the information could be used to the advantage of a foreign country that is an ally, than to admit anything having to do with injury or possible injury to the United States.

18 USCS § 793 (2006)

§ 793. Gathering, transmitting, or losing defense information

(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

(b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

(c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter; or

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or

FOR OFFICIAL USE ONLY

attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense,

(1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or

(2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of its trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer—

Shall be fined under this title or imprisoned not more than ten years, or both.

(g) If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

(h)

(1) Any person convicted of a violation of this section shall forfeit to the United States, irrespective of any provision of State law, any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, from any foreign government, or any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, as the result of such violation. For the purposes of this subsection, the term “State” includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.

(2) The court, in imposing sentence on a defendant for a conviction of a violation of this section, shall order that the defendant forfeit to the United States all property described in paragraph (1) of this subsection.

(3) The provisions of subsections (b), (c), and (e) through (p) of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 ([21 U.S.C. 853 \(b\)](#)), (c), and (e)–(p)) shall apply to—

(A) property subject to forfeiture under this subsection;

(B) any seizure or disposition of such property; and

(C) any administrative or judicial proceeding in relation to such property, if not inconsistent with this subsection.

(4) Notwithstanding section [524 \(c\)](#) of title [28](#), there shall be deposited in the Crime Victims Fund in the Treasury all amounts from the forfeiture of property under this subsection remaining after the payment of expenses for forfeiture and sale authorized by law.

ELEMENTS OF 18 U.S.C. § 793 OFFENSES

793(a)

(1) The accused went upon {entered, flew over, etc.} a vessel {aircraft, fort, etc.} with intent to obtain national defense information;

(2) The vessel {aircraft, fort, etc.} was related to the national defense;

(3) The accused acted with the intent or with reason to believe that information obtained was to be used to the injury of the United States, OR, to the advantage of a foreign country.

793(b)

(1) The accused copied {took, obtained, attempted to take, etc.} a document {sketch, photograph, etc.};

(2) The document {sketch, photograph, etc.} was related to the national defense;

(3) The accused acted with the intent or with reason to believe that the document {sketch, photograph, etc.} was to be used to the injury of the United States or to the advantage of a foreign country.

793(c)

(1) The accused received {obtained, attempted to receive, etc.} from {name of the source} a document {sketch, photograph, etc.};

(2) The document {sketch, photograph, etc.} was related to the national defense;

(3) The accused acted knowing or having reason to believe that the document {sketch, photograph, etc.} had been or would be obtained by any person to the injury of the United States or to the advantage of a foreign country.

793(d)

(1) The accused had lawful possession of {access to, control over, etc.} a document {sketch, photograph, etc.};

FOR OFFICIAL USE ONLY

- (2) The document {sketch, photograph, etc.} was related to the national defense;
- (3) The accused had reason to believe the document {sketch, photograph, etc.} could be used to the injury of the United States or to the advantage of a foreign country;
- (4) The accused willfully communicated {delivered, attempted to deliver, etc.} the document {sketch, photograph, etc.} to {person}, who was not entitled to receive it, **OR**, willfully retains the document {sketch, photograph, etc.} and fails to deliver it on demand to the officer or employee of the United States entitled to receive it.

793(e)

- (1) The accused had unauthorized possession of {access to, control over, etc.} a document {sketch, photograph, etc.};
- (2) The document {sketch, photograph, etc.} was related to the national defense
- (3) The defendant had reason to believe the document {sketch, photograph, etc.} could be used to the injury of the United States or to the advantage of a foreign country;
- (4) The accused willfully communicated {delivered, attempted to deliver, etc.} the document {sketch, photograph, etc.} to {person}, who was not entitled to receive it, **OR**, willfully retains the document {sketch, photograph, etc.} and fails to deliver it to the officer or employee of the United States entitled to receive it.

793(f)

- (1) The accused had authorized possession of {access to, control over, etc.} a document {sketch, photograph, etc.};
- (2) The document {sketch, photograph, etc.} related to the national defense;
- (3) The accused, through gross negligence, permitted the document {sketch, photograph, etc.} to be lost {stolen, destroyed, etc.}, **OR**, having knowledge the document {sketch, photograph, etc.} had been lost {stolen, destroyed, etc.}, failed to make prompt report of such to his superior officer

SAMPLE SPECIFICATION FOR 18 U.S.C. § 793(e)

CHARGE: Violation of the UCMJ, Article 134.

Specification: In that Electrician's Mate First Class _____, U. S. Navy, Navy Submarine Training Center Pacific Detachment San Diego, California, on active duty, did, at or near San Diego, California, on divers occasions between on or about 1 July 20__ and on or about 15 July 20__, having unauthorized possession of documents and material relating to the National Defense, willfully and unlawfully retain said documents and materials and fail to deliver the said documents and materials to the officer or employee of the United States entitled to receive them, in violation of Title 18, United States Code, Section 793(e).

CHAPTER 12

The Sentencing Case

Issues associated with classified information continue during the presentencing stage of a court-martial. The evidence rule for introducing classified information during a presentencing proceeding is unique. Under Military Rule of Evidence (M.R.E.) 505, the standard for admissibility of classified information in sentencing is stricter than for the case on the merits. M.R.E. 505(i) (4)(B) provides that in presentencing proceedings, classified evidence, even if previously found to be relevant and material, is only admissible if there is no unclassified version of the evidence available. Therefore, defense and trial counsel should not assume that the military judge will allow either side to introduce classified evidence during the presentencing stage of a court-martial. If the military judge allows classified evidence during the presentencing stage, the same rules and procedures pertaining to classified information for earlier stages of the court-martial apply.

A. Sentencing Issues in a National Security Case. The government case in aggravation and the defense case in extenuation and mitigation are both limited because court-martial parties, including members, will rarely, if ever, fully understand the true extent and nature of the actual harm to the national security caused by the misconduct. Although the victims in such cases are easy to identify--all U.S. citizens-- the traditional concept of victim impact is challenging because of the difficulty in quantifying and describing the harm. Further, any such evidence is normally classified and subject to M.R.E. 505. Additionally, it is very possible in some cases that, depending on the sensitivity of the evidence, the owner of the classified information will not allow any mention or discussion of their information at any stage of a court-martial. As a result, members may never see the most damaging and sensitive pieces of information passed or mishandled by an accused. Likewise, the owner of classified information may prevent a trial counsel from introducing information in aggravation based on similar sensitivity concerns.

1. Case in Aggravation. In the sentencing stage, the trial counsel can typically argue a theory of general deterrence. In a national security case, the deliberate divulging of secrets is an extremely serious offense against the government and the nation, and as such, arouses intense passion. The compromise of classified material can not only reveal sensitive substantive information, but also betray sources and methods. At the worst, the compromise can place the lives of military personnel and others directly in jeopardy. In either case, the special trust that the government placed in the accused has been violated. The personnel security program makes the protection of classified material a personal responsibility. Trial counsel should emphasize the deterrent effect that a well-publicized punishment of the accused will have on all those with access to classified information.

In developing a case in aggravation, the trial counsel should be prepared to present witnesses to testify about the harm to national security that could result

from the accused's conduct.¹ There is no requirement to demonstrate actual harm, but only to demonstrate the level of harm that could occur. For instance, in *United States v. Weinmann*, the accused admitted to passing a manual on the Tomahawk weapon system to an agent of a foreign government. The government's sentencing case included a stipulation of expected testimony from the Tomahawk Program Manager detailing exactly what type of information and vulnerabilities in the weapon system an adversary could learn from the compromised manual. The government then presented the testimony of a Strike Group Commander (a Rear Admiral) who they qualified as an expert in battle planning and questioned as to what effect a compromised Tomahawk system would have on the planning to attack an enemy Integrated Air Defense System (IADS).

When the compromised information is intelligence information, an official from the intelligence agency concerned would be the best witness to testify about the level of harm to national security. If the accused's actions led to the compromise of sources and methods, that would be an important fact to bring out in aggravation and should be able to be stated in an unclassified manner.² If they are unavailable to provide live testimony, affidavits can be substituted. Code 17 can assist in identifying and obtaining appropriate witnesses and affidavits.

If the accused had a particular duty to safeguard classified information, above and beyond the average service member, that would be an aggravating factor, e.g., the accused was a Top Secret Control Officer. For the average service member, trial counsel can show the special trust provided to the accused by presenting the non-disclosure agreements he signed when first granted access to classified material. In these agreements, the accused recognizes that the government is affording the accused a special trust and acknowledges the severe penalties he may incur if that trust is breached. The agreements also demonstrate that the accused was on notice of both the government's trust and confidence in the accused, and the harm that could result from the compromise of classified material.

Another possible aggravating factor is the accused's knowledge of the importance of the classified information that he disclosed or mishandled. The more it can be shown that the accused was aware of the potential harm that resulting from disclosure, the stronger the case in aggravation. In the *Weinmann* case, the

¹ Note well, though, that a formal damage assessment will not likely be initiated until AFTER the completion of the court-martial when the accused would then be available for debriefing.

² Although the unclassified manner may simply be to put as senior an official as possible on the stand to say "We lost valuable sources and methods," without any other details provided. However, trial counsel can develop a more effective case in aggravation by working diligently with the intelligence agency concerned to develop additional unclassified details about the value and worth of the compromised sources and methods. For example, the number of years it took to develop the source and method, an imprecise valuation of the amount of money it took to develop the particular source (e.g., over 100 million dollars), whether the source or method had to be removed from operation and/or whether or not it could be replaced by other means.

government presented the testimony of one of Weinmann's former instructors who had trained him on the classified information at issue in the case. The instructor testified about the training Weinmann received on the Tomahawk system and about Weinmann's rating, which routinely dealt with the Tomahawk system.

2. Case in Extenuation and Mitigation. The defense has two goals with its sentencing case: mitigate the case in aggravation presented by the government and place an affirmative case in extenuation before the military judge or members

. In preparing to mitigate the harm to the national defense, defense counsel must thoroughly review the government's allegations of harm and ensure it is not overstated. Depending on the facts and circumstances of a particular case, a defense expert may be needed to assist in this review. In addition to reviewing the government's assertions, an expert can also point out ways that the harm can be, or has been, minimized and the impact of the government taking or, more often, not taking any of these measures. To return to the *Weinmann* case by way of example, the defense presented an unclassified stipulation of testimony from the Tomahawk Program Manager that laid out the defense argument on what the Tomahawk manual revealed. Specifically, the defense pointed out what facts were not contained in the manual, such as Tomahawk flight paths, and what areas an adversary would be disappointed to learn were not covered in the manual. This second stipulation by the Program Manager also pointed out that the compromised manual had not been rescinded or revised by the Navy and that the Navy had not taken any steps to mitigate the loss of the manual. Defense cross-examination of the government's battle planning expert confirmed that he was not aware of any promulgated changes in Tomahawk employment tactics as a result of the compromised manual.

In a mishandling case, it is often the case that no compromise occurred, which mitigates any potential harm to the national security. In mishandling cases, the reason why the accused improperly stored or mishandled the information is often an important mitigating factor. For instance, if the accused took the information home to study for rate exams, as often seems to be the case, it can be shown that he had good intentions, although he used improper means. This can be a very effective mitigating factor, especially if the accused has a good record of performance.³

Another way to mitigate the harm to national defense is to demonstrate that the classified information at issue was either available in the public domain or has since been released to the public. Again, this type of inquiry is dependent on the facts of each particular case. It must be emphasized that simply because information is in the public domain, whether a commercial source or an

³ Staff Judge Advocates should urge commanding officers to take such factors into account when deciding whether NJP or court-martial is the appropriate forum for disposition of a mishandling case.

anonymous leak, does not make the information unclassified, nor does it excuse the accused's conduct. Just because information is publicly available does not mean that properly classified information should be afforded a lesser level of protection.⁴

Especially in mishandling cases, defense counsel should review the command's security procedures in light of the requirements of the information security manual, SECNAV M-5510.36. A lax security environment may provide a useful argument in extenuation or mitigation. The command security manager should be interviewed with an eye toward discovering how the command has handled other instances of mishandling, whether more or less serious than the case confronting the accused.

Finally, as in any court-martial, defense counsel can argue such extenuating factors as the accused's youth and inexperience, difficult personal or family circumstances, or dire financial situation. In an espionage case, there may be evidence that the accused was initially misled by aggressive enemy agents. In mishandling or espionage cases, there may be evidence that the defendant had a lack of familiarity with classified material and/or the Intelligence Community.

B. Special Issues in National Security Cases. There are two provisions of federal law that are likely to be implicated in cases involving classified information and that counsel need to be aware of when preparing a sentencing case. One provision, the Hiss Act, is unique to such cases while the other, the Smith Amendment, is implicated by any conviction resulting in more than a year of actual confinement. The Smith Amendment is important to understand in classified information cases because of its potential impact on an accused's security clearance.

1. Hiss Act, 5 U.S.C. § 8312. The Hiss Act states that individuals convicted of specified offenses are not eligible to receive an annuity or retirement pay. All of the offenses relate to national security. The Hiss Act includes three Uniform Code of Military Justice articles: aiding the enemy (104), spying (106), and espionage (106a). Federal offenses listed in the Hiss Act include gathering, transmitting, or losing defense information (18 U.S.C. § 793), gathering or delivering defense information to aid a foreign government (18 U.S.C. § 794), disclosure of classified information (18 U.S.C. § 798), treason (18 U.S.C. § 2381), rebellion or insurrection (18 U.S.C. § 2383), activities affecting armed forces generally (18 U.S.C. 2387), activities affecting armed forces during war (18 U.S.C. § 2388), recruiting for service against the United States (18 U.S.C. § 2389), and enlistment to serve against the United States (18 U.S.C. § 2390). The offense within the purview of the Hiss Act that is most often charged in courts-martial is 18 U.S.C. § 793: gathering, transmitting, or losing defense information.

⁴ Paragraph 4-12 of SECNAV M-5510.36 provides the mechanism by which someone in possession of classified information that they believe is improperly or no longer classified can challenge the classification of information. Defense counsel should carefully consider the impact of using this procedure once an accused is facing court-martial.

A historical review of relatively recent courts-martial with classified information issues suggests that 18 U.S.C. § 793 is the most common offense charged in all courts-martial involving classified information issues, whether the case involves espionage or is a relatively straightforward mishandling case. If a court-martial assimilates one of these federal crimes, the Hiss Act is only triggered when the executed sentence includes death, dishonorable discharge, or dismissal from service.

(a) Defense Counsel and the Hiss Act. Defense counsel must consider the implications of the Hiss Act any time they have a case with classified information. Defense counsel should read the Hiss Act to determine whether it applies to any of the charged offenses and strategize accordingly. An important issue that defense counsel must recognize is the possibility that failing to advise the accused on the implications of the Hiss Act may result in ineffective assistance of counsel issues on appeal. In 1960, a military court addressed this specific issue in the government's favor, ruling that counsel's failure to advise an accused that a conviction would result in a denial of retirement benefits under the Hiss Act did not render the plea improvident. United States v. Pajek, 11 C.M.A. 686 (1960). However, considerable ineffective assistance of counsel case law has developed since 1960. Above and beyond any ineffective assistance of counsel issue, it is simply good practice to ensure that the accused is fully informed of all potential consequences of the court-martial, whether contested or by plea.

(b) Trial Counsel and the Hiss Act. From a trial counsel perspective, the implications of the Hiss Act are less significant in an egregious case involving classified information, such as espionage and treason, since most sentences would include a punitive discharge. However, the likelihood of a punitive discharge is less certain when facing less serious offenses, e.g. mishandling classified information cases. In these less serious cases it is important for the trial counsel to recognize what is truly at stake when negotiating plea agreements with defense counsel and discussing the case with the convening authority. The trial counsel must fully understand what if any charges are within the purview of the Hiss Act and whether the additional requirement of an executed sentence including death, dishonorable discharge, or dismissal from service is applicable. Perhaps most importantly, it is imperative that staff judge advocates develop a clear strategy prior to charging so that the government has options during later stages of the court-martial process. Trial counsel and staff judge advocates are encouraged to consult with Code 17 for support during the development of charges.

2. The Smith Amendment, 10 U.S.C. § 986. The Smith Act, enacted in 2000 and amended in 2006, prohibits a person from obtaining a security clearance if convicted of any crime in any U.S. court that results in not less than one year of confinement actually served. The Smith Amendment applies to grants of new security clearances and periodic renewals for DoD employees, active duty members of the Army, Navy, Air Force, or Marine Corps, and employees of DoD contractors. While the law does allow for waivers of this prohibition, senior DoD

FOR OFFICIAL USE ONLY

officials have granted very few waivers. Although less consequential than the Hiss Act, defense counsel especially should consider the application of a potentially qualifying conviction. The relevance of a post-conviction security clearance is more likely in a case involving classified information issues since the accused probably possessed a security clearance prior to the court-martial.

CHAPTER 13

Post-Trial Matters

In a court-martial with classified information issues, responsibilities pertaining to the protection of classified information continue throughout the post-trial process. This chapter starts by introducing two general issues. The first issue, post-trial debriefs, is primarily relevant to national security cases, but is also potentially relevant to high-visibility mishandling cases. The second issue, a specific limitation on authority to remit and suspend sentences, is unique to national security cases. Additionally, this chapter discusses the post-trial responsibilities for the parties to a court-martial with classified information issues: trial counsel, defense counsel, staff judge advocate, Navy and Marine Corps Appellate Review Activity, appellate counsel, and appellate courts.

A. Post-Trial Debriefs. All judge advocates involved in a national security case or other case involving classified information issues that the intelligence community (IC) is concerned about should not underestimate the importance of a post-trial debrief to the IC. The debrief is a valuable tool the IC uses to, among other matters, better understand the extent of the compromise of classified information, e. g., damage control, and support counter-intelligence efforts. The IC wants to learn as much about the information compromised and techniques of U.S. adversaries as possible. In a national security case, the post-trial debrief is more often focused on intelligence issues than law enforcement matters.

1. Timing of the Debrief. One issue that judge advocates involved in a classified information case have to consider is the timing of the post-trial debrief, with the options being pretrial, between entry of plea and sentencing, or post-sentencing. In the federal criminal system, there is normally a considerable gap between the trial on the merits and sentencing phase of a criminal trial. The intelligence debrief in a federal espionage case usually begins, and is often completed, during this gap between conviction and sentencing. The court-martial process does not normally include such a gap between the trial on the merits and sentencing phases, but it could be agreed to by the parties as part of pretrial negotiations. Although the norm for courts-martial would be to conduct the debrief after sentencing, there are situations where one of the other options would be preferable. If there is concern about the accuracy of what the accused is agreeing to admit as part of his plea, the convening authority may desire the debrief and polygraph to occur prior to entry of pleas to ensure that the accused is being completely truthful. Debriefs that occur before entry of pleas or between entry of plea and sentencing provide an additional incentive for the accused to fully cooperate and be truthful, because such cooperation may result in a lesser sentence than he otherwise would have received. It should be noted that convening authorities may be reluctant to give an accused the opportunity to claim full cooperation with the government as part of his mitigation case on sentencing, however, this is the norm in federal court. In addition, especially in espionage cases, the intelligence community has a vested interest in the accused's full and complete cooperation, using as many incentives as possible (e.g., immunity, reduced sentence, recommendations on confinement location). When the debrief and polygraph occur post-sentencing, there will likely still be a period of suspended confinement (the

difference between the adjudicated sentence and the confinement cap in the pretrial agreement) to hold over the accused's head in an effort to ensure his truthful cooperation. However, as in any regular court-martial, there is a certain amount of inertia that works against vacating a suspended sentence, which is further strengthened in espionage cases due to the classified nature of the information. Particularly in espionage cases, the staff judge advocate to the convening authority should ensure that the intelligence community stakeholders have an opportunity to comment on the timing and urgency of the debrief before entering a pretrial agreement with the accused.

Contested Cases. Of course, pretrial debriefs are not usually an option in a contested case. Following trial, and assuming there has been a conviction, the convening authority may still order the accused to submit to a debrief by providing testimonial immunity to him, thereby eliminating any Fifth Amendment self-incrimination problem.

2. Immunity. Immunity is an important component of the debrief because it is another mechanism to encourage the accused to be truthful. If the debrief occurs prior to the trial, Military Rule of Evidence 410 provides the necessary protection to the accused because his statements are being made essentially during the course of plea negotiations and are not admissible in any court-martial proceeding against the accused. Grants of immunity in cases with classified information issues require consultation with the Department of Justice. The "Memorandum of Understanding (MOU) Between the Departments of Justice and Defense Relating to the Investigation and Prosecution of Certain Crimes" requires consultation with DoJ for a proposed grant of immunity in a case involving espionage, subversion, aiding the enemy, sabotage, spying, or violation of rules or statutes concerning classified information or the foreign relations of the United States. (DoD Instruction 5525.07, recently reissued on 18 June 2007, implements this MOU. See Annex E.) Additionally, JAGMAN 0138d requires consultation with DoJ in all cases involving national security or foreign relations of the United States.

3. Post-Trial Polygraphs. When an accused agrees to be debriefed, he normally also agrees to subject himself to polygraph examinations in order to verify his truthfulness. Any pretrial agreement containing a polygraph requirement should specify, to the extent feasible, what the government expects of the accused, who will conduct the polygraph, the scope of the polygraph, and what, if any, role the defense counsel can have, and the consequences if the accused can not "pass" the polygraph.

Chapter 11, Pretrial Agreements, contains a more detailed discussion of the issues associated with polygraphs and immunity since the pretrial agreement usually covers these issues.

B. Limitation on Authority to Remit and Suspend Sentences. JAGMAN 0159 provides that "[n]o official of the DON, other than the Secretary of the Navy, may remit or suspend, pursuant to article 74(a), UCMJ, and R.C.M. 1107, MCM, any part or amount of the approved sentence in any case designated as a national security case in accordance with section 0126." (Emphasis added.) It is important to remember that the convening authority can still exercise clemency pursuant to UCMJ Article 60 when the convening authority takes initial action approving the

findings and sentence. The Secretary of the Navy has only reserved “supplemental clemency” authority in National Security Cases. *United States v. Allen*, 31 M.J. 572 (N-M.C.C.R. 1990).

C. Responsibilities. The conclusion of a court-martial involving classified information involves more work on the part of all responsible parties than does a regular court-martial. Usually some portion, or all, of the record of trial will require special handling and storage throughout the process of review, authentication, and forwarding to the appellate court. In addition, extra copies of classified information used during the trial must be disposed of properly. Defense counsel in particular should conduct a thorough review and screening of their case file to ensure that no classified information or notes remain when they retain their files after transferring from the command.

1. Trial Counsel:

- (a) Ensure that all classified evidence is properly marked and stored.
- (b) Inform interest agencies, particularly the original classification authority’s agency, e.g., NSA, CIA, of the results of the court-martial. Code 17 can support this effort.
- (c) Confirm with the court security officer and court reporter that all classified material is accounted for and secured, including a sweep of the deliberation room, judge’s chamber, and other relevant areas.
- (d) Remind defense counsel to return all defense copies of classified material. Defense counsel notes may be retained but must be properly marked and stored.
- (e) Ensure that the record of trial is properly marked and stored.
- (f) Consider feasibility of separating classified portions of record of trial into a classified annex, leaving bulk of record of trial unclassified.
- (g) Work with the staff judge advocate to ensure accused complies with any pretrial agreement debrief and polygraph requirements.

2. Defense Counsel:

- (a) Account for and return or properly dispose of unneeded classified material.
- (b) Properly mark and store any classified or potentially classified notes.
- (c) Work with trial counsel and staff judge advocate to ensure client complies with any pretrial agreement debrief and polygraph requirements.
- (d) Consider value of post-trial cooperation with intelligence community or law enforcement

- (e) Ensure that any appellate defense counsel have appropriate clearances prior to initiating classified discussions.

3. Staff Judge Advocate:

- (a) Account for classified material contained in record of trial and make sure pages and the record of trial are properly marked and stored.
- (b) Prior to authentication, discuss with trial counsel feasibility of separating classified portions of record of trial into a classified annex, leaving bulk of record of trial unclassified.
- (c) Work with trial counsel and defense counsel to ensure accused complies with any pretrial agreement debriefs and polygraph requirements.
- (d) Ensure that record of trial and allied papers are properly marked, wrapped, and sent to appellate review activity.
- (e) Comply with special handling rules that may apply depending on the type of classified information contained in the record of trial.
- (f) Alert Navy and Marine Corps Appellate Review Activity (NAMARA/Code 40) that a classified record of trial is incoming.
- (g) Confirm receipt by NAMARA.
- (h) Ensure that command copies are properly marked and stored.

4. Navy and Marine Corps Appellate Review Activity:

- (a) Confirm that the record of trial and allied papers are properly marked, wrapped, and accounted for upon receipt and receiving personnel are properly cleared and trained.
- (b) Contact staff judge advocate to acknowledge receipt of record of trial.
- (c) If the record of trial is separated into classified and unclassified portions, only enter the unclassified portions into the “standard” record of trial system. Classified portion of record of trial must be properly marked and stored in accordance with its classification level. Code 17 can store SECRET records of trial.
- (d) Notify Appellate Defense and Appellate Government of the receipt of a classified case.

5. Appellate Defense and Appellate Government:

- (a) Ensure assigned appellate defense and appellate government personnel have appropriate clearances and all classified material is handled and stored properly, including the record of trial.
- (b) Coordinate appellate review with appellate court officials to ensure the proper handling and storage of classified material.

6. Appellate Court:

- (a) Ensure all appellate court officials have appropriate clearances and all classified material is handled and stored properly, including the record of trial.
- (b) Consider the potential need to close the courtroom.

FOR OFFICIAL USE ONLY

This page intentionally left blank

ANNEX A

**STAFF JUDGE ADVOCATE/TRIAL COUNSEL CHECKLIST
FOR
CLASSIFIED INFORMATION CASES**

References:

28 C.F.R., Part 17

Executive Order 12958, Part 4.1(i)

SECNAVINST 5510.36, DoN Information Security Program

JAGMAN 0126, 0137, 0138, 0143, 0144, 0150, 0159

M.R.E. 505

R.C.M. 707, 1104

A. Notification of Investigation

- ____ 1. Identify cognizant NSCDA from JAGMAN 0126; notify SJA for NSCDA.
- ____ 2. Ensure Command is following classified information loss/compromise procedures found in Ch. 12, SECNAVINST 5510.36, including notifications of OCAs.
- ____ 3. Advise OJAG Code 17 of case status: (DSN 325-5464/5, (202) 685-5464/5; FAX DSN 325-5467, (202) 685-5467).
- ____ 4. Identify prospective TC that holds an appropriate security clearance (at the same or higher level as the classified information) at earliest stage of investigation.
- ____ 5. Notify Senior Trial Counsel at TSO East or TSO West, as appropriate, of possible national security case.

B. Investigation

- ____ 1. Assess litigation consequences of each proposed investigatory action (e.g. search and seizure, chain of custody, etc.).
- ____ 2. Ensure that the NCIS case agent has contacted the NCIS-HQ National Security Law Unit: 202-433-0877.
- ____ 3. Call OJAG Code 17 for estimate of time requirements for classification reviews.
- ____ 4. Assess speedy trial consequences of the timing of apprehension, if applicable.

FOR OFFICIAL USE ONLY

- ___ 5. Remind investigators of speedy trial implications of apprehension when other investigative techniques and avenues remain to be explored.
- ___ 6. Adhere strictly to the "third agency rule" (E.O. 12958, Part 4.1(i)) when dealing with non-DOD intelligence agencies (must have permission of originating agency).
- ___ 7. Request assistance from OJAG Code 17 to resolve any problems.
- ___ 8. If the accused has agreed to speak to investigators, verify his or her understanding of the classification level of the information.
- ___ 9. Determine what classified information is at issue.. Determine if sensitive compartmented information is involved.
- ___ 10. Obtain a determination from the NSCDA whether the case is a "national security case" as defined in JAGMAN 0126. Does the case involve, to "a serious degree":
 - ___ the compromise of a military or defense advantage over any foreign nation?
 - ___ an allegation of willful compromise of classified information?
 - ___ military or defense capability to successfully resist hostile or destructive action, overt or covert?
 - ___ terrorist activities?
- ___ 11. Obtain a decision from the NSCDA about the proper disposition of the case.
- ___ 12. Contact Program Manager in special access programs to determine special access requirements.
- ___ 13. Consider speedy trial implications and the existence of possible exclusions under RCM 707 or case law for the time required to complete classification reviews.
- ___ 14. Coordinate with OJAG Code 17 to initiate classification reviews of materials at issue in the case and likely to be entered into evidence.

C. Charges

- ___ 1. Identify all potential charges under UCMJ and Federal criminal statutes.
- ___ 2. Draft charges and specifications.

Annex A-2

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

- ___ 3. Consider selection of a representative sample of specifications and supporting documentary evidence to demonstrate the subject's pattern and scope of activities.

D. Convening Authority

- ___ 1. Identify and contact appropriate convening authority IAW JAGMAN 0126 and the determination of the NSCDA.
- ___ 2. Discuss accuser/command influence issues, if any, with CA and OJAG Code 17.

E. Security Clearances

- ___ 1. Confirm appropriate level security clearances for:
- ___ Art. 32 investigation officer
 - ___ military judge
 - ___ trial counsel
 - ___ military defense counsel
 - ___ civilian defense counsel
 - ___ court reporters
 - ___ bailiff(s)
 - ___ investigation security officer(s)
 - ___ court security officer(s)
 - ___ members
 - ___ witnesses
 - ___ brig chasers
- ___ 2. Obtain appointment of an investigation security officer in writing. Appointment may be in a Protective Order issued by the CA if an Article 32 investigation is directed.
- ___ 3. Obtain appointment of a court security officer in writing in a Protective Order issued by the CA before referral of charges or by the military judge after referral of charges.

Annex A-3

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

- ____ 4. Ensure that members with proper security clearances are detailed.
- ____ 5. Maintain a record of due diligence in submission of appropriate clearance applications and requests for completion of classification reviews, for speedy trial purposes.

F. Security Officers

- ____ 1. Establish contact with command special security officer (SSO).
- ____ 2. Obtain SSO review of security clearance application packages of court personnel before transmittal.
- ____ 3. In cases before members, consult with SSO to prepare request for special instructions from the military judge on security matters.

G. Civilian Defense Counsel

- ____ 1. Via OJAG Code 17, request CNO (N09N2) issue a Limited Access Authorization for civilian defense counsel, if required.
- ____ 2. If request is denied, coordinate with Appellate Government on preparation of counter briefs on motions to dismiss on 6th Amendment grounds.

H. Protection of Classified Evidence

- ____ 1. Determine if investigative reports are classified and how quickly they can be declassified or redacted (see SECNAVINST 5510.36).
- ____ 2. After classification reviews, determine whether closed sessions will be necessary at trial.
- ____ 3. Before charges are preferred, have the CA issue a protective order to all parties. Include a written admonishment to the accused that disclosure of classified information to counsel who does not have the required security clearance is a violation of the UCMJ. The military judge should also be requested to issue a protective order after referral of charges.
- ____ 4. Brief the civilian defense counsel on requirements for handling classified information and prohibitions on disclosure of such information and accompanying penalties.
- ____ 5. Obtain a written acknowledgement of the briefing from civilian counsel.

FOR OFFICIAL USE ONLY

- ___ 6. Ensure defense counsel knows of duty to notify trial counsel in writing of anticipated disclosure of classified information at trial per M.R.E. 505(h).

I. Pretrial Agreements

- ___ 1. Ensure pretrial agreements are consistent with JAGMAN 0137 and approved by SECNAV in national security cases.
- ___ 2. Include, as appropriate, provisions for the accused to:
- ___ cooperate in debriefings and damage assessments
- ___ submit to polygraph examination(s)
- ___ agree to UNCLASSIFIED stipulation of facts as to general subject matter and classification of evidence
- ___ UNCLASSIFIED forum

J. Immunity

- ___ 1. Draft grants of immunity to apply only to court-martial.
- | ___ 2. Alternatively, obtain permission from DOJ/DOD GC to extend the grant of immunity to all Federal prosecutions.
- ___ 3. Have all grants of immunity approved by DOJ via Codes 17/20 per JAGMAN 0138

K. Protective Orders/Courtroom Security

- ___ 1. Include requirements for handling and disclosure of classified information in a protective order.
- ___ 2. Aggressively employ and demonstrate a full understanding of M.R.E. 505 to counsel and intelligence agencies' operational staffs to foster cooperation.
- ___ 3. Ensure proper application of all required security measures in:
- ___ E.O. 12958, Part 4
- ___ 28 C.F.R., Part 17
- ___ SECNAVINST 5510.36

FOR OFFICIAL USE ONLY

- ____ 4. Where evidence is collected under a warrant issued pursuant to the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. 1801-1811, immediately contact OJAG Code 17 for guidance and assistance.
- ____ 5. Anticipate situations that may require the trial to be closed to protect disclosure of classified information.

L. Evidentiary Considerations and Discovery

- ____ 1. Seek declassification or redaction of information requested by the defense in lieu of nondisclosure under M.R.E. 505.
- ____ 2. Ensure the CA responds in writing to a defense request for classified material.
- ____ 3. Consider all options when the Government seeks nondisclosure of classified information requested by the defense.
- ____ 4. Resist disclosure by providing information required for military judge determinations and actions under M.R.E. 505(i).
- ____ 5. Identify possible alternatives to complete nondisclosure of classified information:
 - ____ substitute unclassified information
 - ____ enter into unclassified stipulation of facts
 - ____ disclose only a redacted version of the information
 - ____ disclose under limiting conditions of a protective order
 - ____ dismiss selected charges/specifications
 - ____ dismiss all charges and substitute alternative disciplinary or administrative actions against the accused
- ____ 6. Take steps to avoid dismissal by the military judge under M.R.E. 505(f) when classified information is not disclosed.
- ____ 7. When classified information is disclosed, move for a protective order from the military judge.
- ____ 8. Ensure that the military judge excises unneeded portions of classified information before delivery of remaining material to the accused.

Annex A-6

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

- ____ 9. Ensure all parties understand that disclosure during discovery and subsequent use at trial are distinct issues.

M. Evidentiary Considerations at Trial

- ____ 1. Identify and prepare expert witnesses to prove proper classification of materials.
- ____ 2. Invoke M.R.E. 505 privilege if the accused requests under Brady the production of Government witness statements that include classified information.
- ____ 3. Anticipate that certain classified portions of prior witness statements will be inconsistent with testimony and be prepared to move for an in camera proceeding pursuant to M.R.E. 505(i).
- ____ 4. In coordination with military judge and CSO, determine if and when the courtroom should be closed to the general public per M.R.E. 505.

N. Interlocutory Appeal

- ____ 1. If the military judge dismisses any charges or specifications, request a stay for up to 72 hours.
- ____ 2. If an appeal of the ruling is considered:
- ____ contact NAMARA for approval
- ____ file a notice of appeal within 72 hours with proper certification
- ____ 3. If there will be no appeal, promptly inform the military judge and defense counsel.

O. Sentencing

- ____ 1. Obtain witnesses to testify about the amount of damage to national security caused by the accused's actions.
- ____ 2. Obtain witnesses/affidavits via OJAG Code 17 on significance of the accused's actions.
- ____ 3. Obtain witnesses/affidavits via OJAG Code 17 on other situations that could cause similar compromise of national security.

P. Post-Trial Duties

- ____ 1. Ensure that a proper security classification is assigned to the record of trial and on each of its pages that contain classified information.

Annex A-7

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

- ____ 2. Contact the Court Security Officer for assistance.
- ____ 3. Where there is an appeal on grounds of objections sustained to withholding evidence under M.R.E. 505, prepare sealed exhibits of the text of relevant documents and submit them along with motion and materials with the record of trial.
- ____ 4. Follow JAGMAN 0150C in the handling of classified records of trial
- ____ 5. Remove classified portions from the Record of Trial before forwarding to the Accused, in accordance with R.C.M. 1104(b)(1)(D).
- ____ 6. If the record of trial contains Sensitive Compartmented Information, follow procedures set forth in the Memorandum of Agreement between OJAG and NCIS.
- ____ 7. Permit the Court Security Officer to detach from his/her duties only after completion of the post-trial classification review and portion marking of the record of trial.

FOR OFFICIAL USE ONLY

ANNEX B

**DEFENSE COUNSEL CHECKLIST
FOR
CLASSIFIED INFORMATION CASES**

References:

SECNAVINST 5510.36 DoN Information Security Program

JAGMAN 0126, 0137, 0138, 0143, 0144, 0159

M.R.E. 505

A. Initial Steps

- ___ 1. Notify your chain of command and command Security Manager (SM) that you have a case involving classified information.
- ___ 2. Read SECNAVINST 5510.36, DoN Information Security Program, to familiarize yourself with proper handling and marking of classified materials.
- ___ 3. Security Clearance and Access
- ___ (A). Verify your security clearance level with your Security Manager (SM). Make sure he/she records your “access” in JPAS. (Your security clearance level must be at least at the level of the highest level of classified information involved in the case. If necessary, submit necessary paperwork for an upgrade in clearance ASAP.)
- ___ (B). Verify security clearance of your paralegal or other staff/co-counsel who will assist you.
- ___ (C). Determine the security clearance status of the Accused by coordinating with your SM
- ☐ None ever given
 - ☐ Suspended by Command
 - ☐ Revoked by DoNCAF
 - ☐ Still in place: ☐ (C) ☐ (S) ☐ (TS) ☐ (SCI)
- ___ (D). Civilian Defense Counsel (CDC)? Determine security clearance of CDC by coordinating with your SM. Submit “Limited Access Authorization” for CDC’s temporary clearance via OJAG Code 17 (see template). Note that CDC may have to complete a SF 86 Security Clearance Questionnaire and submit fingerprint cards.
- LAA granted by DoNCAF Date: _____
- Expiration: _____
- NonDisclosure Agreement (SF 312) Executed?

Annex B-1

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

Protective Order Executed?

Note: CDC may store classified information, including motions, evidence, or notes, only in a government facility approved for classified material storage (such as the NLSO).

___ 4. Handling of Classified Information

- ___ (A). Classified Storage: Coordinate with your command SM, your host activity, or the CA's SM (via the TC) for a GSA-safe or other approved storage arrangement for classified material.
- ___ (B). Classified Transmission via *secure* Phone/Fax/Email: Coordinate with your command SM, your host activity, or the CA's SM (via the TC) for a STE/STU III secure phone/fax and SIPRNET access in order to transmit classified material, if needed.
- ___ (C). Determine if sensitive compartmented information or special access programs are involved because SCI information requires special handling. If so, immediately contact OJAG Code 17 or your local Special Security Officer (SSO) via your SM.
- ___ (D). Communications with the Accused: If the Accused has a security clearance (or LAA), DC and ACC may discuss classified information without notifying the government but only up to the lower clearance level between them. For example, if DC has a Secret (S) clearance, and ACC has a Top Secret/Sensitive Compartmented Information (TS/SCI) clearance, they may discuss up to and including Secret information only.
- ___ (E). Adhere strictly to the "third agency rule" (E.O. 12958, Part 4.1(i)) when dealing with non-DOD intelligence agencies. You must have permission of originating agency to disclose its classified information to the Accused or anyone else.

___ 5. Speedy Trial: Assess and consider speedy trial implications.

___ 6. National Security Case designation:

- (A). Has the case been designated a "National Security Case" pursuant to JAGMAN 0126?
Identify NSCDA: _____
Date designated: _____

Does the case involve, to "a serious degree":

___ the compromise of a military or defense advantage over any foreign nation?

Annex B-2

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

___ an allegation of willful compromise of classified information?

___ military or defense capability to successfully resist hostile or destructive action, overt or covert?

___ terrorist activities?

(B). Determine the outcome of the NSCDA's decision about the proper disposition of the case.

(C). Read JAGMAN Sections 0126, 0137, 0138, 0143, 0144, 0159

B. Pre-trial Discovery

___ 1. Submit written requests for classified evidence to the CA via the TC. CA must respond in writing per M.R.E. 505(d). Note that disclosure during discovery and subsequent use at trial are distinct issues.

___ 2. Request copies of the CA's Preliminary Inquiry and JAGMAN reports and messages conducted under SECNAVINST 5510.36, Chapter 12, if this is a loss/compromise case.

___ 3. Obtain copies of the Classification Reviews (CR), OCA letters, and M.R.E. 505 letters from TC.

(A). Does each CR state the *current* classification level of the material at issue?

(B) For loss/compromise cases, does each CR state the classification level of the material at issue *at the time of the offense*? Is the classification level stated in the CR different from that level marked on the item at issue?

___ 4. Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. 1801-1811: Was any of the evidence obtained under a FISA warrant? If so, challenges to the FISA Order can only be litigated in Federal District Court.

___ 5. Subject Matter Assistance: If needed, request a subject matter expert be assigned to the defense team.

C. Litigation Issues

___ 1. Determine what classified information is likely to be used in your client's defense and submit written Notice under M.R.E. 505(h).

___ substitution of the unclassified information

Annex B-3

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

___ unclassified stipulation of facts

___ redaction of the classified information

___ dismissal of the selected charges/specifications

___ dismissal of all charges and substitute alternative disciplinary or administrative actions against the accused

___ 2. If government seeks to deny defense request, identify possible alternatives to complete disclosure of classified information:

___ 3. Anticipate situations that may require the trial to be closed to protect disclosure of classified information. In coordination with military judge, TC, and Court Security Officer (CSO), determine if and when the courtroom should be closed to the general public per M.R.E. 505.

___ 4. Plan cross and direct examinations of witnesses to accord with bifurcated (open/closed) testimony.

___ 5. Plan introduction of classified evidence to accord with closed sessions.

___ 6. Ensure Accused and Defense witnesses are briefed on the bifurcated testimony procedures.

___ 7. Ex Writs.

___ 8. Presentencing.

(A). Classified Evidence: Request alternatives to the relevant and material classified evidence unless no unclassified version is available, per M.R.E. 505(i)(4)(B).

(B). Extenuation & Mitigation:

Witnesses on Accused's lack of training on handling classified material?

Any possibility mishandled information was subsequently declassified, downgraded, or misclassified?

___ 9. Special considerations for Designated National Security Cases

(A). PTAs must be approved by SECNAV.

(B). Immunity Requests must be approved by DOJ.

Annex B-4

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

D. Post-trial

(A). Records of Trial (ROT) authentication: If the ROT contains classified information, the CA must delete/remove it from the Accused's copy, attach a certificate to the ROT, and serve a copy on the Accused. Follow JAGMAN 0150C in the handling of ROTs.

(B). Clemency: If possible, keep clemency matters unclassified.

(C). If the ROT contains SCI, follow procedures set forth in the Memorandum of Agreement between OJAG and NCIS (contact OJAG Code 17).

E. Generally

(A). Contact the Investigation Security Officer (ISO) for Art. 32 assistance, and the Court Security Officer (CSO) for court-martial assistance.

(B). Request assistance from OJAG Code 17 to resolve any other problems.

FOR OFFICIAL USE ONLY

This page intentionally left blank

Annex B-6
FOR OFFICIAL USE ONLY

ANNEX C

Role of the Investigation Security Officer and the Court Security Officer

As stated above, the protective order will appoint an investigation security officer and/or court security officer who is charged with safeguarding classified material during the proceeding. Both the investigation security officer and court security officer are neutral and serve as the security advisor to the Article 32 investigating officer or military judge and serve as experts on protecting classified information. The investigation security officer and court security officer should have considerable familiarity with the material relevant to the proceeding so that they can best advise the investigating officer or military judge with regard to what information is classified and the required handling procedures for the specific classified information at issue. If specific programs or special access material is at issue in a particular session (open or closed), it may be necessary to have a subject matter expert serve as a security officer to assist in signaling the investigating officer or military judge when a question calls for classified information or testimony inadvertently strays into classified matters.

It is paramount to remember that none of the security officers is a member of the prosecution or defense team. Rather, all security officers are primarily responsible to the investigating officer or the military judge for providing security guidance and assistance to the proceeding, including, as necessary, the government and defense teams. The security officers are there to prevent the military judge and the government and defense teams from committing security violations. They advise the investigation or court from a security perspective, not from a legal perspective. The defense should request an expert in security issues from the convening authority should they feel the need, based on the facts of the case, to receive privileged advice on those issues.

Security officers should be experienced military members with a broad background in information, personnel, and physical security. Convening authority staff judge advocates, working with the local security managers and special security officers, should identify a pool of individuals with requisite backgrounds.. These individuals must be cleared for the material that will be at issue in the proceeding. This means that if the proceeding involves classified material from a Special Access Program (SAP) or at the level of Top Secret/Sensitive Compartmented Information, then the security officers must be "read in" and cleared to handle that particular information. It is incumbent upon the staff judge advocate to ensure that an investigation security officer is assigned to the case at the outset. This is usually done by naming the investigation security officer in the Article 32 appointing order or in the protective order.

The security officers also ensure that all the necessary parties have the requisite security clearances and accesses. They also generate an access list that contains the names of the personnel authorized to be in the courtroom during classified sessions. The bailiff or a door sentry may use this list to prevent unauthorized access to the courtroom.

FOR OFFICIAL USE ONLY

This page intentionally left blank

ANNEX D

Classified Information Procedures Act: Statute, Procedures, and Comparison with M.R.E. 505

Classified Information Procedures Act, 18 United States Code Appendix § 1

§ 1. Definitions

(a) "**Classified information**", as used in this Act, means 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)).

(b) "**National security**", as used in this Act, means the national defense and foreign relations of the United States.



Comparison with M.R.E. 505. CIPA § 1(a) is essentially identical to M.R.E. 505(b)(1), and CIPA § 1(b) is essentially identical to M.R.E. 505(b)(2). Note that CIPA is a PROCEDURAL statute that has, at its foundation, the ability of the United States to assert the State Secrets Privilege. CIPA does not contain the privilege language; it merely provides the mechanism for the United States to proceed in a case where the State Secrets Privilege is waived to the extent needed for a given case. The State Secrets Privilege enables the government to refuse to give evidence upon a showing of reasonable likelihood of danger that the evidence will disclose a secret of state. *See, e.g., United States v. Reynolds, 345 U.S. 1, 7-8, (1953)* (privilege to protect military and state secrets belongs to government and must be asserted by it via formal claim of privilege lodged by head of department with actual control over the matter); *Frost v. Perry, 919 F. Supp. 1459, 1464-1465 (D. Nev. 1996)* (military and state secret privilege was properly invoked by Secretary of the Air Force).

In contrast, M.R.E. 505(a) states that the Rule is a “general rule of privilege” to protect information “if disclosure would be detrimental to national security.”

§ 2. Pretrial conference

At any time after the filing of the indictment or information, any party may move for a pretrial conference to consider matters relating to classified information that may arise in connection with the prosecution. Following such motion, or on its own motion, the court shall promptly hold a pretrial conference to establish the timing of requests for discovery, the provision of notice required by section 5 of this Act, and the initiation of the procedure established by section 6 of this Act. In addition, at the pretrial conference the court may consider any matters which relate to

classified information or which may promote a fair and expeditious trial. No admission made by the defendant or by any attorney for the defendant at such a conference may be used against the defendant unless the admission is in writing and is signed by the defendant and by the attorney for the defendant.



Comparison with M.R.E. 505. CIPA § 2 is reflected in M.R.E. 505(e). In conformance with military practice, 505(e) establishes that pre-trial hearings are available after referral of charges and prior to arraignment, when a military judge has control of a case. Since Federal practice has no corollary to pre-referral, there is no counterpart in CIPA to M.R.E. (d) which imposes certain responsibilities upon a convening authority.

§ 3. *Protective orders*

Upon motion of the United States, the court shall issue an order to protect against the disclosure of any classified information disclosed by the United States to any defendant in any criminal case in a district court of the United States.



Comparison with M.R.E. 505. CIPA § 3 addresses protective orders which, in military practice, are set forth in both M.R.E. 505(g)(1) and R.C.M. 405(g)(6). Note that while R.C.M. 405 states that a designated authority “may” issue a protective order, M.R.E. 505(g)(1), like CIPA, states that the military judge “shall” issue such an order upon request of the Government. Protective orders are discussed in Chapter 6.

§ 4. Discovery of classified information by defendant

The court, upon a sufficient showing, may authorize the United States to delete specified items of classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure, to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove. The court may permit the United States to make a request for such authorization in the form of a written statement to be inspected by the court alone. If the court enters an order granting relief following such an ex parte showing, the entire text of the statement of the United States shall be sealed and preserved in the records of the court to be made available to the appellate court in the event of an appeal.



Comparison with M.R.E. 505. CIPA § 4 is mirrored in M.R.E. 505(d), which permits a convening authority to order the use of evidentiary substitutes such as substitutes, redactions, deletions, stipulations, etc. during the pre-referral period. This same provision is also contained in M.R.E. 505(g)(2), where this authority is granted to the military judge. However, as discussed more fully in Chapter 9, the military judge may determine that an evidentiary substitute is insufficient and “disclosure of the classified information itself is necessary to enable the accused to prepare for trial.”

§ 5. Notice of defendant's intention to disclose classified information

(a) Notice by defendant. If a defendant reasonably expects to disclose or to cause the disclosure of classified information in any manner in connection with any trial or pretrial proceeding involving the criminal prosecution of such defendant, the defendant shall, within the time specified by the court or, where no time is specified, within thirty days prior to trial, notify the attorney for the United States and the court in writing. Such notice shall include a brief description of the classified information. Whenever a defendant learns of additional classified information he reasonably expects to disclose at any such proceeding, he shall notify the attorney for the United States and the court in writing as soon as possible thereafter and shall include a brief description of the classified information. No defendant shall disclose any information known or believed to be classified in connection with a trial or pretrial proceeding until notice has been given under this subsection and until the United States has been afforded a reasonable opportunity to seek a determination pursuant to the procedure set forth in section 6 of this Act, and until the time for the United States to appeal such determination under section 7 has expired or any appeal under section 7 by the United States is decided.

(b) Failure to comply. If the defendant fails to comply with the requirements of subsection (a) the court may preclude disclosure of any classified information not made the subject of notification and may prohibit the examination by the defendant of any witness with respect to any such information.



Comparison with M.R.E. 505. The defense notice requirement of CIPA § 5 is found in M.R.E. 505(h). 505(h) provides more detail on the notice requirement and substitutes “prior to arraignment” for the thirty days prior to trial language in CIPA. Both contemplate a judicial order specifying a timeline, however, and this is how it works in practice. 505(h)(3) provides more details on what is required in the written notice. It uses the “brief description” term of CIPA but specifies that this “must be more than a general statement of the areas about which the evidence may be introduced. The accused must state, with particularity, which items of classified information he reasonably expects will be revealed by his defense.” 505(h)(2) expands on the continuing duty to notify intent of CIPA, and 505(h)(4) is essentially the same language regarding prohibition against disclosure as in CIPA. 505(h)(5) provides the same sanctions for failure to comply as does CIPA § 5(b).

§ 6. Procedure for cases involving classified information

(a) Motion for hearing. Within the time specified by the court for the filing of a motion under this section, the United States may request the court to conduct a hearing to make all determinations concerning the use, relevance, or admissibility of classified information that would otherwise be made during the trial or pretrial proceeding. Upon such a request, the court shall conduct such a hearing. Any hearing held pursuant to this subsection (or any portion of such hearing specified in the request of the Attorney General) shall be held in camera if the Attorney General certifies to the court in such petition that a public proceeding may result in the

disclosure of classified information. As to each item of classified information, the court shall set forth in writing the basis for its determination. Where the United States' motion under this subsection is filed prior to the trial or pretrial proceeding, the court shall rule prior to the commencement of the relevant proceeding.



Comparison with M.R.E. 505. CIPA § 6 is the “engine” that drives CIPA. It provides the procedural framework for the *ex parte* or *ex parte in camera* reviews by a judge for all determinations concerning the use, relevance, or admissibility of classified information. There are some key differences in the M.R.E. analogue, 505(i). For clarity, the differences or notable similarities are set forth following each subsection of CIPA § 6.

CIPA § 6(a):

- *In camera* in the Federal court means outside of the presence of the defendant. In a court-martial the accused has an absolute right to be present at all proceedings, thus *in camera* means the public is excluded from that portion of the court-martial. *Ex parte in camera* is the same for both, either Government counsel and military judge, or military judge alone review the information.
- A Federal judge shall hold an *in camera* review if the Attorney General certifies to the court “that a public proceeding may result in the disclosure of classified information.” In military practice the Government must have head of agency invocation of the privilege, per 505(c), and an affidavit regarding the reasonably expected damage to national security for disclosure justifying the classification of the information. M.R.E. 505(i)(3); *See* Chapters 7 and 8.
- The military judge, like the Federal judge, must make a ruling on the information “prior to commencement of the relevant proceeding.” 505(i)(4)(B).
- Both CIPA and the M.R.E. require a written determination of the judge’s ruling, though on its face M.R.E. 505(i)(4)(C) seems to only require a written order if the judge determines that the information meets the disclosure standards of 505(i)(4)(B). However, in practice a military judge will, in all likelihood, issue a written ruling for any decision under this Rule section.

(b) Notice.

(1) Before any hearing is conducted pursuant to a request by the United States under subsection (a), the United States shall provide the defendant with notice of the classified information that is at issue. Such notice shall identify the specific classified information at issue whenever that information previously has been made available to the defendant by the United States. When the United States has not previously made the information available to the defendant in connection with the case, the information may be described by generic category, in such form as the court may approve, rather than by identification of the specific information of concern to the United States.

(2) Whenever the United States requests a hearing under subsection (a), the court, upon request of the defendant, may order the United States to provide the defendant, prior to trial, such details as to the portion of the indictment or information at issue in the hearing as are needed to give the defendant fair notice to prepare for the hearing.



Comparison with M.R.E. 505. The notice requirement of CIPA § 6(b) is found in M.R.E. 505(i)(4)(A). While this notice provision under CIPA and 505 are similar, including the same “generic category” language, there is no equivalent under 505 for CIPA § 6(b)(2) due to military practice differences.

(c) Alternative procedure for disclosure of classified information.

(1) Upon any determination by the court authorizing the disclosure of specific classified information under the procedures established by this section, the United States may move that, in lieu of the disclosure of such specific classified information, the court order--

(A) the substitution for such classified information of a statement admitting relevant facts that the specific classified information would tend to prove; or

(B) the substitution for such classified information of a summary of the specific classified information.

The court shall grant such a motion of the United States if it finds that the statement or summary will provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information. The court shall hold a hearing on any motion under this section. Any such hearing shall be held in camera at the request of the Attorney General.

(2) The United States may, in connection with a motion under paragraph (1), submit to the court an affidavit of the Attorney General certifying that disclosure of classified information would cause identifiable damage to the national security of the United States and explaining the basis for the classification of such information. If so requested by the United States, the court shall examine such affidavit in camera and ex parte.



Comparison with M.R.E. 505. This section is one that is very different from the comparable M.R.E. 505 section and highlights the primary difference between the Federal and military systems. CIPA does not provide the Government with the ability to close a courtroom to the general public and CIPA therefore is only applicable to pre-trial evidentiary issues.

In Federal court, if a judge rules that the information must be disclosed, all the government can do is try to provide an acceptable substitute and have the judge conduct an *ex parte in camera* review of the information and the proposed substitute. The judge “shall” approve a substitute if the “statement or summary will provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information.”

In contrast, since a court-martial can be closed to all but cleared and necessary parties under M.R.E. 505(j)(5), the standard for disclosure to an accused is different. 505(i)(4)(B) states that classified information is NOT subject to disclosure “unless the information is relevant and necessary to an element of the offense or a legally cognizable defense and is otherwise admissible in evidence.” 505(i)(4)(D) then addresses alternatives to full disclosure, similar to CIPA, with the exception that the military judge can determine that the “use of the information itself is necessary to afford the accused a fair trial.” In Federal court this result would likely result in a case or charges being dismissed, but in a court-martial, the possibility of disclosure only in a closed proceeding may ameliorate the possible damage to national security enough to permit the court to proceed.

(d) Sealing of records of in camera hearings. If at the close of an in camera hearing under this Act (or any portion of a hearing under this Act that is held in camera) the court determines that the classified information at issue may not be disclosed or elicited at the trial or pretrial proceeding, the record of such in camera hearing shall be sealed and preserved by the court for use in the event of an appeal. The defendant may seek reconsideration of the court's determination prior to or during trial.



Comparison with M.R.E. 505. The sealing requirement of CIPA § 6(d) is found in M.R.E. 505(i)(4)(C). While this notice provision under CIPA and 505 are very similar, 505 requires the record of any in camera proceeding to be attached to the record, not only those where disclosure is denied. This is perhaps a reflection of the mandatory appellate review in the military system. Attachment of the “entire unaltered text of the relevant documents” to a sealed record of trial is also required by 505(g)(4).

(e) Prohibition on disclosure of classified information by defendant, relief for defendant when United States opposes disclosure.

(1) Whenever the court denies a motion by the United States that it issue an order under subsection (c) and the United States files with the court an affidavit of the Attorney General objecting to disclosure of the classified information at issue, the court shall order that the defendant not disclose or cause the disclosure of such information.

(2) Whenever a defendant is prevented by an order under paragraph (1) from disclosing or causing the disclosure of classified information, the court shall dismiss the indictment or information; except that, when the court determines that the interests of justice would not be served by dismissal of the indictment or information, the court shall order such other action, in lieu of dismissing the indictment or information, as the court determines is appropriate. Such action may include, but need not be limited to--

(A) dismissing specified counts of the indictment or information;

(B) finding against the United States on any issue as to which the excluded classified information relates; or

(C) striking or precluding all or part of the testimony of a witness.

An order under this paragraph shall not take effect until the court has afforded the United States an opportunity to appeal such order under section 7, and thereafter to withdraw its objection to the disclosure of the classified information at issue.



Comparison with M.R.E. 505. The remedies section of CIPA § 6(e) is found in M.R.E. 505(i)(4)(E). While again the provisions under CIPA and 505 are similar, 505 has differences that are related to military practice. One notable omission from 505 is the ability of the Government to seek an interlocutory appeal of a judge's decision and ordered sanction under 505(i)(4)(E) and seek a stay of proceedings pending that appeal. However, as discussed below with respect to CIPA § 7, this is remedied in R.C.M. 908, which specifically addresses the availability of an interlocutory appeal of an “order or ruling that ... directs the disclosure of classified information...” and contains provisions for seeking stays of proceedings.

(f) Reciprocity. Whenever the court determines pursuant to subsection (a) that classified information may be disclosed in connection with a trial or pretrial proceeding, the court shall, unless the interests of fairness do not so require, order the United States to provide the defendant with the information it expects to use to rebut the classified information. The court may place the United States under a continuing duty to disclose such rebuttal information. If the United States fails to comply with its obligation under this subsection, the court may exclude any evidence not made the subject of a required disclosure and may prohibit the examination by the United States of any witness with respect to such information.



Comparison with M.R.E. 505. CIPA § 6(f) has no counterpart in M.R.E. 505. The Government has no formal requirement for reciprocal discovery, *i.e.*, to provide the defendant with the information it expects to use to rebut the classified information. While this will likely be the subject of a timely motion by astute defense counsel and generally ordered by a military judge (if not already provided *sua sponte* by the Government), in the event that reciprocal discovery is litigated, counsel should be aware that only CIPA has this requirement.

§ 7. Interlocutory appeal

(a) An interlocutory appeal by the United States taken before or after the defendant has been placed in jeopardy shall lie to a court of appeals from a decision or order of a district court in a criminal case authorizing the disclosure of classified information, imposing sanctions for nondisclosure of classified information, or refusing a protective order sought by the United States to prevent the disclosure of classified information.

(b) An appeal taken pursuant to this section either before or during trial shall be expedited by the court of appeals. Prior to trial, an appeal shall be taken within ten days after the decision or order appealed from and the trial shall not commence until the appeal is resolved. If an appeal is taken during trial, the trial court shall adjourn the trial until the appeal is resolved and the court of appeals (1) shall hear argument on such appeal within four days of the adjournment of the trial, (2) may dispense with written briefs other than the supporting materials previously submitted to the trial court, (3) shall render its decision within four days of argument on appeal, and (4) may dispense with the issuance of a written opinion in rendering its decision. Such appeal and decision shall not affect the right of the defendant, in a subsequent appeal from a judgment of conviction, to claim as error reversal by the trial court on remand of a ruling appealed from during trial.



Comparison with M.R.E. 505. As noted above in the discussion under CIPA § 6(e), there is no specific provision in 505 for the Government to seek an interlocutory appeal of a judge's decision and ordered sanction under 505(i)(4)(E) or to seek a stay of proceedings pending that appeal. However, this is remedied in R.C.M. 908, which specifically addresses the availability of an interlocutory appeal of an "order or ruling that ... directs the disclosure of classified information..." and contains provisions for seeking stays of proceedings and expedited reviews by the Courts of Criminal Appeal.

§ 8. *Introduction of classified information*

(a) Classification status. Writings, recordings, and photographs containing classified information may be admitted into evidence without change in their classification status.

(b) Precautions by court. The court, in order to prevent unnecessary disclosure of classified information involved in any criminal proceeding, may order admission into evidence of only part of a writing, recording, or photograph, or may order admission into evidence of the whole writing, recording, or photograph with excision of some or all of the classified information contained therein, unless the whole ought in fairness be considered.

(c) Taking of testimony. During the examination of a witness in any criminal proceeding, the United States may object to any question or line of inquiry that may require the witness to disclose classified information not previously found to be admissible. Following such an objection, the court shall take such suitable action to determine whether the response is admissible as will safeguard against the compromise of any classified information. Such action may include requiring the United States to provide the court with a proffer of the witness' response to the question or line of inquiry and requiring the defendant to provide the court with a proffer of the nature of the information he seeks to elicit.



Comparison with M.R.E. 505. CIPA § 8 is contained within M.R.E. 505(j), one of two primarily procedural provisions of 505 that do not seem to require the 505 privilege assertion sections to have effect. 505(j)(1) and (2) are identical to CIPA § 8(a) and (b), respectively, while 505(j)(4) is very similar to CIPA § 8(c). CIPA has no direct counterpart to (j)(3), though CIPA § 6(c) is similar. As mentioned earlier, CIPA contains no authority to close a courtroom and therefore there is no analog to 505(j)(5). 505(j)(6) is a military procedural provision regarding record of trial preparation that has no counterpart in CIPA.

§ 9. *Security procedures*

(a) Within one hundred and twenty days of the date of the enactment of this Act [enacted Oct. 15, 1980], the Chief Justice of the United States, in consultation with the Attorney General, the Director of National Intelligence, and the Secretary of Defense, shall prescribe rules establishing procedures for the protection against unauthorized disclosure of any classified information in the custody of the United States district courts, courts of appeal, or Supreme Court. Such rules, and any changes in such rules, shall be submitted to the appropriate committees of Congress and shall become effective forty-five days after such submission.

(b) Until such time as rules under subsection (a) first become effective, the Federal courts shall in each case involving classified information adopt procedures to protect against the unauthorized disclosure of such information.

[The Security Procedures are set forth in the text following the statute in the U.S. Code Annotated. These Procedures are not applicable to a court-martial but may be used as guidance in establishing a security plan. See also Chapter 6 of this Guide.]

§ 9A. Coordination requirements relating to the prosecution of cases involving classified information

(a) Briefings required. Appropriate United States attorney, or the designees of such officials, shall provide briefings to the senior agency official, or the designee of such official, with respect to any case involving classified information that originated in the agency of such senior agency official.

(b) Timing of briefings. Briefings under subsection (a) with respect to a case shall occur--

(1) as soon as practicable after the Department of Justice and the United States attorney concerned determine that a prosecution or potential prosecution could result; and

(2) at such other times thereafter as are necessary to keep the senior agency official concerned fully and currently informed of the status of the prosecution.

(c) Senior agency official defined. In this section, the term "senior agency official" has the meaning given that term in section 1.1 of Executive Order No. 12958 [50 USCS § 435 note].



Comparison with M.R.E. 505. No M.R.E. 505 counterpart. *But see* the National Security Case requirements and coordination requirements discussed in Chapters 3, 4, and 7!

§ 10. Identification of information related to the national defense

In any prosecution in which the United States must establish that material relates to the national defense or constitutes classified information, the United States shall notify the defendant, within the time before trial specified by the court, of the portions of the material that it reasonably expects to rely upon to establish the national defense or classified information element of the offense.



Comparison with M.R.E. 505. No M.R.E. 505 or specific military practice counterpart. However, if the Government is charging an accused under Federal statutes that have as elements of an offense that "material relates to the national defense or constitutes classified information" normal court-martial practice would generally include notice of the evidence to be relied upon. If not provided or if unclear, a defense counsel may decide that a motion for a bill of particulars or other motion may be appropriate.

[§§11- 16 Miscellaneous Administrative Provisions. (Omitted from this Annex)]

2054 Synopsis of Classified Information Procedures Act (CIPA)

[From Title 9 U.S. Attorney's Manual Criminal Resource Manual]

I. DEFINITIONS, PRETRIAL CONFERENCE, PROTECTIVE ORDERS AND DISCOVERY

After a criminal indictment becomes public, the prosecutor remains responsible for taking reasonable precautions against the unauthorized disclosure of classified information during the case. This responsibility applies both when the government intends to use classified information in its case-in-chief as well as when the defendant seeks to use classified information in his/her defense. The tool with which the proper protection of classified information may be ensured in indicted cases is the Classified Information Procedures Act (CIPA). *See* Title 18, U.S.C. App III.

CIPA is a procedural statute; it neither adds to nor detracts from the substantive rights of the defendant or the discovery obligations of the government. Rather, the procedure for making these determinations is different in that it balances the right of a criminal defendant with the right of the sovereign to know in advance of a potential threat from a criminal prosecution to its national security. *See, e.g., United States v. Anderson*, 872 F.2d 1508, 1514 (11th Cir.), *cert. denied*, 493 U.S. 1004 (1989); *United States v. Collins*, 720 F.2d 1195, 1197 (11th Cir. 1983); *United States v. Lopez-Lima*, 738 F. Supp. 1404, 1407 (S.D.Fla. 1990). Each of CIPA's provisions is designed to achieve those dual goals: preventing unnecessary or inadvertent disclosures of classified information and advising the government of the national security "cost" of going forward.

A. *Definitions of Terms*

Section 1 of CIPA defines "classified information" and "national security," both of which are terms used throughout the statute. Subsection (a), in pertinent part, defines "classified information" as:

[A]ny 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.

Subsection (b) defines "national security" to mean the "national defense and foreign relations of the United States."

B. *Pretrial Conference*

Section 2 provides that "[a]t any time after the filing of the indictment or information, any party may move for a pretrial conference to consider matters relating to classified information that may arise in connection with the prosecution." Following such a motion, the district court "shall promptly hold a pretrial conference to establish the timing of requests for discovery, the provision of notice required by Section 5 of this Act, and the

initiation of the procedure established by Section 6 (to determine the use, relevance, or admissibility of classified information) of this Act."

C. Protective Orders

Of critical importance in any criminal case, once there exists any likelihood that classified information may be at issue, is the entering of a protective order by the district court. CIPA Section 3 requires the court, upon the request of the government, to issue an order "to protect against the disclosure of any classified information disclosed by the United States to any defendant in any criminal case." The government's motion for a protective order is an excellent opportunity to begin educating the Court, including the judge's staff, about CIPA and related issues. It is essential that the motion include a memorandum of law that provides the court with an overview on national security matters and sets forth the authority by which the government may protect matters of national security, including the general authority of the Intelligence Community (IC) pursuant to the National Security Act of 1947, the Central Intelligence Act of 1949, and various Executive orders issued by the President. For sample motions and protective orders or to discuss any problems you may have with the court on CIPA issues, please contact the ISS. The protective order must be sufficiently comprehensive to ensure that access to classified information is restricted to cleared persons and to provide for adequate procedures and facilities for proper handling and protection of classified information during the pre-trial litigation and trial of the case.

The requirement of security clearances does not extend to the judge or to the defendant (who would likely be ineligible, anyway). Some defense counsel may wish to resist this requirement by seeking an exemption by order of the court. The prosecutor should advise defense counsel that, because of the stringent restrictions imposed by federal regulations, statutes, and Executive Orders upon the disclosure of classified information, such tack may prevent, and will certainly delay, access to classified information. In any case in which this issue arises, the prosecutor should notify the Internal Security Section immediately.

An essential provision of a protective order is the appointment by the court of a Court Security Officer (CSO). The CSO is an employee of the Department's Justice Management Division; however, the court's appointment of a CSO makes that person an officer of the court. In that capacity, the CSO is responsible for assisting both parties and the court staff in obtaining security clearances (not required for the judge); in the proper handling and storage of classified information, and in operating the special communication equipment that must be used in dealing with classified information.

D. Discovery of Classified Information by Defendant

Section 4 provides in pertinent part that "[t]he court, upon a sufficient showing, may authorize the United States to delete specified items of classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure, to substitute a summary of the information for such classified documents, or to substitute a statement admitting the relevant facts that classified information would tend to prove." Like Rule 16(d)(1) of the Federal Rules of

Criminal Procedure, section 4 provides that the Government may demonstrate that the use of such alternatives is warranted in an *in camera*, *ex parte* submission to the court. By the time of the section 4 proceeding, the prosecutor should have completed the government's review of any classified material and have identified any such material that is arguably subject to the government's discovery obligation. Where supported by law, the prosecutor, during the proceeding, should first strive to have the court exclude as much classified information as possible from the government's discovery obligation. Second, to the extent that the court rules that certain classified material is discoverable, the prosecutor should seek the court's approval to utilize the alternative measures described in section 4, i.e., unclassified summaries and/or stipulations. The court's denial of such a request is subject to interlocutory appeal. *See* Section III.A, *infra*.

II. SECTIONS 5 AND 6: NOTICE AND PRETRIAL EVIDENTIARY RULINGS

NOTICE OF INTENT TO USE CLASSIFIED INFORMATION

Following the discovery process under section 4, there are three critical pretrial steps in the handling of classified information under sections 5 and 6 of CIPA. First, the defendant must specify in detail, in a written notice, the precise classified information he reasonably expects to disclose. Second, the Court, upon a motion of the Government, shall hold a hearing pursuant to section 6(a) to determine the use, relevance and admissibility of the proposed evidence. Third, following the 6(a) hearing and formal findings of admissibility by the Court, the Government may move to substitute redacted versions of classified documents from the originals or to prepare an admission of certain relevant facts or summaries for classified information that the Court has ruled admissible.

A. The Section 5(a) Notice Requirement

PRETRIAL EVIDENTIARY HEARING, SUBSTITUTIONS AND STIPULATIONS

The linchpin of CIPA is section 5(a), which requires a defendant who reasonably intends to disclose (or cause the disclosure of) classified information to provide timely pretrial written notice of his intention to the Court and the Government. Section 5(a) expressly requires that such notice "include a brief description of the classified information," and the leading case under section 5(a) holds that such notice

must be *particularized*, setting forth *specifically* the classified information which the defendant reasonably believes to be necessary to his defense.

United States v. Collins, 720 F.2d 1195, 1199 (11th Cir. 1983) (emphasis added) *See also United States v. Smith*, 780 F.2d 1102, 1105 (4th Cir. 1985) (*en banc*). This requirement applies both to documentary exhibits and to oral testimony, whether it is anticipated to be brought out on direct or on cross-examination. *See, e.g., United States v. Collins, supra*, (testimony); *United States v. Wilson*, 750 F.2d 7 (2d Cir. 1984) (same).

If a defendant fails to provide a sufficiently detailed notice far enough in advance of trial to permit the implementation of CIPA procedures, section 5(b) provides for preclusion. *See United States v. Badia*, 827 F.2d 1458, 1465 (11th Cir. 1987). Similarly, if the defendant attempts to disclose at trial classified information which is not described in

his/her section 5(a) notice, preclusion is the appropriate remedy prescribed by section 5(b) of the statute. *See United States v. Smith, supra*, 780 F.2d at 1105 ("A defendant is forbidden from disclosing any such information absent the giving of notice").

B. The Section 6(a) Hearing

The purpose of the hearing pursuant to section 6(a) of CIPA is for the court "to make all determinations concerning the use, relevance, or admissibility of classified information that would otherwise be made during the trial...." 18 U.S.C. App. III § 6(a). The statute expressly provides that, after a pretrial section 6(a) hearing on the admissibility of evidence, the court shall enter its rulings *prior* to the commencement of trial. If the Attorney General or his/her designee certifies to the court in a petition that a public proceeding may result in the disclosure of classified information, then the hearing will be held *in camera*. CIPA does not change the "generally applicable evidentiary rules of admissibility," *United States v. Wilson, supra* 750 F.2d at 9, but rather alters the *timing* of rulings as to admissibility to require them to be made before the trial. *Accord, United States v. Smith, supra*, 780 F.2d at 1106.

At the section 6(a) hearing, the court is to hear the defense proffer and the arguments of counsel, and then rule whether the classified information identified by the defense is relevant under the standards of Fed.R.Evid. 401. *United States v. Smith, supra*, 780 F.2d at 1106. The court's inquiry does not end there, for under Fed.R.Evid. 402, not all relevant evidence is admissible at trial. The Court therefore must also determine whether the evidence is cumulative, prejudicial, confusing, or misleading," *United States v. Wilson, supra*, 750 F.2d at 9, so that it should be excluded under Fed.R.Evid. 403. At the conclusion of the section 6 (a) hearing, the court must state in writing the reasons for its determination as to each item of classified information. 18 U.S.C. App. III section 6(a).

C. Substitution Pursuant to Section 6(c)

If the court rules any classified information to be admissible, section 6(c) of CIPA permits the Government to propose unclassified "substitutes" for that information. Specifically, the Government may move to substitute either (1) a statement admitting relevant facts that the classified information would tend to prove or (2) a summary of the classified information instead of the classified information itself. 18 U.S.C. App. III section 6(c)(1). *See United States v. Smith, supra*, 780 F.2d at 1105. In many cases, the government will propose a redacted version of a classified document as a substitution for the original, having deleted only non-relevant classified information. A motion for substitution shall be granted if the "statement or summary will provide the defendant with substantially the same ability to make his defense as would disclosure of the specified classified information." 18 U.S.C. App. III section 6(c).

If the district court will not accept a substitution proposed by the government, an interlocutory appeal may lie to the circuit court under CIPA section 7. If the issue is resolved against the government, and classified information is thereby subject to a disclosure order of the court, the AUSA must immediately notify the ISS. Thereafter, the Attorney General may file an affidavit effectively prohibiting the use of the contested

classified information. If that is done, the court may impose sanctions against the government, which may include striking all or part of a witness' testimony, resolving an issue of fact against the United States, or dismissing part or all of the indictment. *See* CIPA section 6(e). The purpose of the relevance hearings under 6(a) and the substitution practice under 6(c), however, is to avoid the *necessity* for these sanctions.

III. OTHER RELEVANT CIPA PROCEDURES

A. Interlocutory Appeal

APPEAL FROM INTERLOCUTORY ORDER

Section 7(a) of the Act provides for an interlocutory appeal by the government from any decision or order of the trial judge authorizing the disclosure of classified information, imposing sanctions for nondisclosure of classified information, or refusing a protective order sought by the United States to prevent the disclosure of classified information. Section 7 appeals must be approved by the Solicitor General. The term "disclosure" within the meaning of section 7 includes both information which the court orders the government to divulge to the defendant or to others as well as information already possessed by the defendant which he or she intends to disclose to unapproved people. Section 7(b) provides that the court of appeals shall give expedited treatment to any interlocutory appeal filed under subsection (a). As a matter of *fairness*, the policy of the Department shall be that the defense be given notice of the government's appeal under section 7.

B. Introduction of Classified Information

Section 8(a) provides that "writings, recordings, and photographs containing classified information may be admitted into evidence without change in their classification status." This provision simply recognizes that classification is an executive, not a judicial, function. Thus, section 8(a) implicitly allows the classifying agency, upon completion of the trial, to decide whether the information has been so compromised during trial that it could no longer be regarded as classified.

In order to prevent "unnecessary disclosure" of classified information, section 8(b) permits the court to order admission into evidence of only a part of a writing, recording, or photograph. Alternatively, the court may order into evidence the whole writing, recordings, or photograph with excision of all or part of the classified information contained therein. However, the provision does not provide grounds for excluding or excising part of a writing or recorded statement which ought in fairness to be considered contemporaneously with it. Thus, the court may admit into evidence part of a writing, recording, or photograph only when fairness does not require the whole document to be considered.

Section 8(c) provides a procedure to address the problem presented during a pretrial or trial proceeding when the defendant's counsel asks a question or embarks on a line of inquiry that would require the witness to disclose classified information not previously

found by the court to be admissible. If the defendant knew that a question or line of inquiry would result in disclosure of classified information, he/she presumably would have given the government notice under section 5 and the provisions of section 6(a) would have been used. Section 8(c) serves, in effect, as a supplement to the hearing provisions of section 6(a) to cope with situations which cannot be handled effectively under that section, e.g., where the defendant does not realize that the answer to a given question will reveal classified information. Upon the government's objection to such a question, the court is required to take suitable action to avoid the improper disclosure of classified information.

C. Security Procedures

Section 9 required the Chief Justice of the United States to prescribe security procedures for the protection of classified information in the custody of Federal courts. On February 12, 1981, Chief Justice Burger promulgated these procedures. For further information regarding those procedures, please contact the Justice Management Division Office of Security, (202) 514-2094.

D. Public Testimony By Intelligence Officers

Although the IC is committed to assisting law enforcement where it is legally proper to do so, it must also remain vigilant in protecting classified national security information from unauthorized disclosure. Just as with law enforcement agencies, the successful functioning of the IC turns in significant part upon the ability of its intelligence officers covertly to obtain information from human sources. In carrying out that task, the intelligence officers must, when necessary, be able to operate anonymously, that is, without their connection to an intelligence agency of the United States being known to the persons with whom they come in contact. For that reason, an intelligence agency is authorized under Executive Order 12958 to classify the true name of an intelligence officer.

During the pre-trial progression of an indicted case, as the court enters its CIPA rulings under sections 4 and 6, it may become apparent to the prosecutor that testimony may be required from an intelligence officer or other agency representative engaged in covert activity, either because the Court has ruled under CIPA that certain evidence is relevant and admissible in the defense case, or because such testimony is necessary in the government's rebuttal. Just as the substance of that testimony, to the extent it is classified and is being offered by the defense, must be the subject of CIPA determinations by the court, the prosecutor must also ensure that the same considerations are afforded to the true names of covert intelligence community personnel, if those true names are classified information. That is, the prosecutor must seek the court's approval, under either CIPA section 4 or section 6, of an alternative method to the witness' testimony in true name that will provide the defendant with the same ability that he would have otherwise had to impeach, or bolster, the credibility of that witness.

In any criminal case in which it becomes likely that an intelligence agency employee will testify, the Assistant United States Attorney (AUSA) assigned to the case shall

FOR OFFICIAL USE ONLY

immediately notify the Internal Security Section (ISS). That office, in consultation with the general counsel at the appropriate intelligence agency, will assist the AUSA during pretrial motion practice and litigation on the issue of whether the witness should testify in true name and other issues related to the testimony of intelligence agency personnel.



Department of Defense **INSTRUCTION**

NUMBER 5525.07

June 18, 2007

GC, DoD/IG DoD

SUBJECT: Implementation of the Memorandum of Understanding (MOU) Between the Departments of Justice (DoJ) and Defense Relating to the Investigation and Prosecution of Certain Crimes

- References:**
- (a) DoD Directive 5525.7, "Implementation of the Memorandum of Understanding Between the Department of Justice and the Department of Defense Relating to the Investigation and Prosecution of Crimes," January 22, 1985 (hereby canceled)
 - (b) Acting Deputy Secretary of Defense Memorandum, "DoD Directives Review - Phase II," July 13, 2005
 - (c) DoD Directive 5145.1, "General Counsel of the Department of Defense," May 2, 2001
 - (d) DoD Directive 5106.01, "Inspector General of the Department of Defense," April 13, 2006
 - (e) through (h), see Enclosure 1

1. REISSUANCE AND PURPOSE

This Instruction:

1.1. Reissues Reference (a) as a DoD Instruction in accordance with the guidance in Reference (b) and the authority in References (c) and (d).

1.2. Updates policy, assigns responsibilities, and supplements the MOU between the Departments of Justice and Defense Relating to the Investigation and Prosecution of Certain Crimes (Reference (e)) at Enclosure 1, pursuant to References (c) and (d).

2. APPLICABILITY AND SCOPE

2.1. This Instruction applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense (IG DoD), the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components").

2.2. The term “DoD criminal investigative organizations,” as used herein, refers collectively to the United States Army Criminal Investigation Command, Naval Criminal Investigative Service, U.S. Air Force Office of Special Investigations, and Defense Criminal Investigative Service, Office of the IG DoD.

3. POLICY

It is DoD policy to maintain effective working relationships with the DoJ in the investigation and prosecution of crimes involving DoD programs, operations, or personnel.

4. PROCEDURES

With respect to inquiries for which the DoJ has assumed investigative responsibility based on Reference (e), the DoD criminal investigative organizations should seek to participate jointly with DoJ investigative agencies whenever the inquiries relate to DoD programs, operations, or personnel. This applies to cases referred to the Federal Bureau of Investigation under paragraph C.1.a. of Reference (e) as well as to those cases for which a DoJ investigative agency is assigned primary investigative responsibility by a DoJ prosecutor. The DoD Components shall comply with the terms of Reference (e) and DoD Supplemental Guidance in Enclosure 2.

5. RESPONSIBILITIES

5.1. The IG DoD, shall:

5.1.1. Establish procedures to implement the investigative policies set forth in this Instruction.

5.1.2. Monitor compliance by DoD criminal investigative organizations with the terms of Reference (c).

5.1.3. Provide specific guidance regarding investigative matters, as appropriate.

5.2. The General Counsel of the Department of Defense (GC, DoD), shall:

5.2.1. Establish procedures to implement the prosecutive policies as set forth in Reference (e) and consistent with the DoD Supplemental Guidance provided in Enclosure 2, the Uniform Code of Military Justice (Reference (f)) and the Manual for Courts-Martial (Reference (g)).

5.2.2. Monitor compliance by the DoD Components regarding the prosecutive aspects of Reference (e).

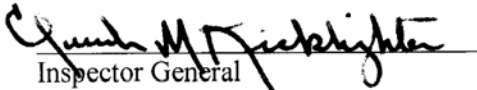
5.2.3. Provide specific guidance on the investigation and prosecution of those crimes addressed in Reference (e), as appropriate.

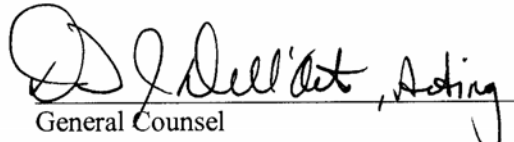
5.2.4. Modify the DoD Supplemental Guidance in Enclosure 2 with the concurrence of the IG DoD, after coordinating with the affected DoD Components.

5.3. The Secretaries of the Military Departments shall establish procedures to implement the policies set forth in this Instruction.

6. EFFECTIVE DATE

This Instruction is effective immediately upon signing by both of the following, whichever date is later.


Inspector General
Department of Defense


General Counsel
Department of Defense

Enclosures – 2

E1. References, continued

E2. DoD Supplemental Guidance to the MOU Between the Departments of Justice and Defense Relating to the Investigation and Prosecution of Certain Crimes

E1. ENCLOSURE 1

REFERENCES, continued

- (e) Memorandum of Understanding between the Departments of Justice and Defense Relating to the Investigation and Prosecution of Certain Crimes, August 1981¹
- (f) Chapter 47 of title 10, United States Code, “Uniform Code of Military Justice (UCMJ)”
- (g) Manual for Courts-Martial, United States, 2005 (R.C.M. 704)
- (h) Title 18 of the United States Code

¹For copies of the signed Memorandum of Understanding, contact the Office of the Deputy General Counsel (Personnel and Health Policy), 1600 Defense Pentagon, Washington, D.C. 20301-1600.

E2. ENCLOSURE 2

DoD SUPPLEMENTAL GUIDANCE TO THE MOU BETWEEN THE DEPARTMENTS OF JUSTICE AND DEFENSE RELATING TO THE INVESTIGATION AND PROSECUTION OF CERTAIN CRIMES

This enclosure contains the verbatim text of Reference (e). Matter that is identified as “DoD Supplemental Guidance” has been added by the Department of Defense. DoD Components shall comply with the MOU and the DoD Supplemental Guidance.

MEMORANDUM OF UNDERSTANDING BETWEEN THE DEPARTMENTS OF JUSTICE AND DEFENSE RELATING TO THE INVESTIGATION AND PROSECUTION OF CERTAIN CRIMES

A. PURPOSE, SCOPE AND AUTHORITY

This Memorandum of Understanding (MOU) establishes policy for the Department of Justice and the Department of Defense with regard to the investigation and prosecution of criminal matters over which the two Departments have jurisdiction. This memorandum is not intended to confer any rights, benefits, privileges or form of due process procedure upon individuals, associations, corporations, or other persons or entities.

This Memorandum applies to all components and personnel of the Department of Justice and the Department of Defense. The statutory bases for the Department of Defense and the Department of Justice investigation and prosecution responsibilities include, but are not limited to:

1. Department of Justice: Titles 18, 21 and 28 of the United States Code; and
2. Department of Defense: The Uniform Code of Military Justice, Title 10, United States Code, Sections 801-940; the Inspector General Act of 1978, Title 5 United States Code, Appendix 3; and Title 5 United States Code, Section 301.

B. POLICY

The Department of Justice has primary responsibility for enforcement of federal laws in the United States District Courts. The Department of Defense has responsibility for the integrity of its programs, operations and installations and for the discipline of the Armed Forces. Prompt administrative actions and completion of investigations within the two (2) year statute of limitations under the Uniform Code of Military Justice require the Department of Defense to assume an important role in federal criminal investigations. To encourage joint and coordinated investigative efforts, in appropriate cases where the Department of Justice assumes investigative responsibility for a matter relating to the Department of Defense, it should share information and conduct the inquiry jointly with the interested Department of Defense investigative agency.

It is neither feasible nor desirable to establish inflexible rules regarding the responsibilities of the Department of Defense and the Department of Justice as to each matter over which they may have concurrent interest. Informal arrangements and agreements within the spirit of this MOU are permissible with respect to specific crimes or investigations.

C. INVESTIGATIVE AND PROSECUTIVE JURISDICTION

1. CRIMES ARISING FROM THE DEPARTMENT OF DEFENSE OPERATIONS

a. Corruption Involving the Department of Defense Personnel

The Department of Defense investigative agencies will refer to the FBI on receipt all significant allegations of bribery and conflict of interest involving military or civilian personnel of the Department of Defense. In all corruption matters that are the subject of a referral to the FBI, the Department of Defense shall obtain the concurrence of the Department of Justice prosecutor or the FBI before initiating any independent investigation preliminary to any action under the Uniform Code of Military Justice. If the Department of Defense is not satisfied with the initial determination, the matter will be reviewed by the Criminal Division of the Department of Justice.

The FBI will notify the referring agency promptly regarding whether they accept the referred matters for investigation. The FBI will attempt to make such decision in one (1) working day of receipt in such matters.

DoD Supplemental Guidance

A. Certain bribery and conflict of interest allegations (also referred to as “corruption” offenses in the MOU) are to be referred immediately to the FBI.

B. For the purposes of this section, bribery and conflict of interest allegations are those which would, if proven, violate sections 201, 203, 205, 208, 209, or 219 of title 18, United States Code (Reference (h)).

C. Under paragraph C.1.a., DoD criminal investigative organizations shall refer to the FBI those “significant” allegations of bribery and conflict of interest that implicate directly military or DoD civilian personnel, including allegations of bribery or conflict of interest that arise during the course of an ongoing investigation.

1. All bribery and conflict of interest allegations against present, retired, or former General or Flag officers and civilians in positions above the GS-15 and equivalent levels, the Senior Executive Service, and the Executive Level will be considered “significant” for purposes of referral to the FBI.

2. In cases not covered by subsection C.1., of this supplemental guidance, the determination of whether the matter is “significant” for purposes of referral to the FBI should be made in light of the following factors: sensitivity of the DoD program involved, amount of money in the alleged bribe, number of DoD personnel implicated, impact on the affected DoD program, and with respect to military personnel, whether the matter normally would be handled under Reference (f). Bribery and conflicts of interest allegations warranting consideration of Federal prosecution, which were not referred to the FBI based on the application of these guidelines and not otherwise disposed of under Reference (f), will be developed and brought to the attention of the Department of Justice through the “conference” mechanism described in paragraph C.1.b of Reference (e).

D. Bribery and conflict of interest allegations when military or DoD civilian personnel are not subjects of the investigations are not covered by the referral requirement of paragraph C.1.a. of Reference (e). Matters in which the suspects are solely DoD contractors and their subcontractors, such as commercial bribery between a DoD subcontractor and a DoD prime contractor, do not require referral upon receipt to the FBI. The “conference” procedure described in paragraph C.1.b. of Reference (e) shall be used in these types of cases.

E. Bribery and conflict of interest allegations that arise from events occurring outside the United States, its territories, and possessions, and requiring investigation outside the United States, its territories, and possessions need not be referred to the FBI.

F. The 1984 MOU references a two (2) year statute of limitations in effect for some Uniform Code of Military Justice offenses. Section 843 of Reference (f), governing statute of limitations has been amended several times since signing the MOU, applying generally a 5 year statute of limitation. It remains important that administrative actions and investigations be completed in a timely manner in order to meet the statute of limitations requirements for the respective offenses, while keeping in mind that the applicable statute of limitation of a particular offense is that which was in effect at the time the offense was committed.

b. Frauds Against the Department of Defense and Theft and Embezzlement of Government Property

The Department of Justice and the Department of Defense have investigative responsibility for frauds against the Department of Defense and theft and embezzlement of Government property from the Department of Defense. The Department of Defense will investigate frauds against the Department of Defense and theft of government property from the Department of Defense. Whenever a Department of Defense investigative agency identifies a matter which, if developed by investigation, would warrant federal prosecution, it will confer with the United States Attorney or the Criminal Division, the Department of Justice, and the FBI field office. At the time of this initial conference, criminal investigative responsibility will be determined by the Department of Justice in consultation with the Department of Defense.

DoD Supplemental Guidance

A. Unlike paragraph C.1.a. of Reference (e), paragraph C.1.b. does not have an automatic referral requirement. Under paragraph C.1.b, DoD criminal investigative organizations shall confer with the appropriate Federal prosecutor and the FBI on matters which, if developed by investigation, would warrant Federal prosecution. This “conference” serves to define the respective roles of DoD criminal investigative organizations and the FBI on a case-by-case basis. Generally, when a conference is warranted, the DoD criminal investigative organization shall arrange to meet with the prosecutor and shall provide notice to the FBI that such meeting is being held. Separate conferences with both the prosecutor and the FBI normally are not necessary.

B. When investigations are brought to the attention of the Federal Procurement Fraud Unit (FPFU), such contact will satisfy the “conference” requirements of paragraph C.1.b. of Reference (e) as both the prosecutor and the FBI.

C. Mere receipt by DoD criminal investigative organizations of raw allegations of fraud or theft does not require conferences with the DoJ and the FBI. Sufficient evidence should be developed before the conference to allow the prosecutor to make an informed judgment as to the merits of a case dependent upon further investigation. However, DoD criminal investigative organizations should avoid delay in scheduling such conferences, particularly in complex fraud cases, because an early judgment by a prosecutor can be of assistance in focusing the investigation on those matters that most likely will result in criminal prosecution.

2. CRIMES COMMITTED ON MILITARY INSTALLATIONS

a. Subject(s) can be Tried by Court-Martial or are Unknown

Crimes (other than those covered by paragraph C.1.) committed on a military installation will be investigated by the Department of Defense investigative agency concerned and, when committed by a person subject to the Uniform Code of Military Justice, prosecuted by the Military Department concerned. The Department of Defense will provide immediate notice to the Department of Justice of significant cases in which an individual subject/victim is other than a military member or dependent thereof.

b. One or More Subjects cannot be Tried by Court-Martial

When a crime (other than those covered by paragraph C.1.) has occurred on a military installation and there is reasonable basis to believe that it has been committed by a person or persons, some or all of whom are not subject to the Uniform Code of Military Justice, the Department of Defense investigative agency will provide immediate notice of the matter to the appropriate Department of Justice investigative agency unless the Department of Justice has relieved the Department of Defense of the reporting requirement for that type of class of crime.

DoD Supplemental Guidance

A. Subsection C.2. of Reference (e) addresses crimes committed on a military installation other than those listed in paragraphs C.1.a. (bribery and conflict of interest) and C.1.b. (fraud, theft, and embezzlement against the Government).

B. Unlike paragraph C.1.a. of Reference (e), which requires “referral” to the FBI of certain cases, and paragraph C.1.b, which requires “conference” with respect to certain cases, subsection C.2. requires only that “notice” be given to DoJ of certain cases. Relief from the reporting requirement of subsection C.2. may be granted by the local U.S. attorney as to types or classes of cases.

C. For purposes of paragraph C.2.a. (when the subjects can be tried by court-martial or are unknown), an allegation is “significant” for purposes of required notice to the DoJ only if the offense falls within the prosecutorial guidelines of the local U.S attorney. Notice should be given in other cases when the DoD Component believes that Federal prosecution is warranted or otherwise determines that the case may attract significant public attention.

3. CRIMES COMMITTED OUTSIDE MILITARY INSTALLATIONS BY PERSONS WHO CAN BE TRIED BY COURT-MARTIAL

a. Offense is Normally Tried by Court-Martial

Crimes (other than those covered by paragraph C.1.) committed outside a military installation by persons subject to the Uniform Code of Military Justice which, normally, are tried by court-martial will be investigated and prosecuted by the Department of Defense. The Department of Defense will provide immediate notice of significant cases to the appropriate Department of Justice investigative agency. The Department of Defense will provide immediate notice in all cases where one or more subjects is not under military jurisdiction unless the Department of Justice has relieved the Department of Defense of the reporting requirement for that type or class or crime.

DoD Supplemental Guidance

For purposes of this paragraph, an allegation is “significant” for purposes of required notice to the DoJ only if the offense falls within prosecutorial guidelines of the local U.S. attorney. Notice should be given in other cases when the DoD Component believes that Federal prosecution is warranted, or otherwise determines that the case may attract significant public attention.

b. Crimes Related to Scheduled Military Activities

Crimes related to scheduled Military activities outside of a military installation, such as organized maneuvers in which persons subject to the Uniform Code of Military Justice are suspects, shall be treated as if committed on a military installation for purposes of this Memorandum. The FBI or other Department of Justice investigative agency may assume jurisdiction with the concurrence of the United States Attorney or the Criminal Division, Department of Justice.

c. Offense is not Normally Tried by Court-Martial

When there are reasonable grounds to believe that a Federal crime (other than those covered by paragraph C.1.) normally not tried by court-martial, has been committed outside a military installation by a person subject to the Uniform Code of Military Justice, the Department of Defense investigative agency will immediately refer the case to the appropriate Department of Justice investigative agency unless the Department of Justice has relieved the Department of Defense of the reporting requirements for the type or class of crime.

D. REFERRALS AND INVESTIGATIVE ASSISTANCE

1. REFERRALS

Referrals, notices, reports, requests and the general transfer of information under this Memorandum normally should be between the FBI or other Department of Justice investigative agency and the appropriate Department of Defense investigative agency at the field level.

If a Department of Justice investigative agency does not accept a referred matter and the referring Department of Defense investigative agency then, or subsequently, believes that evidence exists supporting prosecution before civilian courts, the Department of Defense agency may present the case to the United States Attorney or the Criminal Division, Department of Justice, for review.

2. INVESTIGATIVE ASSISTANCE

In cases where a Department of Defense or Department of Justice investigative agency has primary responsibility and it requires limited assistance to pursue outstanding leads, the investigative agency requiring assistance will promptly advise the appropriate investigative agency in the other Department and, to the extent authorized by law and regulations, the requested assistance should be provided without assuming responsibility for the investigation.

E. PROSECUTION OF CASES

1. With the concurrence of the Department of Defense, the Department of Justice will designate such Department of Defense attorneys as it deems desirable to be Special Assistant United States Attorneys for use where the effective prosecution of cases may be facilitated by the Department of Defense attorneys.

2. The Department of Justice will institute civil actions expeditiously in United States District Courts whenever appropriate to recover monies lost as a result of crimes against the Department of Defense; the Department of Defense will provide appropriate assistance to facilitate such actions.

3. The Department of Justice prosecutors will solicit the views of the Department of Defense prior to initiating action against an individual subject to the Uniform Code of Military Justice.

4. The Department of Justice will solicit the views of the Department of Defense with regard to its Department of Defense-related cases and investigations in order to effectively coordinate the use of civil, criminal and administrative remedies.

DoD Supplemental Guidance

Prosecution of Cases and Grants of Immunity

A. The authority of court-martial convening authorities to refer cases to trial, approve pretrial agreements, and issue grants of immunity under Reference (f) extends only to trials by court-martial. In order to ensure that such actions do not preclude appropriate action by Federal civilian authorities in cases likely to be prosecuted in the U.S. district courts, court-martial convening authorities shall ensure that appropriate consultation as required by this enclosure has taken place before trial by court-martial, approval of a pretrial agreement, or issuance of a grant of immunity in cases when such consultation is required.

B. Only a general court-martial convening authority may grant immunity under Reference (f), and may do so only in accordance with Rule for Courts-Martial 704 of Reference (g).

1. Under Reference (f), there are two types of immunity in the military justice system:

a. A person may be granted transactional immunity from trial by court-martial for one or more offenses under Reference (f).

b. A person may be granted testimonial immunity, which is immunity from the use of testimony, statements, and any information directly or indirectly derived from such testimony or statements by that person in a later court-martial.

2. Before a grant of immunity under Reference (f), the general court-martial convening authority shall ensure that there has been appropriate consultation with the DoJ with respect to offenses in which consultation is required by this enclosure.

3. A proposed grant of immunity in a case involving espionage, subversion, aiding the enemy, sabotage, spying, or violation of rules or statutes concerning classified information or the foreign relations of the United States shall be forwarded to the GC, DoD for the purpose of consultation with the DoJ. The GC, DoD shall obtain the views of other appropriate elements of the Department of Defense in furtherance of such consultation.

C. The authority of court-martial convening authorities extends only to grants of immunity from action under Reference (f). Only the Attorney General or other authority designated under sections 6001-6005 of Reference (h) may authorize action to obtain a grant of immunity with respect to trials in the U.S. district courts.

F. MISCELLANEOUS MATTERS

1. THE DEPARTMENT OF DEFENSE ADMINISTRATIVE ACTIONS

Nothing in this Memorandum limits the Department of Defense investigations conducted in support of administrative actions to be taken by the Department of Defense. However, the Department of Defense investigative agencies will coordinate all such investigations with the appropriate Department of Justice prosecutive agency and obtain the concurrence of the Department of Justice prosecutor or the Department of Justice investigative agency prior to conducting any administrative investigation during the pendency of the criminal investigation or prosecution.

2. SPECIAL UNIFORM CODE OF MILITARY JUSTICE FACTORS

In situations where an individual subject to the Uniform Code of Military Justice is a suspect in any crime for which a Department of Justice investigative agency has assumed jurisdiction, if a Department of Defense investigative agency believes that the crime involves special factors relating to the administration and discipline of the Armed Forces that would justify its investigation, the Department of Defense investigative agency will advise the appropriate Department of Justice investigative agency or the Department of Justice prosecuting authorities of these factors. Investigation of such a crime may be undertaken by the appropriate Department of Defense investigative agency with the concurrence of the Department of Justice.

3. ORGANIZED CRIME

The Department of Defense investigative agencies will provide to the FBI all information collected during the normal course of agency operations pertaining to the element generally known as "organized crime" including both traditional (La Cosa Nostra) and nontraditional organizations whether or not the matter is considered prosecutable. The FBI should be notified of any investigation involving any element of organized crime and may assume jurisdiction of the same.

4. DEPARTMENT OF JUSTICE NOTIFICATIONS TO DEPARTMENT OF DEFENSE INVESTIGATIVE AGENCIES

a. The Department of Justice investigative agencies will promptly notify the appropriate Department of Defense investigative agency of the initiation of the Department of Defense related investigations which are predicated on other than a Department of Defense referral except in those rare instances where notification might endanger agents or adversely affect the investigation. The Department of Justice investigative agencies will also notify the Department of Defense of all allegations of the Department of Defense related crime where investigation is not initiated by the Department of Justice.

b. Upon request, the Department of Justice investigative agencies will provide timely status reports on all investigations relating to the Department of Defense unless the circumstances indicate such reporting would be inappropriate.

c. The Department of Justice investigative agencies will promptly furnish investigative results at the conclusion of an investigation and advise as to the nature of judicial action, if any, taken or contemplated.

d. If judicial or administrative action is being considered by the Department of Defense, the Department of Justice will, upon written request, provide existing detailed investigative data and documents (less any federal grand jury material, disclosure of which would be prohibited by Rule 6(e), Federal Rules of Criminal Procedure), as well as agent testimony for use in judicial or administrative proceedings, consistent with Department of Justice and other federal regulations. The ultimate use of the information shall be subject to the concurrence of the federal prosecutor during the pendency of any related investigation or prosecution.

5. TECHNICAL ASSISTANCE

a. The Department of Justice will provide to the Department of Defense all technical services normally available to federal investigative agencies.

b. The Department of Defense will provide assistance to the Department of Justice in matters not relating to the Department of Defense as permitted by law and implementing regulations.

6. JOINT INVESTIGATIONS

a. To the extent authorized by law, the Department of Justice investigative agencies and the Department of Defense investigative agencies may agree to enter into joint investigative endeavors, including undercover operations, in appropriate circumstances. However, all such investigations will be subject to Department of Justice guidelines.

b. The Department of Defense, in the conduct of any investigation that might lead to prosecution in Federal District Court, will conduct the investigation consistent with any Department of Justice guidelines. The Department of Justice shall provide copies of all relevant guidelines and their revisions.

DoD Supplemental Guidance

When DoD procedures concerning apprehension, search and seizure, interrogation, eyewitnesses, or identification differ from those of DoJ, DoD procedures will be used, unless the DoJ prosecutor has directed that DoJ procedures be used instead. DoD criminal investigators should bring to the attention of the DoJ prosecutor, as appropriate, situations when use of DoJ procedures might impede or preclude prosecution under Reference (f).

7. APPREHENSION OF SUSPECTS

To the extent authorized by law, the Department of Justice and the Department of Defense will each promptly deliver or make available to the other suspects, accused individuals and witnesses where authority to investigate the crimes involved is lodged in the other Department. This MOU neither expands nor limits the authority of either Department to perform apprehensions, searches, seizures, or custodial interrogations.

G. EXCEPTION

This Memorandum shall not affect the investigative authority now fixed by the 1979 "Agreement Governing the Conduct of the Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation" and the 1983 Memorandum of Understanding between the Department of Defense, the Department of Justice and the FBI concerning "Use of Federal Military Force in Domestic Terrorist Incidents."