The Judge Advocate's Handbook For Litigating National Security Cases

Prosecuting, Defending and Adjudicating National Security Cases

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

THE JUDGE ADVOCATE'S HANDBOOK FOR LITIGATING NATIONAL SECURITY CASES

Table of Contents

Preface

National security cases involving classified evidence and testimony present challenges that are outside the realm of normal military justice practice. These cases, particularly those that involve the divulging national secrets, are among the most serious and evoke intense emotions. The evidentiary process by which classified information is presented during hearings closed to the public is complex. The use of classified material at trial imposes significant logistical burdens on Government and defense counsel alike. The procedures and statutes that govern the use of classified evidence are only infrequently encountered in court-martial practice. Therefore, early planning, study, team building, and interagency consultation are the *sine qua non* to the satisfactory resolution of these uniquely complex cases.

The National Security Litigation and Intelligence Law Division (Code 17) of the Office of the Judge Advocate General provides litigation support to Navy-Marine Corps personnel in national security case litigation. Code 17 coordinates classification reviews in litigation involving classified information and thereafter obtains Secretary of the Navy privilege assertions under Military Rule of Evidence 505. Code 17 serves as the Judge Advocate General's and the Navy Legal Service Command's central point of contact for the Department of Justice and components of the Intelligence Community on litigation involving classified information. The Division provides training to staff judge advocates; trial and defense counsel; military judges; Article 32, UCMJ investigating officers; and investigation/court security officers on all matters pertaining to the processing of national security cases.

This Guide is written with the expectation that it will be of immediate and continuing value to those charged with protecting national security information and those who investigate, prosecute, and defend servicemembers accused of espionage and related offenses. Code 17 stands ready to assist in all aspects of these cases. The contact information for Code 17 is as follows:

Division Director:	(202) 685-5464 / DSN 325-5464
Deputy Division Director:	(202) 685-5465 / DSN 325-5465
OJAG Security/SCI Liaison:	(202) 685-5470 / DSN 325-5470
Code 17 Fax (secure):	(202) 685-5467/ DSN 325-5467

ACKNOWLEDGEMENTS

This Litigation Guide was originally conceived and started under the direction of Captain Peter J. McLaughlin, JAGC, U.S. Navy. Captain McLaughlin was the first Director of the National Security Litigation and Intelligence Law Division (OJAG Code 17) until his retirement in February 2002. His experience as a military judge at both the trial and appellate levels, and his participation as an integral member of the National Security Case Commission provided invaluable insight into litigation issues and procedures involving classified information. His Military Judge Overview, appended to this Guide as TAB A, serves as an outstanding stand-alone summary of the principle points in this Guide.

Lieutenant Commander John D. Bauer, who currently serves as Code 17's Deputy Division Director, personally drafted several sections of this Guide, and he reviewed and edited the remainder. Without his outstanding work, this Guide would still be incomplete.

Captain Robert J. Eatinger, JAGC, U.S. Naval Reserve, Commander Christopher C. Gentile, JAGC, U.S. Naval Reserve, Lieutenant Commander Patrick E. Kelly, JAGC, U.S. Naval Reserve, and Lieutenant Commander Sherry E. Sabol, JAGC, U.S. Naval Reserve, members of NAVCIVLAWSUPPACT 106 assigned to drill with Code 17, all contributed considerable time and effort in the development of this Guide. Captain Eatinger and Lieutenant Commander Kelly served on active duty in the Special Programs Office of the Office of the Judge Advocate General (the old OJAG Code 11), though a decade apart. The format and much of the content of this Guide is due to their collective knowledge, skill, and experience in handling litigation issues involving classified material. Their contributions made this Guide possible.

This Guide benefited from information contained in "Prosecuting National Security Cases: A Handbook For Trial Counsel," a similar work the old Code 11 produced under the direction of Commander Homer S. Pointer, JAGC, U.S. Navy (Ret). An earlier edition of that Handbook was conceived and drafted by Major Frank Short, U.S. Marine Corps (Ret). This Guide borrowed liberally from that earlier work.

Drafters of this Guide also benefited from sections of a draft trial guide for cases involving classified information that Captain Melissa L. Barsotti, U.S. Air Force, prepared and generously shared.

Finally, my thanks and appreciation also to Lieutenant Commander Karen S. Somers, JAGC, U.S. Navy, who provided invaluable short-fused assistance in formatting and printing an initial draft of this Guide for dissemination to course participants at the Litigating National Security Cases course held in late May 2002 at Norfolk, VA.

/s/
P. M. DELANEY
Captain, JAGC, U.S. Navy
Deputy Assistant Judge Advocate General
(National Security Litigation and Intelligence Law)

Introduction

The National Security Case Guide is intended for the use of Naval personnel involved in the prosecution, defense, or adjudication of a National Security Case or case involving classified information. The Guide contains information and guidance on the preparation, prosecution, defense, and adjudication of such cases. Information herein will be of use to Convening Authorities and their staff judge advocates, to trial and defense counsel, to Article 32, UCMJ, Investigating Officers and Military Judges, and to personnel detailed as Investigation Security Officers and/or Court Security Officers. The Guide will be updated often, based upon suggestions and comments from practitioners, court opinions, and changes in rules, regulations, or statutes. The Guide will be an on-line resource.

The Guide discusses legal and security issues inherent to National Security Cases. Such issues include classified information, compartmented information, security requirements, the definition of national security cases, coordination with the intelligence community, the difference between criminal and counterintelligence investigations, Rule for Court-Martial 405, and Military Rule of Evidence 505. Appended to the Guide are checklists and sample documents to help illustrate points and issues. Additionally, appended as TAB A to this Guide is an overview and discussion of legal principles tailored for use by military judges. TAB B provides a recommended reading list that includes law review articles and cases. In the end, however, the information in this Guide should be used only as a foundation upon which to build more specific knowledge based upon the facts and needs of each individual case. The Guide is not intended to be a substitute for professional judgment, ingenuity, and zealous representation. Legal discussions and sample documents should not stifle the creativity of counsel. Additionally, the Guide is not intended to usurp military judges' authority to interpret and apply the law.

National Security Cases and cases involving classified information are inherently complex because they impose strict security, reporting, coordination, and approval requirements on top of the necessities of investigating, trying, defending, or adjudicating charges. Some offenses are capital and often are "high visibility" cases overseen by the media, senior government officials, and Congress. All parties to a National Security Case must approach their responsibilities deliberately and pay assiduous attention to detail. These cases take time to investigate and prepare for trial. The regulations for the handling, storage, and communication of classified information must be followed with care.

CHAPTER 1

Classified Information

A. Introduction. In many national security cases, the investigating officer, counsel, and the military judge will be confronted with documents or other material containing classified information. In such cases, all parties must understand what classified information is, as well as their duties and obligations with respect to creating, handling, storing, communicating, disseminating, and transmitting classified information. While the propriety of classification markings is not an element of many federal offenses, it is relevant to decisions to close Art 32 investigations and courts-martial to the public. Appendix 1-A is a comprehensive list of references relating to classified information.

B. What is classified information? While the definitions of "classified information" vary slightly, they all boil down to information that an authorized official of the Executive branch has determined pertains to a limited number of subject matters, is within the custody or control of the United States Government, and, in that official's professional judgment, reasonably can be expected to cause damage to the national security or foreign relations of the United States if disclosed to unauthorized recipients. SECNAVINST 5510.36, Appendix A, defines classified information as "[i]nformation that has been determined to require protection against unauthorized disclosure in the interests of national security and is classified for such purposes by appropriate classification authority per the provisions of E.O. 12958 or any predecessor Order." The official definition is found in E.O. 12958.

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." Id., at § 1.1(c). The Order 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 § 1.1(b). Classified information is defined in E.O. 12968 as "information that has been determined pursuant to Executive Order No. 12958, or any successor order, Executive Order No. 12951, or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011), to require protection against unauthorized disclosure." Id., at § 1.1(d).

Many statutes include "Restricted Data" (RD) within their definitions of classified information as a shorthand reference to information protected for interests of national security. However, RD 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. RD 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 RD as classified information include:

The National Security Act of 1947 ("any information that has been determined pursuant to Executive Order No. 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 Rules of Evidence 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)." Mil. R. Evid. 505(b)(1). Therefore, RD is protected during courts-martial using Mil. R. Evid. 505 procedures in the same way as information classified under E.O. 12958. Trial counsel prosecuting a case involving RD will need a court security officer who understands and has experience with the requirements for safeguarding RD.

C. Substance of Classified Information. For information to be classified under E.O. 12958, 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;

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

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

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, §§ 1.2 and 1.5. An OCA is an official

authorized in writing by the President, or by those authorized officials, to classify information in the first instance.

Once an OCA classifies the 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 is NOT a classification level. The OCA assigns a classification level based on the OCA's subjective evaluation of the severity of the damage to the national security the OCA reasonably expects to occur from the unauthorized disclosure of the information. If the OCA reasonably expects the unauthorized disclosure of the information would cause "exceptionally grave" damage to the national security, the information may be classified up to TOP SECRET. If the OCA reasonably expects the unauthorized disclosure of the information would cause "serious" damage to the national security, the information may be classified no higher than SECRET. If the OCA reasonably expects the unauthorized disclosure of the information would cause damage to the national security, the information is classified no higher than CONFIDENTIAL. *See*, E.O. 12958, § 1.3(a).

D. Classification Markings. 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 the document does not render the *information* unclassified. Rather it causes the *document* containing the classified information to be improperly classified. The reason to mark documents is obvious. Proper markings provide notice that the document contains classified information and must be protected accordingly. The marking of a document as classified, even if improperly so, creates the obligation to protect it in accordance with the relevant regulations. A person who believes a document is improperly marked is obliged to treat it as classified until obtaining a determination otherwise. Ultimately, a person in authorized possession of classified information can submit a "challenge to classification" under E.O. 12958 § 1.9(a). Procedures for making classification challenges within DON are found in SECNAVINST 5510.36 at 4-12. Those procedures require the information to "be safeguarded as required by its stated classification level until a final decision is reached on the challenge." Id., at 4-12.3.

1. Overall marking. The document must be marked at the top and bottom of each page in one of two ways. First, each page is marked at the top and bottom to indicate the highest level of classified information on that page, except the cover and back page of the document must be marked at the top and bottom with the highest level of classified information found anywhere in the document. Second, and more commonly, each page is marked at the top and bottom with the highest level of classified information in the document irrespective of the highest level on the particular page. Intelligence documents will often have additional markings.

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. That means, the marking identifies only the classified level of that paragraph standing by itself and unrelated to information elsewhere in the document. "(U)" means the paragraph contains no classified information. "(FOUO)" means the paragraph contains no classified information, but contains information that

is not publicly releasable for some other reason. "(C)" means the paragraph contains information classified up to CONFIDENTIAL. "(S)" means the paragraph contains information classified up to SECRET. "(TS)" means the paragraph contains information classified up to TOP SECRET.

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. SECNAVINST 5510.36, at 6-11.1. Markings on information such as SENSITIVE, FOR OFFICIAL USE ONLY, NOFORN, ORCON, SPECAT, or a codeword are not classification levels. They are markings that limit the dissemination or handling of information for reasons other than the classification level. Such markings are further defined in Chapter 6 of SECNAVINST 5510.36 and include:

NOFORN - NOT RELEASABLE TO FOREIGN NATIONALS

ORCON - DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR

REL TO - AUTHORIZED FOR RELEASE TO

SPECAT - SPECIAL CATEGORY

PROPIN - CAUTION PROPRIETARY INFORMATION INVOLVED

SAMI - SOURCES AND METHODS INFORMATION

You may see on older document certain dissemination controls or handling caveats that are no longer used. Such markings include:

NOCONTRACT - NOT FOR RELEASE TO CONTRACTORS/CONSULTANTS

WNINTEL - WARNING NOTICE - INTELLIGENCE SOURCES AND METHODS INVOLVED.

E. Classification Authority. A classification authority is an official empowered to determine whether information is classified and so mark it. There are two types of classification authorities: original and derivative.

1. Original Classification Authority (OCA). An OCA is "an individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance." E.O. 12958, § 1.1(g). The only OCAs are the 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, § 1.4(a). Such delegations must be in writing, to a position vice a person, and kept to a minimum. E.O. 12958, § 1.4(c). The President and agency heads or officials designated by the President can delegate

"original classification authority at any level, including "Top Secret." "Senior agency officials,"[1] if delegated ‘‘Top Secret’’ original classification authority, can delegate up to ‘‘Secret’’ or ‘‘Confidential’’ original classification authority. Original classification authority may not be further delegated. OCAs within DON are identified in SECNAVINST 5510.36, Exhibit 4A, updates to which can be found on the CNO (N09N2) homepage at www.navysecurity.navy.mil.

Non-OCAs who create information that they believe should be classified may 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, contractor, licensee, certificate holder, or grantee of an agency that 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 this [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 the person is not sure to which agency to send the information, it must be sent to the Director of the Information Security Oversight Office. E.O. 12958, § 1.4(e). See, SECNAVINST 5510.36 at 4-14.

2. Derivative classification authority. "'Derivative classification' means the incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification." E.O. 12958, § 2.1(a).

a. ‘‘Classification guidance’’ means any instruction or source that prescribes the classification of specific information.

b. ‘‘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.

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

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

A derivative classifier is required to observe and respect the original classification determinations made by OCAs. E.O. 12958, at § 2.2(b)(1); and SECNAVINST 5510.26, at 4-

[1] ‘‘Senior agency official’’ means the official designated by the agency head under E.O. 12958, § 5.6(c) to direct and administer the agency’s program under which information is classified, safeguarded, and declassified. The senior agency official for the Department of the Navy is the Director, Naval Criminal Investigative Service (DIRNCIS), who is double-hatted as CNO (N09N). CNO (N09N2) provides staff support to the DIRNCIS for this purpose. SECNAVINST 5510.36, at 1-5.2.

9.2. Normally, this is done by reference to a source document or classification guide. However, the absence of a classification guide does not negate an OCA's determination to classify information. Guides are merely the recording of original classification decisions. SECNAVINST 5510.36, at 5-1.1. Their purpose is to "facilitate the proper and uniform derivative classification of information." E.O. 12958, at § 2.3(a).

APPENDIX 1-A

Classified Information References

1. Executive Order No. 12958, "Classified National Security Information," Apr. 17, 1995, 60 Fed. Reg. 19825, as amended by Executive Order No. 12972, Sept. 18, 1995, 60 Fed. Reg. 48863,[2] 3 C.F.R. 333 (1996), further amended by Executive Order No. 13142, Nov. 19, 1999, 64 Fed. Reg. 66089, 3 C.F.R. 236 (2000),[3] reprinted at 50 U.S.C. § 435 note.

2. Executive Order No. 12968, "Access to Classified Information," Aug. 2, 1995, 60 Fed. Reg., 40425, 3 CFR 391 (1995), reprinted at 50 U.S.C. § note.

3. Executive Order No. 12951, "Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems," Feb. 22, 1995, 60 Fed. Reg. 10789, reprinted at 50 U.S.C. § 435 note.

4. Order of President of the United States, 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," Oct. 13, 95, 60 Fed. Reg. 53491, reprinted at 32 C.F.R. 2001.

6. Information Security Oversight Office Directive No. 1 Appendix A, "Document Referral," Sep. 13, 99, 64 Fed. Reg. 49388, reprinted at 32 C.F.R. 2001.55.

7. Information Security Oversight Office Directive, "Safeguarding Classified National Security Information," Sep. 24, 99, 64 Fed. Reg. 51853, reprinted at 32 C.F.R. 2004.

8. DOD Directive 5200.1, DOD Information Security Program, 13 Dec 96, reprinted at 32 C.F.R. 159.

9. DOD 5200.1-R, DOD Information Security Program Regulation, 14 Jan 97, reprinted at 32 C.F.R. 159a.

10. DOD 5200.2, DOD Personnel Security Program, 9 Apr 99, reprinted at 32 C.F.R. 156.

11. DOD 5200.2-R, DOD Personnel Security Program Regulation, through change 3, 23 Feb 96, reprinted at 32 C.F.R. 154.

12. SECNAVINST 5510.36, Department of the Navy (DON) Information Security Program Regulation (ISP), through Change 2, 23 Jan 01.

---

[2] E.O. 12972 amended the definition of "agency" in E.O. 12958.

[3] E.O. 13142 extended the dates for the automatic declassification of certain classified information in documents more than 25 years old that have been determined to have historic value, and transferred the Information Security Oversight Office from the General Services Administration to the National Archives and Records Administration.

13. SECNAVINST 5510.30A, Department of the Navy Personnel Security Program, 10 Mar 99.
14. Director of Central Intelligence Directive (DCID) 1/19, "Security Policy for Sensitive compartmented Information," 1 Mar 95

15. DCID 1/19P, Supplement to Director of Central Intelligence Directive (DCID) 1/19, "DCI Security Policy Manual for SCI Control Systems," 1 Mar 95

16. Director of Central Intelligence Directive (DCID) 1/21, "Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF)," 29 Jul 94

17. Director of Central Intelligence Directive (DCID) 6/4, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI), 2 Jul 98

18. Department of Defense Manual 5105.21-M-1, DOD Sensitive Compartmented Information Administrative 19. Security Manual, 3 Aug 98 (NOTAL)

CHAPTER 2

Compartmented Information

A. Introduction. Persons often confuse compartmented information with classified 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." 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, limiting access to individuals with a specific need-to-know. . Compartmented information is often colloquially referred to as "codeword information." This chapter will discuss the two principal categories of compartmented information; Special Access Programs and Sensitive Compartmented Information.

B. Special Access Programs. E.O. 12958, at § 4.1(h) defines "Special Access Programs" or "SAP*s*" 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 § 4.4(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 programs at an absolute minimum, and shall establish them only upon a specific finding that:

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

2. 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; or

3. The program is required by statute.

SECNAVINST 5510.36, at page A-14, defines a SAP as "[a]ny DOD program or activity (as authorized in E.O. 12958) employing enhanced security measures (e.g., safeguarding or personnel adjudication requirement) exceeding those normally required for classified information at the same classification level which is established, approved, and managed as a DOD SAP." 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. SECNAVINST 5510.36, at 1-1.4(c). Further guidance concerning SAPs can be found in DODDIR 0-5205.7, Special Access Program (SAP) policy, 13 Jan 97; DODINST 0-5205.11, Management, Administration, and Oversight of DOD Special Access Programs (SAP*s),* 1 Jul 97; SECNAVINST S5460.3C Management, Administration, Support, and Oversight of SAPs within the Department of the Navy, 5 August 1999; Navy Department Supplement to DoD 5105.21.M-1; and DoD 5220.22-

M-Sup.1 DOD Overprint to the National Industrial Security Program Operation Manual Supplement February 1995.

SAP information is typically identified with a classified codeword or codewords. A person must obtain 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 the particular SAP information. SAP information usually must be stored in areas that have security measures exceeding those required for TOP SECRET. Most non-intelligence SAPs in DOD pertain to weapons systems.

C. Sensitive Compartmented Information (SCI). The Director of Central Intelligence (DCI), is responsible for all Controlled Access Programs within the National Foreign Intelligence Program. 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-Keyhold (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. DCID 3/2, Controlled Access Program Oversight Committee.

The personnel, information, physical security and information systems security procedures required for SCI are set forth in (DCIDs. The Director, Defense Intelligence Agency (DIA), is responsible for administering security policies and procedures issued by the DCI 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 (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. DOD Directive 8520.1, at 5.3.1 and 5.5.1, respectively and SECNAVINST 5510.36, at 1-4.5 and 1-5.6, respectively. 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.

> "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.

D. Controls. 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. SCI Control System/Codeword;

4. Foreign Government Information;

5. Dissemination Controls;

6. Non-Intelligence Community Markings; and

7. Declassification Date.

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//X1

TOP SECRET//TALENT KEYHOLD//RISK SENSITIVE//X1

TOP SECRET//TK//RSEN//X1

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

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 which 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. Examples of portion markings are:

(S//NF//PR)

(TS//TK//RSEN)

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. Since SCI is the most common compartmented information implicated in national security litigation, we will discuss in general the rules that apply to SCI. Compartmented information falling within other special access programs will have their own specific security requirements and 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 SAP or programs at issue.

For example, SCI may be discussed and stored only in Sensitive Compartmented Information Facilities (SCIFs). The structural and security requirements for SCIFs are set forth in DCID 1/21, Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF). The Nondisclosure Agreement (NdA) for access to SCI is different that the NdA 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 before information within that subcompartment may be disclosed to him or her.

CHAPTER 3

Classification Review

A. Introduction. A Classification Review (CR) is a "term of art" with a specific meaning and is the single most critical first litigation support function. A CR, if done properly, results in an official and reliable determination of the current classification of the information at issue, both substantively and procedurally (marking). Without a properly done CR, you can have no assurance the information is currently classified or that the document is properly marked. A CR must be completed before any material can be considered "evidence" in any proceeding.

B. Requests For Classification Review. The Convening Authority and Government counsel must ensure that NCIS requests, in writing to the Chief of Naval Operations (CNO), that a CR be completed. CNO (N09N2) is the office officially tasked with initiating a CR. Code 17 can assist in obtaining the CR. For more information on N09N2, refer to its website at www.navysecurity.navy.mil.

All potentially relevant documents must be sent to the experts with cognizance over that material. The CR and analysis of evidence must precede action under the UCMJ (i.e., before an Art. 32 or Mil. R. Evid. 505 hearing) and the CR should be completed before copies of classified or potentially classified documents are provided to the accused or defense counsel. It is important that a CR be completed to avoid providing the court of defense counsel with multiple versions of a document with conflicting classification markings. Staff Judge Advocates and Government counsel should stay on top of the process to ensure a CR is completed correctly and timely. Code 17 and N09N2 will do the same. Code 17 will also assist in preparing documents for the Secretary of the Navy to assert the Mil. R. Evid. 505 claim of privilege.

C. Substance Of Classification Reviews. N09N2 identifies the Original Classification Authority (OCA) and forwards the documents to that OCA to conduct the CR. Occasionally, there are multiple OCAs for a single document. The CR shall:

1. Verify the current classification level and its duration;

2. Verify the classification level of the information when subjected to compromise;

3. Determine whether some other DON command requires further review; and

4. Provide a general description of the impact on the affected operations.

A CR TAKES TIME! START AT ONCE! Do not start the discovery process until the CR is completed and completed correctly. The CR process could take several months and may require coordination among several agencies.

CHAPTER 4

Security Requirements

A. Introduction. There are three categories of security pertaining to classified information: (1) information security; (2) personnel security; and (3) information systems security, also known as ADP security.

1. Information security. The Navy's Information Security Program is published in SECNAVINST 5510.36. Information security pertains to the policies, rules, and procedures for classifying, safeguarding, transmitting, and destroying of classified information. The rules for classifying information have been set out above.

2. Personnel security. The Navy's Personnel Security Program is published in SECNAVINST 5510.30A. The personnel security rules for SCI are found in DCID 6/4. Personnel security pertains to the policies, rules, and procedures for determining whether and how a person should be processed for, granted, and retain a security clearance. A person may be granted and retain a security clearance only upon 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. Such a determination is made only upon the conclusion of a personnel security investigation. Different types of investigations are required depending upon the level of classified information for which a security clearance is sought. The single authority for granting security clearances for the Navy is the Department of the Navy Central Adjudication Facility (DON CAF). That is, DON CAF grants all CONFIDENTIAL, SECRET, and TOP SECRET security clearances for the Navy. It does not grant access to specific classified information, nor does it grant access to compartmented information. Access to specific classified information requires not only that a person have been granted the requisite security clearance, but also that he or she have executed a nondisclosure agreement and have a "need to know" the information in the performance of his or her official duties. The basic policy is to limit access to classified information to the minimum number of people necessary for the Navy to do its job. SECNAVINST 5510.30A, at 9-2.4, states that limiting access "is the responsibility of each individual possessing classified information. Before allowing access to classified information, individuals possessing classified information must determine that allowing access is justified based on the others' security clearance eligibility and need to know."

The determination whether or not a 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 is not subject to judicial review. Department of Navy v. Egan, 484 U.S. 518 (1988). Courts are authorized, however, to ensure agencies follow their own regulations with respect to an individual's ability to appeal an adverse security clearance determination. In addition, under security procedures established [pursuant to section 9 of the Classified Information Procedures Act of 1980, as amended, 18 U.S.C. App. III] by the Chief Justice of the United States for the Protection of Classified Information, the trial judge may review the government's determination that a defense counsel is not sufficiently trustworthy to be granted access to classified information. The Procedures, at paragraph 5, specifically states that:

> Persons Acting for the Defendant. The government may obtain information by any lawful means concerning the trustworthiness of persons associated with the defense and may bring such information to the attention of the court for the court's consideration in framing an appropriate protective order pursuant to Section 3 of the Act.

In practice, however, U.S. District Judges have relied upon the Department of Justice Court Security Officer to process defense counsel for security clearances. The judges themselves get involved only when defense counsel refuse to cooperate in the security clearance process (See, United States v. Usama bin Laden, 58 F.Supp.2d 113 (S.D.N.Y. 1999), or are found ineligible for a security clearance. The purpose of this review is to ensure the United States does not use eligibility for access to classified information as a ruse to deny a defendant his constitutional right to effective assistance of counsel.

3. Information systems security. The Navy's Information Systems Security Program is published in SECNAVINST 5239.B. Information Systems Security pertains to the policies, rules, and procedures for processing, transmitting, safeguarding, and storage of classified information on Navy information systems.

B. Protective Order. A Protective Order is issued in the event classified information is going to be disclosed to the defense. The purpose of the Protective Order is to guard against the compromise of the classified material to be disclosed. 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 (ISO) and alternates for an Article 32 investigation or a Court Security Officer (CSO) and alternates for a court-martial proceeding. A sample Protective Order and MOU are in APPENDIX 4-A.

C. When is the Protective Order issued? As permitted under Mil. R. Evid. 505, a Protective Order should be issued in any circumstance in which classified material is going to be disclosed to the defense. It can be issued before the Article 32 investigation, and then re-issued before a follow-on court-martial proceeding. If issued before an Article 32 investigation, the Article 32 Convening Authority will issue the Protective Order. Among other things, this Protective Order will require the accused to enter into a Memorandum of Understanding (MOU) with the Article 32 Convening Authority that protects the classified information to be disclosed. Without this MOU, there will be no disclosure of classified information. Once charges are referred, Government counsel will request a Protective Order, including an MOU, from the military judge. 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 Mil. R. Evid. 505 has been invoked. *See*, R.C.M. 405(g)(6).

D. Role of the Investigation/Court Security Officer (ISO/CSO). As stated above, the Protective Order will appoint an Investigation Security Officer or Court Security Officer who will be charged with safeguarding classified material during the proceeding. The Protective Order will also appoint Alternate ISOs/CSOs. The ISO/CSO is tasked with serving as a neutral party responsible for ensuring that classified material is properly safeguarded during the judicial proceeding. The ISO/CSO serves as the security advisor to the Article 32 Investigating Officer or to the military judge at a court-martial. The ISO/CSO is not a subject matter expert with regard to the content of the classified material or programs at issue. Rather, he or she is an expert in protecting classified or classifiable information. In the event that a military judge at court-martial has ruled that the taking of evidence on certain classified matters will be closed to the public, it is likely that a subject matter expert will be needed in the courtroom to signal the judge when testimony or other evidence is tending toward divulging these classified matters. In this instance, the CSO would not have the knowledge to make this determination.

It is paramount to remember that the ISO/CSO is not a member of the prosecution or defense team. Rather, he or she is an Officer of the Court, and as such provides security guidance and assistance to the military judge, and to the prosecution and defense teams. The ISO/CSO is there to prevent the military judge, the prosecutors and the defense team from committing security violations. He or she advises the court from a security perspective, not from a legal perspective.

The ISO/CSO is typically an experienced military member 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 the background that would qualify theme to serve as ISOs/CSOs. 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) at the level of Top Secret/Sensitive Compartmented Information (TS/SCI), then that ISO/CSO must be "read in" and cleared to handle that particular SAP's information. It is incumbent upon the staff judge advocate to ensure that an ISO/CSO is assigned to the case at the outset. This is done by naming the ISO in the Article 32 appointing order.

E. Document Security. Once appointed, the CSO/ISO becomes primarily responsible for document security throughout the proceeding. He or she coordinates the transfer of any classified discovery material from the Government counsel to the defense counsel. In addition, the ISO/CSO is tasked with spotting any security issues with regard to TS/SCI material. In this instance, he or she will serve as a liaison to other intelligence agencies, Original Classification Authorities and their subject matter experts. A particular piece of information may involve the equities of more than one intelligence agency. In addition, the procedures for handling some SCI material may not be universal: different intelligence agencies may have differing document security protocols. The ISO/CSO is tasked with coordinating and resolving these issues.

The ISO/CSO will also maintain an inventory of all classified material used or related to the proceedings. At the conclusion of the case, the ISO/CSO will ensure the classified discovery material is returned to the respective agency. The transcript and the entire record of trial must be handled as classified at the highest level contained therein until the appropriate authorities have

completed a security review. If the transcript and record of trial is determined to contain classified information, then it must be secured in an appropriate space.

F. 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 Special Security Office can frequently provide the ISO/CSO with accredited 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 SCI information) 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/SCI level are being produced, then the appropriate intelligence agency and/or program office must approve use of the computer. At the conclusion of the proceeding, the ISO/CSO must remove the classified information from the laptop computer or the removable hard drive and transfer it to a floppy disk. The disk will then be inventoried and stored with the original transcript or record of trial.

G. Physical Security. The ISO/CSO is also tasked with overseeing that requirements for physical security are met. The ISO/CSO must ensure that the courtroom is secure in the event the military judge conducts *in camera* examinations of classified documents, or 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.

If the evidence in the proceeding involves material classified at the Top Secret/SCI 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 (number). Top Secret/SCI material can only be stored inside a SCIF that has been accredited by a Special Security Office. It is important to remember different intelligence agencies may have differing physical security protocols. Therefore, TS/SCI material may be of such a nature that a particular intelligence agency or program office may have additional approval/accreditation requirements. The ISO/CSO is 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 TS/SCI material 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 TS/SCI level.

H. Security Clearances. All personnel who will handle classified material during a national security case will be required to hold a proper security clearance. This typically includes the military judge, all defense counsel, all trial counsel, court reporters and bailiffs, and the investigation/court security officers. The current policy of the Commander, Naval Legal Service

Command, is to require three military judges, two government counsel, and two defense (one each coast) to maintain security clearances who are ready to assume national security cases. If classified material is to be used for prosecution, appropriate personnel security clearances in accordance with SECNAVINST 5510.36 must be granted to all members of the court, members of the prosecution and defense, court reporters, and interpreters, and all other persons whose presence is required when classified material is introduced before the court. If civilian defense counsel represents the accused, such counsel must likewise be cleared before classified material may be disclosed to him or her.

The early detailing of defense counsel with the appropriate clearances will help avoid delays that might be encountered if the accused forms an attorney-client relationship with a defense counsel who does not have the appropriate clearance. 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. If the case involves Top Secret/SCI information, then the ISO/CSO must contact the particular intelligence agency or program manager in order to determine the requirements for access to program information. Code 17 can assist in this process.

Counsel must determine as soon as possible the security clearances that will be required for personnel involved in the Article 32 investigation and/or court-martial. If the case involves information in a Special Access Program, counsel must contact the Program Manager to determine the requirements for access to program information. Code 17 can assist in identifying and coordinating that contact. Personnel who will be processed for security clearances normally include:

1. Military Judge. The Navy and Marine Corps have military judges who hold SCI clearance. Contact Code 17 if the case may require the military judge to have SCI access.

2. Defense counsel and defense paralegal. Clearance of civilian counsel, paralegals, or expert witnesses/assistants will require time and coordination. The failure by defense counsel to cooperate in obtaining a clearance is not a showstopper. In United States v. Jolliff, a case tried under CIPA in which 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 failure of counsel to cooperate in obtaining a security clearance for himself could lead to disqualification and dismissal from the case by the trial judge. S*ee 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).

3. Trial counsel and trial paralegal.

4. Court Security Officer and alternates.

5. Court reporter and alternates.

6. Bailiff and alternates.

7. Physical security personnel, if needed.

8. Equity holder observers.

APPENDIX 4-A

SAMPLE PROTECTIVE ORDER

)
)
) PROTECTIVE ORDER
)

---

1. In order to protect the national security and pursuant to the authority granted under Rule 505, Military Rules of Evidence (Mil. R. Evid. 505), relevant executive orders of the President of the United States; and regulations of the Department of the Navy; it is hereby ORDERED:

a. That the procedures set forth in this Security Procedures and Mil. R. Evid. 505 and the security procedures referred to above will apply to all matters concerning the Article 32, UCMJ, pre-trial investigation in this case.

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

(1) any classified document (or information contained therein);

(2) information known by the defendant or defense counsel to be classifiable;

(3) classified documents (or information contained therein) disclosed to the defendant 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 a clear indication that they have been officially declassified by the Government agency or department that originated the document or the information contained therein (hereinafter referred to as the "originating agency").

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, telex, 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. These Security Procedures are to insure that persons subject to these Procedures will never divulge the classified information disclosed to them to anyone who is not authorized by the originating agency and in conformity with these procedures.

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

h. Persons subject to these Procedures are admonished that any breach of these Procedures may result in the termination of their access to classified information. In addition, they are admonished that any unauthorized disclosure, possession or handling 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, United States Code, and Sections 421 and 783(b), Title 50, United States Code. In addition, for those persons who are attorneys, a report will be filed with their State Bar Association.

2. Appointment of Investigation Security Officer _____ is appointed the Investigation Security Officer.

3. Personnel Security Investigations and Clearances. This case will 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 special security clearance.

a. The Convening Authority has been advised that the Investigating Officer has the requisite security clearance to have access to the classified information and documents which will be at issue in this case. The Investigating Officer is to have unfettered access to that classified information necessary to prepare for this investigation, subject to requirement in paragraph 3.f, below.

b. The convening authority has been advised that the Government Counsel working on this case _____, has the requisite security clearance to have access to the classified information and documents which will be at issue in this case. The Government Counsel is to have unfettered access to classified information necessary to prepare for this investigation, subject to the requirements in paragraph 3.f, below.

c. As a condition of receiving classified information, any retained defense counsel will agree to the conditions specified herein and execute all necessary forms so that the Government may complete the necessary personnel security background investigation to make a determination whether defense counsel is eligible for a limited access authorization. Any retained defense counsel will also sign the statement in paragraph 3.d. Upon the execution and filing of the statements set forth in paragraphs 3.d and 3.e by any retained defense counsel requiring access to classified information, the Government shall undertake, as expeditiously as possible, the required inquiries to ascertain defense counsel's eligibility for access to classified information.

d. There are two conditions precedent to obtaining access to the classified information at issue in this case.

(1) All individuals, other than the Investigating Officer, Government and detailed defense counsels and personnel of the originating agency, can obtain access only after having provided the necessary information required for, and having been granted, a security clearance or Limited Access Authorization by the Department of the Navy, through the Investigation Security Officer; and

(2) Each person, other than the Department of Navy employees named herein and personnel of the originating agency, before being granted access to classified information must also sign a sworn statement that states:

MEMORANDUM OF UNDERSTANDING

1. I, _____, understand that I may be the recipient of information and intelligence that concerns the 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 established 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 provided for the violation thereof.

2. I agree that I will never divulge, publish or reveal, either by word, conduct, or any other means, such information or intelligence unless specifically authorized in writing to do so by an authorized representative of the U.S. Government or as otherwise ordered by the Court. I further agree to submit for prepublication review any article, speech, or other publication derived from or base upon experience or information gained in the course of United States v. _____. I understand this review is solely to ensure that no classified national security information is contained therein.

3. I understand that this agreement will remain binding upon me after the conclusion of the proceedings in the case of United States v._____.

4. I have received, read and understand the Security Procedures entered by the Convening Authority on _____, 200__, in the case of United States v. _____, relating to classified information, and I agree to comply with the provisions thereof.

_____
Signature/Date

WITNESS SWORN
AND SUBSCRIBED

Any MOU with a retained defense counsel shall include a statement expressing his understanding that the failure to abide by the terms of these Security Procedures will result in a report to his State Bar Association. Each such person executing the above statement must file an original with the Investigating Officer and provide an original each to the Investigation Security Officer and the Government Counsel.

e. In addition to signing the MOU in paragraph 3d, any person who, as a result of this investigation, gains access to information contained in any Department of the Navy Special Access Program, as that term is defined in section 4.2 of Executive Order 12356, to Sensitive Compartmented Information (SCI), or to any information subject to Special Category (SPECAT) handling procedures, shall sign any non-disclosure agreement which is specific to that Special Access Program, Sensitive Compartmented Information, or SPECAT information.

f. All other requests for clearances for access to classified information in this case by persons not named in these Procedures, or requests for clearances for access to information at a higher level of classification, shall be made to the Investigation Security Officer, who, upon approval of the Convening Authority, shall promptly process the requests.

g. Before any person subject to these Security Procedures, other than Government Counsel, Detailed Defense Counsel, and personnel of the originating Agency 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 3.d.

h. The Procedures shall apply to any defense counsel of 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.

4. Handling and Protection of Classified Information.

a. All counsel shall seek guidance from the Investigation Security Officer with regard to appropriate storage and use of classified information.

b. The Investigation Security Officer will provide appropriate physical security protection for any materials prepared or compiled by the defense, or by any person in relation to the preparation of the accused's defense or submission under Mil. R. Evid. 505. The materials and documents (defined above) requiring physical security include, without limitation, any notes, carbon papers, letters, photographs, drafts, discarded drafts, memoranda, typewriter ribbons, magnetic recording, or other documents or any kind or description. Classified materials prepared by the defense shall be maintained by the investigation Security Officer in a separate sealed container to which only the defense counsel shall have access.

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

d. No one shall discuss any 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

e. Written materials prepared for this case by the accused or defense counsel shall be transcribed, recorded, typed, duplicated, copied or otherwise prepared only by persons who are cleared for access to such information.

f. 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 Investigation Security Officer and in accordance with instructions he or she shall issue.

g. Upon reasonable advance notice of the Investigation 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 documents by these Procedures 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 these Procedures. Such notes will be secured in accordance with the terms of these Procedures. Persons permitted to have access to classified documents will be allowed to view their notes within an area designated by the Investigation Security Officer. No person permitted to inspect classified documents by these Procedures, 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 Investigation Security Officer, after he or she has consulted with the Convening Authority.

h. Without prior authorization of the Department of the Navy, there shall be no disclosure to anyone not named in these Procedures by persons who may later receive a security clearance or limited access authorization 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 declassified.

i. The defense shall not disclose the contents of any classified documents or information to any person except those persons identified to them by the Investigating Officer as having the appropriate clearances, and a need to know.

j. All persons given access to classified information pursuant to these Procedures are advised that all information to which they obtain access by these Procedures 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 Investigation Security Officer.

k. A copy of these Procedures shall issue forthwith to defense counsel, with further order that the defense counsel advise the accused named herein of the contents of these Procedures, and furnish him a copy. The accused, through defense counsel, shall forthwith sign the statements set forth in paragraph 3.e of these Procedures, and counsel shall forthwith file an original with the Investigating Officer and provide an original each to the Investigation Security Officer and the Government Counsel. The signing and filing of this statement by the accused is a condition precedent to the disclosure of classified information to the accused.

5. Nothing contained in these Procedures shall be construed as waiver of any right of the accused.

DATE:_____, 200__, at _____

_____
CONVENING AUTHORITY

CHAPTER 5

Reporting Requirements

A. References.

1. JAGMAN § 0126

2. SECNAVINST 5510.36, Department of the Navy Information Security Program Regulation, through Change 2, 23 Jan 01

3. SECNAVINST 5500.30F, Reporting of Counterintelligence and Criminal Violations to Office of the Secretary of Defense Officials

B. Introduction. Due to the sensitive and complex nature of National Security Cases, DOD and DON regulations have established various reporting requirements. Responsibility for these reports falls in varying degrees upon the local command (CO/security manager), the local law enforcement community (Naval Criminal Investigative Service (NCIS)), and the local legal community (Staff Judge Advocate (SJA)/Trial Counsel (TC)). Although the SJA/TC is not personally responsible for all of the reports, he or she needs 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.

C. Command-Immediate Reports. Upon discovery of a possible loss or compromise of classified information, chapter 12 of SECNAVINST 5510.36 requires the cognizant commanding officer to (1) notify immediately the local NCIS office and (2) initiate a command preliminary inquiry (PI). As defined in paragraph 12-1 of SECNAVINST 5510.36, a loss occurs when the information cannot be physically located or accounted for, and a compromise occurs when the information is disclosed to an unauthorized person. A possible loss or compromise does not necessarily include every instance of mishandling of classified information. The commanding officer is ultimately responsible for these requirements, but it is typically the command security manager who carries them out.

The requirement to notify NCIS arises as soon as the command learns of a possible loss or compromise of classified information. Timely notice to NCIS helps to ensure that evidence is preserved for a possible counterintelligence or criminal investigation. If the NCIS office intends to open an investigation, it is required to promptly notify the command.

Of equal importance is the requirement for the command to initiate a PI. The PI must be completed within 72 hours, and should contain a conclusion as to the likelihood of an actual loss or compromise. The command is required to conduct a PI regardless of whether NCIS has initiated its own investigation. In certain cases, however, the NCIS Special Agent in Charge (SAC) may request the commanding officer to delay the PI in order to preserve evidence for the NCIS investigation. This is another reason why it is important to notify NCIS and bring them into the case at the earliest opportunity.

Unless the PI concludes that the loss or compromise did not occur, or that the possibility of compromise is remote, the PI must be sent to the offices listed in paragraph 12-4 of SECNAVINST 5510.36. As an additional requirement, if the possible loss or compromise involves special types of classified information, such as SCI or SAP, paragraph 12-8 requires that the PI also be sent to the offices listed for that specific type of information. See APPENDIX 5-A for a list of the offices that receive the PI.

D. Command -72 Hour Report. Within 72 hours of discovery of the violation, the PI must be completed and distributed. Paragraph 12-4 of SECNAVINST 5510.36 requires that the PI be sent to the following offices: CNO (N09N2); the immediate superior in command (ISIC); the originator of the information; the Original Classification Authority (OCA); and the local NCIS office. Paragraph 12-8 contains additional reporting requirements for incidents that involve special types of classified information, such as SCI or SAP. See APPENDIX 5-A for a summary of the offices that must receive the PI. The PI does not need to be sent if it concludes that a loss or compromise did not occur, or that the possibility of compromise is remote.

Special attention should be given to cases that involve TS/SCI information. First, it is important to ensure that the Special Security Officer (SSO) has been notified. Often, the command's designated SSO is from a different command and serves as SSO by agreement. Accordingly, the SSO would not necessarily become aware of the incident in the normal course of events, as would the command security manager. The involvement of the SSO is vital in cases that involve TS/SCI material to ensure proper handling of the information. Also, as listed in APPENDIX 5-A, whenever the incident involves TS/SCI material, or information relating to intelligence sources and methods, the Director of Naval Intelligence (DNI) must be notified of the PI.

E. NCIS Reports. If NCIS initiates an investigation, JAGMAN § 0126a, requires NCIS to notify the appropriate Department of Justice investigative agency in compliance with the Memorandum of Understanding between the Departments of Defense and Justice (See Appendix 3, MCM (DOD Dir 5525.7)). In addition, JAGMAN § 0126b requires NCIS to notify OJAG (Code 17) if its investigation indicates a suspect may have committed a national security offense. These notices are primarily intended to help facilitate procedural requirements for grants of immunity and pretrial agreements in national security cases.

When the NCIS investigation involves allegations of espionage, SECNAVINST 5500.30F, requires NCIS to notify the Under Secretary of the Navy and, as applicable, the VCNO or ACMC. 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.

F. Staff Judge Advocate/Trial Counsel Reports. Under JAGMAN § 0126f, the "responsible command, convening authority, or judge advocate" is required to make certain reports to the Judge Advocate General (Code 17) on cases involving classified information, whether or not designated a national security case. 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.

As soon as the command first becomes aware of the case, the judge advocate should notify OJAG (Code 17). This is in addition to the requirement to notify NCIS contained in JAGMAN § 0126a, and does not take precedence over or substitute for that obligation. Also, this is deliberately duplicative of the requirement contained in JAGMAN § 0126b for NCIS to notify OJAG, and one cannot be substituted for the other. Additionally, the judge advocate should notify OJAG whenever a major development occurs in the case, such as designation as a national security case, preferral of charges, or imposition of pretrial restraint. Finally, regardless of any major developments, the judge advocate should provide a report at least once every 60 days.

G. Report to National Security Case Disposition Authority. Only certain officers are authorized to initially dispose of national security cases. These officers are listed in JAGMAN § 0126c and are designated as national security case disposition authorities (NSCDA). Commanding officers who receive reports or allegation of potential national security cases must, in addition to complying with the other notification requirements, forward the case to a designated NSCDA. The NSCDA, using the criteria discussed in Chapter 7, then must determine whether the case is a national security case. Upon making this determination, the NSCDA must report this to OJAG (Code 17) as a major development. As with other reports to OJAG, the command will typically rely on the SJA or TC, if one is assigned, to ensure proper processing.

H. Miscellaneous Reports. OJAG (Code 17) is required to notify the Department of the Navy General Counsel (DON GC) if serious disciplinary action is being contemplated with respect to compromise of classified information. Additionally, OJAG (Code 17) is responsible to ensure that the Secretary of the Navy and the CNO or the Commandant of the Marine Corps, as appropriate, are kept advised of the status of such cases. In making these reports, OJAG (Code 17) necessarily relies on the reports described above to collect the appropriate information.

APPENDIX 5-A

REPORTING CHECK LIST

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 USCINCSTRAT 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.

CHAPTER 6

Coordinating with Outside Agencies

A. Coordinating With Investigative Agencies. Coordination between various investigative agencies having jurisdiction over national security matters is critical. In the course of any investigation, other investigative agencies may have either employed or may be planning to employ certain investigative techniques available for counterintelligence rather than for law enforcement purposes. Such investigative actions could significantly affect prosecutorial decisions. Likewise, prosecutorial decisions taken without proper coordination with other investigative agencies could undermine or call into question the use of counterintelligence investigative techniques by any of the involved agencies. Thus, it is imperative that upon learning of a national security case, Trial Counsel, through Code 17, contact and coordinate with any other investigative agency having jurisdiction over the matter.

Investigation of national security cases may lend itself to use of either counterintelligence or law enforcement investigative techniques or both. Traditionally, investigative agencies determine at the outset of an investigation whether they are seeking counterintelligence information for intelligence purposes or evidence for law enforcement purposes. Executive Order 12333 sets forth in broad terms the counterintelligence authorities of agencies belonging to the intelligence community. It is significant to note that, in accordance with section 1.4 of the Executive Order, counterintelligence activities within the United States must be coordinated with the FBI. See also the Memorandum of Understanding between the FBI and DOD for counterintelligence activities within the United States. The Executive Order also requires each agency to have established procedures approved by the Attorney General for collecting information on United States persons.

When contemplating prosecution of a national security matter, Trial Counsel must develop a comprehensive understanding of the underlying investigation and investigative techniques employed. When conducting a counterintelligence investigation for intelligence purposes, agencies may employ investigative techniques that may be too sensitive for public disclosure at trial. Use of information derived from such techniques for prosecution must be authorized by the originating agency and, in some cases, may require prior authorization by the Attorney General of the United States.

In addition to understanding the techniques employed by investigative agencies, Trial Counsel must also gain familiarity with any "walls" that may exist, or may have existed, between an intelligence collection agency and the law enforcement community. Any such walls will govern the information sharing mechanism established between the two communities and provide insight into how/whether information may be used at trial. Information sharing walls have been, in essence, the clearinghouse through which information obtained by one community would pass before being given to the other. The purpose of such a wall has been twofold. First, the wall protected intelligence equities by insuring foreign intelligence information passed to law enforcement from the intelligence community would be used for lead purposes only and would not become germane to the case-in-chief for prosecution. Thus the wall reduced the risk that sensitive intelligence gathering or investigative techniques would be lost through public

disclosure. In turn, the wall protected the United State's ability to prosecute a case by ensuring information derived from sensitive techniques employed by the intelligence community would not be implicated in a manner which would require the United States to halt litigation – i.e., a case would not get to a point which would force the government to decide that further litigation would cause unacceptable damage to the national security by causing undesired disclosure of information. More recently, law enforcement saw a rise in use of walls to protect certain types of law enforcement information from unlawful disclosure to the intelligence community, i.e., ensuring the statutory prohibitions against sharing grand jury and/or Title III electronic surveillance with the intelligence community were observed.

Some of the perceived problems in information sharing were addressed by the USA Patriot Act of 2001, Pub. L. 107-56, 115 STAT. 272 (October 26, 2001). Among other changes, the U.S.A. Patriot Act removed the statutory prohibitions against sharing grand jury and/or Title III electronic surveillance information with the intelligence community and encouraged the increased sharing of information obtained through intelligence sources with law enforcement. It also brought the legal standard for use of certain intelligence investigative authorities more in line with the law enforcement authorities. Although the U.S. Patriot Act relaxed some of the restrictions on information sharing, the general concept of maintaining a distinction between the intelligence and law enforcement communities remains.

Due to the nature of national security cases and the breadth and implication of operational and policy questions underlying the national security decision-making process, questions regarding use of investigative techniques and coordination with other agencies typically need to be resolved at the national level. While the Navy may have a strong criminal prosecution interest from an evidentiary and policy point of view, the Navy must take into consideration broader evidentiary and policy implications that may affect equities beyond those of the Navy or the local command. Coordination through Code 17 is not intended to limit the prosecutorial discretion of the Trial Counsel or local commander. Rather, coordination through Code 17 provides a process through which Trial Counsel and the local commander will be able to make the most fully informed investigative and prosecutorial decisions that will serve the national security interests of the United States while preserving the Navy's ability to effectively prosecute its case.

B. Coordinating With Equity Owners.

1. Prosecutions involving other federal agencies. The Intelligence Community is comprised of 13 government agencies and organizations that carry out the intelligence activities of the United States. Often, national security litigation will touch upon the equities of several intelligence agencies. In addition to the Intelligence Community, a variety of other federal agencies routinely produce sensitive or classified materials and oversee classified programs. Thus, close coordination with other Executive Branch Departments and agencies is necessary from the onset of any litigation that may involve national security matters.

2. Code 17's role. Within the Office of the Judge Advocate General, Code 17 is charged with effecting proper liaison with other Executive Branch departments and agencies for all national security litigation. Code 17 will initiate all contacts with outside agencies and facilitate

discussions of inter-agency issues likely to arise in litigation. Additionally, Code 17, in conjunction with CNO (N09N2), will assist counsel in obtaining authorization to use information belonging to other agencies in litigation.

3. Liaison with other agencies. Code 17 will initiate all contacts with Executive Branch departments or agencies on behalf of the JAGC in national security cases and all other cases involving classified information. Staff judge advocates or trial counsel assigned to any case involving classified materials or programs must contact Code 17 immediately upon making the determination that the case at hand may involve classified information or meet the definition of a national security case set forth in JAGMAN 0159 (see Chapter 7 of this Guide on "Designation As A 'National Security case'"). Code 17 will, in turn, contact relevant agency and facilitate discussions with government counsel.

4. Work with attorneys rather than operators. As part of its investigation and/or classification review, the Navy may identify information or evidence that originated in another Executive Branch department or agency. In cases that may lead to litigation, all discussions regarding evidentiary matters involving classified materials must be coordinated at the Headquarters level, through the respective Office of General Counsel or Judge Advocate General. Although Code 17 will initiate and coordinate this contact, it is imperative that counsel maintains all discussions with third agencies through agency counsel, rather than making direct contact with research and development or operational personnel independent of Code 17 and agency counsel. This is particularly important when working a case that involves intelligence information, because each agency within the Intelligence Community operates under its own authorities and is responsible for fulfilling specified intelligence requirements. Attorneys representing the agency whose information is involved are best suited to identify any potential issues that must be considered prior to trial. In addition, agency counsel is in the best position to identify appropriate witnesses for litigation. Coordination with agency counsel will ensure counsel is fully educated on the complexity and sensitivity of issues that are likely to arise in litigation. In addition, agency counsel will be able to identify for counsel potential limitations regarding the use of certain evidence at trial. Although such limitations may directly impact counsel's ability to bring certain charges against the accused, coordination with agency counsel allows for a vigorous and thorough discussion prior to bringing charges. The goal of such discussions should ultimately be a prosecutorial decision that reflects the best interests of the United States overall.

5. Classified information and Brady disclosures. In certain cases, trial counsel may be confronted with an apparent conflict between a legal obligation to disclose exculpatory evidence, as set forth in R.C.M. 701, *see also Brady v. Maryland*, 373 U.S. 83 (1963), and another agency's obligation to protect intelligence sources and methods or sensitive information. Generally, when an agency provides support to an ongoing investigation that becomes ripe for prosecution, that agency's records may be subject to the discovery process. In such cases, trial counsel, in conjunction with Code 17, must work with agency counsel to determine whether the agency has exculpatory information that must be disclosed to the defense to insure constitutional due process or satisfy any other procedural or ethical requirement. If such information is identified, trial counsel must work with Code 17 and agency counsel to determine if there is any way the information may be disclosed in proceedings. If possible, such discussions should take

place prior to the preferral of charges against an accused or the filing of any responsive document in civil litigation. A determination that the information cannot be disclosed to the defense or opposing party may result in the dismissal of charges or the ultimate inability of the government to effectively prosecute its case.

6. The "third-agency rule". When working with classified material, trial counsel should be cognizant of and adhere strictly to what is known as the "third agency rule". Executive Order 12958 section 4.2(b) expressly states:

> "Classified information shall remain under the control of the originating agency or its successor in function. An agency shall not disclose information originally classified by another agency without its authorization…"

When preparing for litigation, trial counsel must understand that this provision requires authorization from the originating agency before disclosing classified information to any person or agency outside official Navy channels. Thus, prior to sharing classified information with any outside person or agency, trial counsel must identify the originator(s) of the information and seek express authorization to share such information with a specified person or agency. CNO (N09N2) and Code 17 will assist trial counsel in obtaining such authorization. This restriction applies within and among government agencies, as well as to sharing information with cleared opposing counsel and/or the accused. Thus, government counsel should not share any potentially classified information with anyone not assigned to the prosecutorial or investigative team prior to discussing the case with Code 17 and obtaining appropriate authorizations. Government counsel should keep in mind; a third-agency's determination of whether or not to authorize use of certain information may greatly impact upon what charges can be successfully prosecuted. Thus, Government counsel should not prefer charges that could implicate third agency information without complying with the third-agency rule as discussed herein.

In order to fully comply with the third-agency rule, government counsel must obtain the originating agency's authority to share information prior to releasing any such information to other members of the Intelligence Community, including other military or DOD components, or any other Executive Department or agency. Because this also applies to sharing information with the Department of Justice, trial counsel must, through Code 17, coordinate all discussions of classified material with the relevant agencies. Again, government counsel is not authorized to share any classified material with cleared opposing counsel or the accused without the express authorization of the originating agency.

7. The Foreign Intelligence Surveillance Act (FISA). The Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. 1801 et. seq., as amended by the USA Patriot Act of 2001, Pub. L. 107-56, 115 STAT. 272 (October 26, 2001), provides a statutory framework by which the government may obtain information through electronic surveillance, pen register/trap and trace, subpoena or physical search for foreign intelligence purposes. Special consideration must be given whenever techniques authorized by the Foreign Intelligence Surveillance Court (FISC) have been used in a national security investigation.[4] If trial counsel learns that techniques authorized by the FISC were used in the course of an investigation, trial counsel should request

[4] See earlier discussion of "significant purpose."

Code 17 to immediately contact the Office of Intelligence Policy and Review (OIP&R)[5] at the Department of Justice. Trial counsel should also request Code 17 to contact any other agency counsel whose agency may have an interest in the FISA information at issue.

When contemplating use of FISA derived information as evidence in a military justice proceeding, trial counsel should be aware of the following issues:

a. AG Authorization. The FISA, at 50 U.S.C. 1806(b), specifically requires the Attorney General of the United States to authorize any use of FISA information, or any information derived therefrom, in a law enforcement proceeding. (Although this Guide addresses military justice litigation which is, by definition, a law enforcement proceeding, AG authorization is required as a matter of OIP&R policy prior to use of such information in any proceeding that could lead to litigation of an underlying FISC Order). Upon learning of any information derived from a FISC authorized technique, trial counsel should contact Code 17 for proper coordination with OIP&R.

b. Notice to the aggrieved person and the court. As statutorily mandated, the United States must provide an aggrieved person[6], prior to use, notice that it intends to use information obtained through FISC authorized techniques against an aggrieved person in proceedings. The court or other authority in which the information is to be used must also be notified. Notice must be provided prior to use in any proceeding. If trial counsel intends to use FISA information in its prosecution, OIP&R will assist in providing appropriate language to satisfy the notice requirements. OIP&R should also be contacted to determine to what extent information obtained in the course of an investigation in which FISC authorized techniques were used is considered to be FISA derived.

c. Litigation of the FISA surveillance or search. In accordance with the FISA, an aggrieved person may challenge the introduction of information acquired through FISC authorized techniques on the grounds that the information was unlawfully authorized or acquired (50 U.S.C. 1806(e), 1825(f), 1845(e)). Jurisdiction to hear such a suppression motion falls solely in the District Court in the same District as the authority in which FISA information is to be

[5] As set forth in 28 CFR 0.33 (Subpart F-1), OIPR supervises all litigation involving matters of concern to the Foreign Intelligence Surveillance Court.

[6] "Aggrieved person" is a term of art that reflects the authority that was obtained from the FISC. See 50 USC 1806(k) regarding electronic surveillance; 50 USC 1821(2) regarding physical search; 50 USC 1841(3) regarding pen register/trap and trace.

used. Military Courts do not have jurisdiction to hear cases involving a challenge to the legality of use of FISA techniques. United States v. Horton, 17 M.J. 1131 (NMCMR 1983).

d. Disclosure of FISA information and underlying techniques. Investigations involving the use of FISA techniques are classified and often very sensitive. If another agency or organization obtained a FISC Order, that agency's counsel should be involved in all discussions regarding the use of its FISA derived information.

CHAPTER 7

Designation as a "National Security Case"

A. Introduction. "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 will actually be designated as national security cases. Whether a case qualifies 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. In addition, once designated as a national security case, the case is subject to special procedural requirements. The limitation on initial disposition authority is pursuant to R.C.M. 306 and JAGMAN § 0126c. Initial disposition authority for cases involving national security has been limited to those officers listed in JAGMAN § 0126c. The list is made up of very senior commanders, typically 3-star and 4-star admirals and generals. An officer who is a convening authority but not an NSCDA must forward a potential national security case to an appropriate NSCDA. 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.

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 § 0159a, a "national security case" is one which:

> to any serious degree . . . involves the compromise of a military or defense advantage over any foreign nation; involves an allegation of willful compromise of classified information, or affects our military or defense capability to successfully resist hostile or destructive action, overt or covert.*
>
> (*See the last paragraph of this chapter for pending changes to the definition).

Examples of offenses which may be designated as national security cases include, but are not limited to, charges under Article 92, UCMJ (Violation of General Order), Article 106a, UCMJ (Espionage), 18 U.S.C.§ 793 (Espionage), and other federal statutes. See Chapter 8 of this Guide for a more detailed discussion of charges.

Designation of a case as a national security case is not an automatic conclusion, but rather requires the NSCDA to weigh many factors. Even a case that involves a charge under 18 U.S.C. § 793, the federal espionage statute, could be designated a non-national security case if no actual compromise occurred or if the offense is not of a "serious degree." The factors which the NSCDA must consider include the type of information involved, the status of the unauthorized recipient (if any), and the intent of the accused. For example, if no actual compromise occurred, the case would not involve an unauthorized recipient, but it still could be a national security case if the accused had the intent to give the information to a foreign agent. On the other hand, 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.

Because designation of a case as a national security case involves a significant amount of discretion, it is important that the NSCDA be the officer who exercises that discretion. Accordingly, a case should be forwarded to an NSCDA if it appears to involve any of the factors in the definition. A good rule of thumb is that the case should be forwarded if it meets any of the listed criteria (i.e., actual compromise, allegation of willful compromise), and then let the NSCDA determine if it rises to a "serious degree."

C. Identification of NSCDA and Convening Authority. Although the accused's commanding officer may be a convening authority, he or she likely is not a 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. If the CO does not have the proper level of authority, he simply forwards the case up his chain of command to the first officer with the proper authority. The only difference is that the NSCDA may be several levels higher up the chain. 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 GCMs. 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 Guide, must be followed.

D. Special Requirements - Pretrial Agreements and Immunity. One of the most significant special requirements in a national security case is that the government may not enter into a pretrial agreement (PTA) without the approval of the Secretary of the Navy. In accordance with JAGMAN § 0137c, if the accused proposes a PTA which the convening authority is inclined to accept, the convening authority must request permission from the Secretary before actually accepting it. The convening authority's request must give the background of the case, summarize the available evidence, and justify why a PTA is in the best interest of the government. JAGMAN § 0137c outlines the information which must be included

in the approval request. Code 17 will assist in this process. It is important to note that while secretarial approval is required for entering into a PTA, 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). Just as with other major federal cases, if the government intends to grant immunity to any witness in a national security case, it must first consult with the Department of Justice, as discussed in JAGMAN §§ 0125 and 0138. Code 17 will assist the convening authority and trial counsel if they desire to immunize a witness. Chapter 10 of this Guide provides further discussion on PTAs and grants of immunity.

E. Special Requirements - Post-Trial. If a case has been designated as a national security case, only the Secretary of the Navy may remit or suspend any part or amount of the sentence. This is requirement is found in JAGMAN § 0159 and correlates to the requirement that the Secretary of the Navy must approve any proposed PTA in a national security case. It is also important to keep in mind that 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 in accordance with SECNAVINST 5510.36. Before forwarding a record of trial which contains any classified portions, contact Code 17 to coordinate transfer and storage.

F. Pending Changes. Although not yet approved, there are several pending recommendations for JAGMAN revisions to sections dealing with national security cases. The definition of a national security case, currently found in JAGMAN § 0159a, will be combined with § 0126, for ease of reference. The definition will also be expanded to include acts of terrorism and to expressly state that attempts to commit and conspiracies to commit covered offenses are included in the definition. Current section 0126c, which is the list of NSCDAs, will be updated to better reflect current Department of Navy command organization. Also, if approved, Commander in Chief, U.S. Atlantic Fleet, will be designated as the NSCDA for second echelon commanders who are not themselves NSCDAs. Finally, the requirement in section 0126f to make periodic case status reports to OJAG once every 60 days will be changed to require reports once every 30 days.

CHAPTER 8

Charges in a National Security case

A. Introduction. Charges in national security cases often include violations of articles under the UCMJ, as well as violations of other federal statutes, such as offenses under title 18, U.S.C. It is essential for judge advocates to be familiar with the practice of charging violations of federal statutes under Clause 3 of Article 134, UCMJ (Crimes and Offenses Not Capital). Possible charges in a national security case or a case involving classified information include, but are not limited to, those offenses listed in JAGMAN § 0159a. The charges discussed below are a sampling of those that are typically charged in these cases.

B. Charging under the Uniform Code of Military Justice.

1. Article 92 – Failure to obey order or regulation. An Article 92 violation would most likely be charged in a case involving a relatively minor allegation of mishandling of classified information, as opposed to a more serious case of a willful compromise. The applicable regulation is Secretary of the Navy Instruction (SECNAVINST) 5510.36. The issue to be aware of is 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 SECNAVINST 5510.36. Provisions in chapters 10 and 12 are the most likely to support such a charge.

Another option to consider is to charge a violation of the Classified Information Executive Order. Section 4.2(c) of 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) also contains language that simply and clearly prohibits unauthorized disclosures of classified information.

A third possibility under Article 92 is 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 SECNAVINST 5510.36 and E.O. 12958, and, in many cases, the service member received an indoctrination upon being granted a clearance and signed a non-disclosure agreement (NDA). A failure to safeguard classified information would constitute a dereliction of this duty and, depending on the facts, could be charged either as willful or negligent.

2. Article 106a – Espionage. The Uniform Code of Military Justice has specific provisions regarding Espionage, the elements of which are set forth in Article 106a. Generally speaking, 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. 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." Transmission of certain types of information may be punishable by death. Article 106a identifies such information warranting a capital charge as that 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.

To succeed on an Article 106a charge, 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.

To succeed on a capital charge, 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.

3. Article 134 - The General Article. Service members may be charged under Clause 3 of Article 134, UCMJ, for violations of federal statutes that are not specifically contained in the UCMJ. Several such statutes are available in national security cases and cases involving classified information. JAGMAN § 0159 contains a list of federal statutes that relate to national security. Many cases will involve the statutes discussed below. Sample specifications are provided in Appendix 8-A.

a. 18 U.S.C. § 793. In many cases involving national security or classified information, the evidence will indicate a violation of 18 U.S.C. § 793 ("Section 793"), which 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 differs from Article 106a, UCMJ (espionage), in that is does not require any intent or attempt to give the information to a foreign entity. Section 793 is in effect a lesser offense than espionage, and is aimed at preventing 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.

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, but is often 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, whereas 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 national security cases. Within title 18, counsel should consider section 1001 (false statements when the falsification or concealment concerns any actual, prospective, or attempted commission of a crime against national security), section 792 (harboring or concealing persons), section 794 (gathering or delivering defense information to aid foreign government), and section 798 (disclosure of classified information). In addition, sections 2151 through 2156 of title 18 (chapter105) 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 which 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 or receive classified information, or conspire to do so.

C. Death penalty eligible national security cases

1. Eligible Articles.

a. 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 orindirectly, is guilty of this offense. For the offense of aiding the enemy, either a court-martial or a military commission may award the death penalty.

b. 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 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.

c. Art 106a. – Espionage (if referred capital) . Any person subject to this chapter who, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, transmits, or attempts to do so, to any entity described in paragraph two below, either directly or indirectly, anything described in paragraph three below, shall be punished as a court-martial may direct.

2. For the death penalty to be imposed, for the foregoing offenses, the requirements of R.C.M. 1004 must be met. 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 UNDER ARTICLE 134, UCMJ

§ 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.

§ 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:

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.

CHAPTER 9

Classified Information Protections

A. Military Rule of Evidence 505.

1. Purpose. Military Rule of Evidence (Mil. R. Evid.) 505 is an executive privilege designed to protect classified information from disclosure at an Article 32 hearing or court-martial. Under Mil. R. Evid. 505, classified information is privileged from disclosure if disclosure would be detrimental to national security. This privilege, also known as the "classified information privilege", is asserted by the head of the executive agency or department concerned. Within the Department of the Navy, it is the Secretary of the Navy (SECNAV) who *personally* asserts the privilege over classified material. SECNAV is then said to be "claiming" the privilege.

2. Procedures for asserting the privilege. SECNAV may assert the privilege based upon a finding that 1) the information at issue is properly classified and that 2) disclosure would be detrimental to national security. These findings are the *sine qua non* of assertion of the privilege, and SECNAV relies on subject matter experts to establish them in sworn affidavits. As the name implies, a subject matter expert is someone in a position to be intimately familiar with the classified material in question. Typically, a subject matter expert works for an organization or command that is an Original Classification Authority (OCA), and they are frequently the same individuals involved in the classification review of the material (see below). The subject matter expert's affidavit first establishes his or her credentials and provides a brief and general discussion of the nature of classified information. Next, the affidavit explains the type of material at issue, the level at which it is classified (Confidential, Secret or Top Secret), and the degree of damage to national security that would result from its disclosure at a judicial proceeding. Finally, the subject matter expert states that it is his or her opinion that SECNAV should assert the Mil. R. Evid. 505 privilege to prevent disclosure of the classified material at the judicial proceeding. The subject matter expert's affidavit is then forwarded to the head of the agency or command for which the expert works. This head of the agency or command, who, as mentioned above, is also the OCA, then endorses the affidavit. The expert's affidavit, along with the endorsement of the OCA, is then forwarded to SECNAV via the Judge Advocate General. A sample affidavit and OCA endorsement is provided in Appendix 9-A.

Next, SECNAV reviews the sworn affidavit of the subject matter expert and its endorsement. He then relies upon the information provided to him in the affidavit and asserts the claim of the Mil.R.Evid. 505 privilege. A sample of the letter in which SECNAV asserts the claim of privilege is in Appendix 9-B.

3. Code 17 assistance. Code 17 maintains a library of sample affidavits and endorsements and is readily available to assist those tasked with preparing them. In addition, Code 17 also serves as the focal point for the routing of the affidavits to SECNAV (via the Judge Advocate General) and prepares the necessary executive correspondence required to accompany them.

4. Utility of Mil. R. Evid. 505. Mil.R.Evid. 505 allows SECNAV to authorize a witness or trial counsel to assert the privilege on his behalf. The authority claiming the privilege may authorize witnesses or counsel to assert it on his behalf, and this authorization may be presumed in the absence of evidence to the contrary.

Mil. R. Evid. 505 is useful because if the need for invoking this privilege is properly anticipated some of the myriad difficulties surrounding protection of classified can be avoided later on as tempo of court proceedings increases. Since invocation of the privilege is predicated on the proper classification of the potential corpus of relevant evidence, timely arrangement of the official classification review is essential, especially in more complex cases involving a large volume of material or when there is more than one classification authority participating in the review process.

5. Targeting potential classified evidence. In the course of investigation, NCIS may discover the subject has possession of a substantial library of classified documents in a variety of formats, hard copy or digital. The documents may reflect a pattern of behavior spanning many years, involving several duty stations and affecting several classified programs. Some of the information may originate in other federal agencies or military departments. Trial Counsel should ensure a thorough classification review is conducted prior to making any determinations as to the possible use of any document in further investigation or at trial.

One of the most critical aspects of trial preparation will be choosing which documents to use in litigation and/or plea negotiations. As a practical matter, not all documents discovered in the course of an investigation are likely to be used in this manner. Instead, Trial Counsel should identify a representative sample of documents that reflect the subject's pattern of behavior and scope of criminal activity. While the Trial Counsel may identify the "ideal" set of documents to be used to prove certain charges, the originating agency of the information could ultimately object to and prevent such use. Thus, in identifying a representative sample, Trial Counsel should determine for each document, exactly what each document will prove and how each document will further the case to be presented. The originating agency(ies) will ultimately make the determination of whether or not and how documents may be used in litigation.

In the course of identifying documents for use, NCIS may be in a position to further question the subject. In some cases, NCIS has been able to obtain sworn statements from a subject for use later at trial or in negotiations. Relevant questions regarding the subject's knowledge of the documents include, but are not limited to: where a document came from; how the subject came to possess it; how/where the subject stored it; what the subject knew about the document's classification level; what the subject intended to do with the document; and to whom the subject may have given the document or given access to the document. Such questioning should be conducted only after coordination with the originating agency. The subject shall be afforded all appropriate warnings prior to such questioning by NCIS.

All discussions with the originating agencies and questions regarding use of certain documents should be coordinated with Code 17.

B. Applying Mil. R. Evid. 505 To The Article 32, UCMJ, Hearing (R.C.M. 405). All Government/ trial counsel, Staff Judge Advocates, and defense counsel must be intimately familiar with R.C.M. 405. A thorough review of the Rule is essential before proceeding with this section.

1. Cautions for classified information in preparing for and participating in the Article 32 hearing. Having reviewed R.C.M. 405, the application of the classified information privilege under Mil. R. Evid. 505 will now be discussed. In a case involving national security and/or classified material, the convening authority's responsibilities are particularly important. Therefore, the staff judge advocate is a key player. First rule -- STOP and REFLECT. Remember that inactivity does not always signal inattention, and activity does not always result in achievement. The Article 32 investigation appointing authority's staff judge advocate must take an active role in all cases involving national security and/or classified information. This is not so much to speed the process along, but to slow the process to prudent dispatch. As Code 17 predecessors have emphasized, the national interests in a complete and expeditious damage assessment may, in the context of an espionage investigation, be so compelling as to outweigh the value of prosecution. The determination of the relative importance of these competing interests requires dispassionate consideration -- without regard to parochial or institutional agenda -- and should therefore vest in senior policymakers in the Executive Branch.

The function of intelligence officers, criminal investigators, attorneys, and commanders should be to ensure that the policymakers are aware of the various interests at stake so as to be able to make an informed decision. Therefore, the staff judge advocate must engage the security manager for assistance and advice to ensure the equity owners are notified of possible compromise and concur in disciplinary proceedings. Therefore, the equity owners 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. In that regard, the Intelligence Community controls the process. This may be relatively easy in cases involving SECRET and CONFIDENTIAL information, particularly technical and training publications, or information that does not involve "sources and methods" of intelligence gathering. The values change, however, when addressing TOP SECRET and TOP SECRET/ SENSITIVE COMPARTMENTED INFORMATION (TS/SCI or "CODEWORD").

In many instances when information contains "sources and methods" the U.S. Government uses to gather intelligence information and is extraordinarily sensitive. In some instances, the violation may be insignificant when compared to the harm that might result from litigation and discovery rules. One function of Code 17 is to quickly make the link between cognizant convening authorities, staff judge advocates, and the legal staffs of Intelligence Community (IC) in national security and/or classified information cases. If the Article 32 appointing authority is presented with preferred charges, an initial consideration might be to dismiss them pending further investigation under R.C.M. 401(c)(1) and consultation with the IC legal staffs. If the suspect is in the brig, consider release. If release is not a valid option, ensure that the diligence exercised in consulting the IC legal staffs and the disciplinary processing of the charges, if any, is real and documented.

2. Article 32 and the classified information privilege. As was stated, the classified information privilege under Mil. R. Evid. 505 does apply at the Article 32 hearing. R.C.M. 405 states that:

> If, prior to referral the Government agrees to disclose to the accused information to which the protections afforded by Mil. R. Evid. 505 or 506 *may apply*, the convening authority, or other person designated by regulation of the Secretary concerned, may enter an appropriate protective order, in writing, to guard against the compromise of information disclosed to the accused.
> R.C.M. 405(g)(6). (emphasis added).

This provision suggests that the convening authority must act to protect *possibly*, and not just certainly, classified information from disclosure (use), that might have been or will be disclosed (discovery) to the defense, before any classification review has been accomplished. This can be done by a separate protective order or included in the Article 32 appointing order. The protective order in Appendix 4-A may be tailored for this purpose.

In *ABC, Inc. v. Powell*, 43 M.J. 363 (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." The Article 32 appointing authority and pretrial investigating officer no longer have unbounded discretion to order Article 32 investigations closed to the public.

The need for a classification review before the decision to pursue serious disciplinary action or court-martial is now paramount. CNO(N09N2) are the experts that assist NCIS and the command in determining who will perform the task of classification review. By way of review, ordinarily the Original Classification Authority (OCA) appoints a subject area expert to review the classified information to ensure it was properly classified at the time it was mishandled, is properly classified now, and recommends the Mil. R. Evid. 505 privilege be asserted. The expert will provide an affidavit to that effect. The OCA then endorses that affidavit. Code 17 assists the cognizant command staff judge advocate and NCIS in coordinating the classification reviews with N09N2. Code 17 and N09N2 have exemplars of the affidavits. These affidavits are key to the process. Although R.C.M. 405 applies Mil. R. Evid. 505 to the pretrial investigation, by its very terms M.R.E 505(i)(4)(A) requires only affidavits, briefs and arguments to determine the privilege (*See also* Mil. R. Evid. 104, which states that the military judge is not bound by the rules of evidence in determining the existence of a privilege) and, in most instances, provides the foundation under *Grunden* to close the proceedings. That is, in the extraordinary circumstance in which the Article 32 appointing authority chooses to allow the Investigating Officer any such discretion.

1. Unclassified Article 32 hearing. Under R.C.M. 405 and Mil. R. Evid. 505, the Article 32 appointing authority can avoid litigation before the IO of what parts of a pretrial investigation should/can be closed to the public by exercising his or her authority to order an unclassified pretrial investigation. This can be done before classification review (R.C.M. 405(g)(1)(B) protecting information that "may be protected" under Mil. R. Evid.

505, or R.C.M 405(g)(6) protecting information to which Mil. R. Evid. 505 "may apply" by protective order) or after classification review and the privilege is claimed (Mil. R. Evid. 505(d)). The Article 32 appointing order would include an order that no classified information is to be disclosed at the Article 32 investigation and that unclassified substitutes and testimony will be taken as appropriate under R.C.M. 405(g)(6), Mil. R. Evid. 505(d), and 505(i)(4)(D). Depending on the circumstances, the defense would likely have the opportunity to review the substitutes and verify their accuracy with the original evidence.

2. Article 32 Appointing Authority orders closed sessions**.** Alternatively, in the extraordinary circumstance in which classified information must be disclosed at the Article 32 hearing, the Article 32 appointing authority can review the classification review and order portions of the hearings closed. This must be done with care, and the Article 32 appointing authority must express in the closure order the considerations required by Mil. R. Evid. 505 and *Grunden* in ordering sessions closed to the public to receive evidence on certain subject matter.

C. 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. That is, the Government cannot provide the defense with copies of or access to the classified information in the investigative file or otherwise requested by the defense in order simply to avoid litigation over discovery. Rather, the Government must first determine that the defense has or reasonably may have a "need-to-know" the classified information. This is because a possessor of classified information may not provide that information to another who does not have a need-to-know. E.O. 12958, at § 4.2. The bottom line rule is that if the defense has no need-to-know classified information, the Government may not provide it. Such a rule should not chill defense counsel from zealously representing the accused and from seeking access to classified information that defense counsel believes may assist in the preparation of the defense.

Where there is a disagreement between the Government and defense counsel on whether the defense has a need-to-know, the disagreement must be decided by the convening authority before referral of charges phase; and by the military judge after referral of charges. In fact, the military judge, upon a defense pretrial motion for appropriate relief may reverse the need-to-know determination of the convening authority and remand the case for a new Art 32 investigation.

The principles used to determine the defense's need-to-know classified information are those relevant to criminal discovery and privileged information. The *procedures* used to make those determinations are found in R.C.M. 405(g)(6) and Mil. R. Evid. 505(d) for Art 32 investigations and Mil. R. Evid. 505(g) for courts-martial.

Another 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). In a case involving classified information from multiple originating agencies, the process for obtaining approval from each agency to disclose its classified information to the

defense can be complex and quickly grow unwieldy if not started early. Thus, immediate consultation with Code 17, N09N2, and the originating agencies is important to ensure the Government will have permission to disclose to the defense that classified information for which the defense has a need-to-know.

In light of the approval requirements to providing classified discovery, convening authorities should forego or dismiss charges that would unnecessarily bring classified information into the case. Further, trial counsel should select carefully the 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.

Before beginning classified discovery, trial counsel *must* assure that:

1. The classification review of the material to be produced has been completed;

2. Improperly marked documents have been corrected with proper markings; and

3. Classified information no longer warranting protection in the interests of national security has been declassified.

In other words, trial counsel must be sure before providing in discovery any classified document that the classified document is properly classified. While the proper classification of a document may be irrelevant to the elements of an offense, it is necessary to invoking the protections of Mil. R. Evid. 505.

In any case in which the Government believes classified information may be subject to or sought in discovery, it must determine as soon as possible whether it intends (or may be permitted by the originating agency) to produce that information. Because there will be cases in which the Government does not foresee that the defense may request discovery of classified information, the investigating officer is required to notify the convening authority "as soon as practicable" upon receipt of such a request. R.C.M. 405(g)(1)(B).

If the Government determines it will not produce the classified information regardless of a defense request, it should obtain from the convening authority an order barring the disclosure of any classified evidence during the Art. 32 investigation. The convening authority may issue such an order without requesting a formal invocation of the Mil. R. Evid. 505 claim of privilege so long as the convening authority reasonably believes the privilege *may* apply. R.C.M. 405(g)(6). The best practice is for the convening authority to issue such an order with the Art 32 appointing order. Code 17 has sample orders. However, before the convening authority issues such an order, the convening authority's staff judge advocate, Government counsel, and Code 17 should review the case and assess the likelihood that such a decision will withstand a motion for appropriate relief.

Upon receiving a defense request for discovery of classified information, 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 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)(6). With respect to classified information, the custodian of evidence may include both the originating agency and the convening authority. The originating agency 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 originating agency'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 originator of the classified information, he or she may lack the authority to release it.

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)(3)(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 originating agency and the convening authority -- if both have determined the classified evidence not to be 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. R.C.M. 405(g)(3)(C). Unless the defense request was wholly frivolous, the defense should expect to file such a motion as soon after referral of charges as possible.

D. Protective Orders. During the pre-referral stage, if the Government agrees to produce classified discovery to the defense, the convening authority may enter a protective order. R.C.M. 405(g)(6). Although the rule is permissive, it should be treated as mandatory. The convening authority may issue such a protective order only the Secretary of the Navy has asserted the Mil. R. Evid. 505 claim of privilege over the classified information. Mil. R. Evid. 505(d). The defense must raise any objection to the terms of the protective order or to a withholding of information after referral of charges in a pretrial motion for appropriate relief under R.C.M. 906(b)(3). Mil. R. Evid. 505(d). The sample protective order in Appendix 4-A, designed for issuance by a military judge, may be tailored for issuance by the convening authority in the pre-referral stage. The substance of the order remains the same.

If the defense does have a need-to-know certain classified information, trial counsel should examine whether a permissible alternative exists to disclosure of the classified

information (discussed in greater detail under protective orders). Producing the actual classified information should only occur when there is no permissible alternative.

Permissible alternatives to disclosure of classified evidence are found in Mil. R. Evid. 505(d) and (g). These alternatives include:

1. Redacting some or all of the classified information from documents before producing them;

2. Substituting unclassified descriptions of the classified information or a summary of the entire document; and

3. Substituting a statement admitting the relevant facts the classified information would tend to prove.

The first alternative--redacting the classified information out of the document--is the preferred alternative when the classified information is irrelevant. 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 §§ 783(b),[7] 798,[8] and 1924, all of which can be assimilated under Art. 134. In addition, violations of general orders for handling classified information do not require a showing the classified information at issue was properly classified. 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 should select that limited amount of classified information to use as evidence for such purposes and redact the rest of the classified information from the document.

The second alternative--substituting unclassified descriptions of classified information or a summary of the entire document--is the preferred alternative where the precise classified information is not necessary to the purpose of the document. An example might be the name of a covert intelligence agency employee. In such a case, the Government might substitute "CIA

[7] "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).

[8] "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).

employee 1" in place of the precise name. Another example might be a classified technical document containing the chemical composition of radar-absorbent material. The Government might provide a summary of the document to the effect that the document is x pages in length, provides the chemical composition of a radar-absorbent material, and bears the marking "SECRET" on the top and bottom of both pages.

The third alternative--substituting a statement admitting the relevant facts the classified information would tend to prove--is the preferred alternative where the classified information is not amenable to redaction or summarization, and the fact sought to be proved is unclassified and not central to the case. In practice, this is rarely done.

APPENDIX 9-A1

CLASSIFICATION REVIEW- SAMPLE OCA COVER LETTER

From: Commander, Naval Sea Systems Command
To: Office of the Judge Advocate General (Code 17)

Subj: CLASSIFICATION REVIEW AND DECLARATION ICO U.S. v. BROWN

Ref: (a) CNO ltr 5510.4 Ser 09N2/001 of 1 Jan CY [request for classification review]

Encl: (1) Declaration of A. A. Smith [affidavit of subject matter expert]

1. Reference (a) requested classification review of Document Alpha in support of the investigation into the alleged misconduct of Seaman Brown, to include an affidavit from a subject matter expert and an endorsement by the Original Classification Authority.

2. I am an Original Classification Authority for up to and including SECRET information regarding the Alpha program, to which Document Alpha pertains. I am the supervisor of A.A. Smith. I have over 20 years experience with the Alpha program, and Mr. Smith has worked with the program for 15 years. Mr. Smith is available as a subject matter expert witness should that be necessary.

3. I have reviewed enclosure (1) and agree with Mr. Smith's analysis of Document Alpha, and that its disclosure to unauthorized persons could cause damage to the security of the United States. Declassification of the information for the purpose of prosecuting a court-martial is not warranted. I strongly recommend that the Secretary of the Navy assert the claim of privilege under Military Rule of Evidence 505 for this information.

4. Please direct any questions regarding this matter to my Staff Judge Advocate at DSN xxx-xxxx.

M. R. JONES
Commander

APPENDIX 9-A2

CLASSIFICATION REVIEW- SAMPLE DECLARATION

DECLARATION

I, LCDR _____, USN, declare and state:

BACKGROUND

I am a ____ in the United States Navy and currently serve as the Anti-Submarine Warfare (ASW) Sensors Requirements Officer in the Office of the Chief of Naval Operations (N780). N780 is responsible for all matters pertaining to Maritime Surveillance policy. I have served in this position for ____ years and report to _____, Head, Aviation Plans and Requirements Division. I have served in the United States Navy for over ____ years, ___ of which include experience in Maritime Surveillance, ASW operations as a pilot, ASW Operator, and staff officer. As part of my official duties, I have been granted a TOP SECRET security clearance and am authorized access to classified information pertaining to _____. I further am familiar with the classification guides for information pertaining to _____.

PURPOSE OF DECLARATION

As part of my official duties, I have been made aware of a criminal investigation against LT _____ , USN, for the alleged improper handling of classified material. I was tasked to review certain classified materials to determine whether those materials contain information that is currently and properly classified. I submit this declaration to set forth the results of my review. I have determined that the materials I reviewed contain information that is currently and properly classified information pursuant to executive order and implementing regulations. I will also set forth the damage to the national security that I reasonably expect could be caused by the unauthorized disclosure of information in the materials.

I have deliberately excluded classified information from this declaration to facilitate its handling and use during any judicial proceeding.

CLASSIFIED INFORMATION

"Classified information" is information that has been determined pursuant to Executive Order 12958 (EO 12958) or any predecessor order "to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form." EO 12958, at §1.2(a) provides that:

> Information may be originally classified under the terms of this order only if all of the following conditions are met:
> (1) an original classification authority [OCA] is classifying the information;

(2) the information is owned by, produced by or for, or is under the control of the United States Government;
(3) the information falls within one or more of the categories of information listed in section 1.5 of this order; and
(4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security and the original classification authority is able to identify or describe the damage.

Upon determining that information is classified, the OCA then assigns one of three classification levels, based upon his assessment of the potential damage. EO 12958, at § 1.3(a) provides that if the OCA determines the unauthorized disclosure of the information reasonably could be expected to cause exceptionally grave damage to the national security, he classifies the information at the TOP SECRET level. If he determines the unauthorized disclosure of the information reasonably could be expected to cause serious damage to the national security, he classifies the information at the SECRET level. If he determines the unauthorized disclosure of the information reasonably could be expected to less than serious damage to the national security, he classifies the information at the CONFIDENTIAL level.

EO 12958, at § 1.7, provides that classified materials shall be marked as follows:

(a) At the time of original classification, the following shall appear on the face of each classified document, or shall be applied to other classified media in an appropriate manner:
(1) one of the three classification levels defined in section 1.3 of this order;
(2) the identity, by name or personal identifier and position, of the original classification authority;
(3) the agency and office of origin, if not otherwise evident;
(4) declassification instructions, which shall indicate one of the following:
(A) the date or event for declassification, as prescribed in section 1.6(a) or section 1.6(c); or
(B) the date that is 10 years from the date of original classification, as prescribed in section 1.6(b); or
(C) the exemption category from declassification, as prescribed in section 1.6(d); and
(5) a concise reason for classification which, at a minimum, cites the applicable classification categories in section 1.5 of this order.
(b) Specific information contained in paragraph (a), above, may be excluded if it would reveal additional classified information.
(c) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, which portions are exempt from declassification under section 1.6(d) of this order, and which portions are unclassified. In accordance with standards prescribed in directives issued under this order, the Director of the Information Security Oversight Office may grant waivers of this requirement for specified classes of documents or information. The Director shall revoke any waiver upon a finding of abuse.

EO 12958, at §1.7(f) specifies that classified information does not lose its classified status simply because a portion-marking was omitted.

EO 12958, at §1.6 provides that at the time of original classification, the OCA is to attempt to determine a date or event upon which the information can be declassified. The date or event is not to exceed 10 years. The date may be extended for 10-year intervals, not to exceed 25 years.

CLASSIFICATION DETERMINATION

I was tasked to and did review the following document, provided to me by Mr. _____ of the Office of the Chief of Naval Operations (N09N2): an official message from Commander Task Group (CTG) 12.0 dated _____; subject: "Anti-Submarine Warfare Exercise (ASWEX) 96-2 Post Prosecution Report," hereafter referred to as "the message." The message describes the ASWEX including objectives, forces involved, times, locations, environmental data, tactics employed, the effectiveness of those tactics, and lessons learned. Those matters are within my official responsibility. While I did not conduct a line-by-line review of the message to determine whether each paragraph was properly classified, I did determine that it contains currently and properly classified information. First, the information was contained within an official Department of the Navy originated document and, therefore, was produced by the United States Government. Second, the information pertains to "military plans, weapons systems, or operations," a category of information that may be classified under EO 12958, at § 1.5(a). Further, I reviewed Department of the Navy Security Classification Guide – OPNAVINST C5513.2B, "Air Warfare Programs and S5513.5B, Undersea Warfare Programs (U)." This Guide documents classification decisions made by a Department of the Navy OCA. The message I reviewed contains information that this Guide documents has been classified by an OCA. Further, the declassification date or event of the information in the message has not passed.

In addition, the message bears classification markings of "SECRET" at the top and bottom of each page, and portion-markings at the beginning of each paragraph. The highest level portion-marking of any individual paragraph was "(S)."

Therefore, information within the message meets both the substantive and procedural requirements of EO 12958 to be currently and properly classified.

PROTECTION OF INFORMATION

EO 12958, at § 4.2(f) requires each agency head "to establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons." Within the Department of the Navy, the Secretary of the Navy has established such controls via the Information and Personnel Security Program Regulations, SECNAVINST 5510.36 and 5510.30A. Pursuant to SECNAVINST 5510.36, 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 that provide protection for the classified material.

IMPACT ON NATIONAL SECURITY IF INFORMATION RELEASED

Based upon my experience with classified information pertaining to U.S. Navy maritime surveillance and ASW, I can articulate the reasonably expected damage to the national security that would occur should the information in the document be disclosed in an unauthorized manner. The release of the information reasonably could be expected to:

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 countermeasures by 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.

I declare under penalty of perjury that the foregoing is true and correct.
Executed on this _____ day of _____ 2002.

_____
LCDR USN
OPNAV N78
ASW Sensors Requirements Officer

APPENDIX 9-B

SAMPLE MIL. R. EVID. 505 SECRETARIAL ASSERTION

From: Secretary of the Navy
To: Commander, Naval Submarine Forces, U.S. Pacific Fleet

Subj: AUTHORITY TO ASSERT CLASSIFIED INFORMATION PRIVILEGE IN THE CASE OF UNITED STATES V. _____, USN

Ref: (a) Affidavit of _____, USN dtd 3 Jan CY
(b) Letter of Director, Submarine Warfare Division dtd 3 Jan CY
(c) Military Rule of Evidence 505, Manual for Courts-Martial

1. Based upon my review of references (a) and (b), and pursuant to my authority to classify information originally as TOP SECRET, I find that the information addressed in those references is properly classified and that disclosure would be detrimental to the national security of the United States.

2. In accordance with reference (c), I hereby claim the classified information privilege over the information addressed in references (a) and (b), and authorize the Government Counsel, or any other individual designated by you, to assert that privilege on my behalf at any Article 32, Uniform Code of Military Justice, investigation, court-martial or ancillary proceeding.

Secretary of the Navy

CHAPTER 10

Pretrial Agreements

A. Approval authority under JAGMAN 0137c. No Department of the Navy official is authorized to enter into a pretrial agreement (PTA) in any national security case, as defined in JAGMAN section 0159a, without first obtaining permission to do so from the Secretary of the Navy (see Chapter 7 of this Guide for discussion on designating a case as a national security case). If an offer to plead guilty is received for the accused or the accused's counsel, the convening authority (CA) may enter into pretrial agreement discussions. If the discussions result in terms which are mutually agreeable to the CA and the accused, the CA shall request, by priority message (with information copies to the Chief of Naval Operations or the Commandant of the Marine Corps, as appropriate, and the Judge Advocate General), permission from the Secretary of the Navy to enter into a written pretrial agreement embodying those terms. The message request shall 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 of the accused; and

5. A summary of the factors which warrant entry into a pretrial agreement.

B. Special Procedures. Obtaining approval for a pretrial agreement is similar to obtaining the assertion of the privilege under Mil. R. Evid. 505 - both require personal action by the Secretary of the Navy. Code 17 will coordinate this process. Special provisions in PTAs in national security cases may include provisions for cooperation by the accused in post-trial debriefings and damage assessments, as well as for the use of polygraphs during these sessions. They may also provide for stipulations of fact as to the proper classification of evidence. A well-crafted PTA will ensure the record of trial remains unclassified and can prevent many logistical challenges associated with handling classified information. A sample pretrial agreement, with special provisions for dealing with classified information and national security issues, is provided in Appendix 10-A.

C. Grants of Immunity. In cases involving pretrial agreements, the Government may determine that it is beneficial to grant some form of immunity to the accused. For instance, subsequent to trial, the Government may grant the accused immunity to encourage his or her cooperation in post-trial polygraphs, or to facilitate testimony against a co-accused. If the case has been designated a national security case, any grant of immunity, either to a witness or to the accused, must be coordinated with the Department of Justice. This is in accordance with DOD Directive 5525.7 (Memorandum of Understanding between DOD and DOJ) and JAGMAN § 0138.

Contact Code 17 if the convening authority is contemplating any grants of immunity. Refer to JAGMAN §§ 138-140, and R.C.M. 704 for a detailed discussion of grants of immunity. The Memorandum of Understanding between DOD and DOJ is Appendix 3, Manual for Courts-Martial.

APPENDIX 10-A

SAMPLE PRETRIAL AGREEMENT

NAVY-MARINE CORPS TRIAL JUDICIARY
SOUTHWEST JUDICIAL CIRCUIT
UNITED STATES NAVY

UNITED STATES	)	**GENERAL COURT-MARTIAL**
	)	
v.	)	**MEMORANDUM OF**
	)	**PRETRIAL AGREEMENT**
BRASSO S. BIRD	)	
YN3 USN	)	

PART I: TERMS AND CONDITIONS

I, **YN3 BRASSO S. BIRD, United States Navy**, the accused in a General Court-Martial, do hereby certify:

1. That, for good consideration and after consultation with my defense counsel, I do agree to enter a voluntary plea of GUILTY to the charges and specifications as set forth and approved in this agreement, provided the sentence as approved by the Convening Authority will not exceed the maximum sentence set forth and approved in this agreement;

2. That it is expressly understood that, for the purpose of this agreement, the sentence is considered to be in these parts namely: a period of confinement or other restraint, a punitive discharge, an amount of forfeiture, and any other lawful punishment;

3. That should the Court award a sentence which is less, or of which a part is less, than that set forth and approved in this agreement, then the Convening Authority, according to law, will only approve the lesser sentence;

4. That I am satisfied with my defense counsel in all respects and consider my defense counsel qualified and effective in representing me in this court-martial;

5. That no person or persons whosoever have made any attempt to force or coerce me into making this offer or pleading guilty;

6. That my defense counsel has fully advised me of the meaning and effect of my guilty plea and that I fully understand and comprehend the meaning thereof and all of their attendant effects and consequences;

7. That I understand that I may withdraw my plea of guilty at any time before my plea is actually accepted by the military judge. I understand further that, once my plea of guilty is accepted by the

Court, I may ask permission to withdraw my plea of guilty at any time before sentence is announced, and that the Court may, at its discretion, permit me to do so;

8. That it is expressly understood that this pretrial agreement will become null and void in the event: (1) I fail to plead guilty to the charges and specifications as set forth below; (2) the Court refuses to accept my plea of guilty to the charges and specifications as set forth below; (3) the Court accepts my plea to the charges and specifications as set forth below, but prior to the time sentence is announced, I ask permission to withdraw my plea, and the Court permits me to do so; (4) the Court initially accepts my plea of guilty to the charge and specification as set forth below but, prior to the time the sentence is adjudged, the Court sets aside my plea of guilty and enters a plea of not guilty on my behalf; (5) I fail to plead guilty to the charges and specifications as set forth below at a rehearing, should one occur; or (6) I fail to follow the terms set forth in this agreement;

9. That my defense counsel has advised me that I may be placed on mandatory appellate leave without pay and allowances under the provisions of Article 76a of the Uniform Code of Military Justice (UCMJ), notwithstanding any provision regarding forfeitures or fines in the Maximum Sentence Appendix of this agreement. Furthermore, I agree, that should a dismissal be adjudged, I will submit, within five (5) working days from the date of trial, a written request to be placed on appellate leave, which may be without pay or allowances;

10. That my counsel has fully advised me of, and I understand, the meaning and effect of UCMJ Articles 57 and 58b. I also understand that if the adjudged sentence is subject to the provisions of one or more of these Articles, THIS AGREEMENT WILL HAVE NO EFFECT on the application of those Articles on the adjudged sentence UNLESS THE EFFECT IS SPECIFICALLY AND EXPRESSLY SET FORTH in Part I or II of this agreement;

11. That, as consideration for this agreement, I request to be tried by Military Judge alone. I understand my right to be tried and sentenced by a Court composed of members, and I expressly waive this right. I acknowledge that I have had adequate opportunity to consult with, and have so consulted with, my defense counsel regarding the meaning and ramifications of this term of this pretrial agreement;

12. That my defense counsel has advised me that I may be processed for an administrative separation and that I may therefore be deprived of virtually all veterans' benefits based upon my current period of active service, and that I may therefore expect to encounter substantial prejudice in civilian life in many situations, even if part or all of the sentence, including a dismissal, is suspended or disapproved pursuant to this agreement. I acknowledge that I have had adequate opportunity to consult with, and have so consulted with, my defense counsel regarding the meaning and ramifications of this term of this pretrial agreement;

13. That, as consideration for this agreement, I have entered into a Stipulation of Fact with the Government for each of the charges and specifications to which I am entering a plea of guilty pursuant to this pretrial agreement. The Stipulation of Fact is marked as **Prosecution Exhibit 1 for identification**, and I understand that the Government may offer the Stipulation of Fact as a matter to be considered by the Court during both the findings and sentencing phase of the court-martial. My defense counsel and I have reviewed the Stipulation of Fact and concur that the entire Stipulation is true and is admissible during both the findings and sentencing phase of the court-martial.
Furthermore my defense counsel and I have reviewed the Stipulation of Fact and concur that there

are no objections to the Court's consideration of the entire Stipulation of Fact or any portion thereof when formulating an appropriate sentence in this case. We both concur that the matters therein are appropriate matters for consideration under R.C.M. 1001. I further agree that the Stipulation of Fact may be provided to the Military Judge immediately before trial to assist the Military Judge in crafting an inquiry into the providence of my pleas of guilty and can be relied upon by the military judge as an inseparable and essential part of my responses during the providence inquiry. Failure of any party to this agreement to agree to, enter into, sign, and remain a party of the Stipulation of Fact, will make this agreement null and void, and both I and the Convening Authority would be relieved of all obligations and responsibilities which either of us would have been otherwise required to meet by the terms of this pretrial agreement. I acknowledge that 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;

14. That, as consideration for this agreement, I will not request or otherwise require the Government to provide for the personal appearance of witnesses at Government expense to testify during the sentencing phase of the Court-Martial. I acknowledge that 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;

15. That it is expressly understood that in the event I should commit any misconduct in violation of the UCMJ (as determined unilaterally, without a hearing, by the Convening Authority), after the signing of the pretrial agreement, but before the date sentence is announced, the Convening Authority may withdraw from this pretrial agreement by giving notice to the accused prior to the entry of pleas. Should the Convening Authority do so, I understand that the pretrial agreement would thereby become null and void, and both I and the Convening Authority would be relieved of all obligations and responsibilities which either of us would have been otherwise required to meet by the terms of this pretrial agreement;

16. That, as consideration for this agreement, I will not object to the docketing of my case on the first available date on the court docket requested by trial counsel as approved by the military judge, subject to the availability of my defense counsel, for purpose of taking my pleas and entering findings thereon per this pretrial agreement. I acknowledge I have had 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;

17. That, as consideration for this agreement, I agree to waive all motions which do not deprive me of the right to due process or the right to challenge the jurisdiction of the Court-Martial. However, I do not waive any motions that are otherwise non-waivable per R.C.M. 705(c)(1)(B). These motions may be made at any time. My defense counsel and I are not aware of any matters or motions which are non-waivable per R.C.M. 705(c)(1)(B) and do not presently intend to raise any such matters or motions;

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

a. I shall submit to and cooperate in all interviews and polygraph examinations requested by the investigators specified by the Convening Authority, which interviews and examinations shall concern the disclosure of the information referenced in the charge sheet to any person or

foreign government, the encryption/decryption of computer files seized by law enforcement authorities in conjunction with this case, the circumstances surrounding the allegations contained within the charge sheet, and may also include questions typically asked in a polygraph examination for ascertaining if a person may continue to hold a Top Secret security clearance;

b. I shall 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 interviews and polygraph examinations, at times and places 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;

c. If the results of any polygraph examination reflect that I have provided deceptive or "no opinion" responses to any questions, I will cooperate with investigators to resolve any issues related to the deceptive or "no opinion" responses by fully cooperating in additional interviews and polygraph examinations. If, in the opinion of the polygraph examiner, I continue to provide deceptive or "no opinion" responses to any questions, that opinion and the responses therefore shall be conveyed to the Convening Authority. The Convening Authority, 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 examiner's opinion that I provided deceptive or "no opinion" responses to any questions and the basis of that opinion, may elect to declare this pretrial agreement null and void;

d. Before declaring this pretrial agreement null and void and before electing not to be bound by the terms of this pretrial agreement, the Convening Authority will provide me with a hearing and an opportunity to be heard within the true meaning of R.C.M. 1109, MCM;

e. My defense counsel shall be provided notice and a reasonable opportunity to be present during each and every interview and polygraph examination, but shall not be in the examination room during the polygraph examinations referred to in subparagraphs "a.", "b.", and "c." of paragraph 18. My defense counsel shall be provided the opportunity to review the questions that will be posed to me during the interviews and polygraph examinations prior to each interview and examination;

f. Any communication made by me during any interview and polygraph examination conducted pursuant to this paragraph (paragraph 18) of this pretrial agreement are statements made in the course of plea discussions under Military Rule of Evidence 410. As such these statements are not admissible at court-martial except as provided for in Military Rule of Evidence 410;

(1) However, if it is discovered that I knowingly possessed classified information above the "Secret" classification or that I knowingly caused to be transmitted or disclosed classified information to any person whom I knew to be a non-U.S. citizen or foreign government, then the Convening Authority may declare this agreement null and void;

(2) Should this agreement become null and void for any reason, paragraph 18, subparagraph "f." clauses 1 and 2 will remain in full force and effect.

19. 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:

a. I shall submit to and cooperate in all requested interviews, interrogations, and polygraph examinations by investigators specified by the Convening Authority concerning all of the charges and specifications referred to trial, as well as any additional matters relating to the compromise of classified material. Such cooperation shall extend to disclosing my knowledge of the actual event, or potential, compromise of classified material or information by any person or entity whatsoever;

b. I will answer all questions orally and, where requested, in writing, fully and completely, under oath, to the best of my knowledge and belief. I will submit to as many interviews, interrogations 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 all matters. This period of cooperation will extend for a period of 24 months from the date the sentence is imposed;

c. It is further provided that at the conclusion of the interviews and interrogations, and at the direction of the Convening Authority, I shall be examined by one or more Government certified polygraph examiners. If the results of any polygraph examinations reflect that I have provided deceptive or "no opinion" responses to any questions, I will cooperate with investigators to resolve any issues related to the deceptive or "no opinion" responses by fully cooperating in additional interviews, interrogations and polygraph examinations. If, in the opinion of the polygraph examiner, I continue to provide "no opinion" responses to polygraph examinations or deceptive answers regarding all or any part of the interviews, interrogations or examinations, that opinion and the reasons therefore shall be conveyed to the Convening Authority;

d. That, as further consideration for this agreement, I agree that after trial by court-martial, 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 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 1.3 and 1.4(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;

e. If information is given to the Convening Authority that I have violated the provision of paragraph 19, subparagraphs "a.", "b.", "c." or "d." of this agreement after trial but prior to his having taken action on the record of trial, the Convening Authority may elect not to be bound by

the sentence-limiting provision of this pretrial agreement. However, before electing not to be bound by the sentence limitations, the Convening Authority will provide me with a hearing and opportunity to be heard within the true meaning of R.C.M. 1109, MCM. If during this hearing 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 to questions asked during interviews, interrogations or examinations and the basis for those opinions, then I will be entitled to present evidence based on a polygraph examination from an independent source. The Convening Authority agrees to pay for one (1) alternative polygraph examination from an independent source if I elect to have such an examination. The independent source polygrapher must hold, or be able to gain, the necessary security clearance in accordance with current regulations;

f. If information is given to the Convening Authority that I have violated the provision of paragraph 19, subparagraphs "a.", "b.", "c." or "d." of this agreement after he has taken action on the record of trial, the Convening Authority may use this information in determining if I have violated the provision of paragraph 19, subparagraphs "a.", "b.", "c." or "d." of this agreement. Prior to making such a determination, the Convening Authority will provide me with a hearing and opportunity to be heard within the true meaning of R.C.M. 1109, MCM. If during this hearing the Convening Authority wants to consider the results of polygraph examinations, including a polygraph examiner's opinion that I proved "no response" or deceptive responses to questions asked during interviews, interrogations or examinations and the basis for those opinions, then I will be entitled to present evidence based on a polygraph examination from an independent source. The independent source polygrapher must hold or be able to gain the necessary security clearance, in accordance with current regulations, to conduct such an examination. If I elect to use an independent polygrapher, I agree to pay for such polygraph services. I agree that if, after conducting the above hearing in accordance with the provisions of R.C.M. 1109, MCM, the Convening Authority determines that I have violated a provision of either paragraph 19, subparagraphs "a.", "b.", "c." or "d." the Convening Authority may vacate any portion of the sentence which was suspended pursuant to this agreement or otherwise;

g. The Convening Authority shall provide me with a grant of testimonial immunity for any information obtained by Government agents from me pursuant to paragraph 19, subparagraphs "a.", "b.", and "c.". Furthermore, my defense counsel shall be provided notice and a reasonable opportunity to be present during each and every period of interview or interrogation. The Convening Authority will pay for the presence of my detailed defense counsel at any of these interview or interrogations for the first two months after sentence is announced. After two months, counsel may be present, but at no expense to the Convening Authority. This presence shall include the opportunity to be present at the site, but counsel shall not be in the examination room during the examinations referred to in paragraph 19, subparagraphs "a.", "b.", and "c.".

20. That, as consideration for this agreement, I hereby certify that I have conditionally waived my Article 32 pre-trial investigation to which I am currently entitled, relating to the allegations set forth in the charges and specifications which are the subject of this agreement. I fully understand my absolute right to have an Article 32 investigative hearing and have conditionally waived that right. Once I have been arraigned pursuant to this pretrial agreement, all conditions precedent to the enforcement of this Article 32 waiver will be satisfied. Thereafter, this Article 32 waiver will be binding and enforceable and will not be affected, in any way, should the

pretrial agreement become null and void for any reason. I acknowledge that 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. Should this agreement become null and void, for any of the reasons set forth above, this paragraph will remain in full force and effect.

21. That, as consideration for this agreement, I agree to the admissibility, for any and all purposes, of any and all classification reviews and related affidavits of compromised classified information and damage assessments of the compromise of 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. I and my defense counsel 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;

22. That, as consideration for this agreement, 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 1.3 and 1.4(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;

23. That I, as consideration for this agreement, request and stipulate that any time from the signing of this agreement by both parties until such time as either (1) the pretrial agreement becomes null and void for any reason, or (2) I enter guilty pleas as set forth below, is excludable delay for purpose of R.C.M. 707, UCMJ. Should this agreement become null and void, for any of the reasons set forth above, this paragraph will remain in full force and effect.

This agreement and its appendices constitutes all the conditions and understandings of both the Government and the accused regarding the plea in this case.

I. PLEAS OF THE ACCUSED

CHARGE	PLEA
To Charge I: Violation of UCMJ, Art. 80:	NOT GUILTY
Specification:	NOT GUILTY
To Charge II: Violation of UCMJ, Art. 92:	GUILTY
Specification:	GUILTY

Charge III: Violation of UCMJ, Art. 134:	GUILTY
Specification 1:	GUILTY
Specification 2:	NOT GUILTY

II. MAXIMUM SENTENCE TO BE APPROVED BY THE CONVENING AUTHORITY

See Maximum Sentence Appendix (Part II) to this Memorandum of Pretrial Agreement.

Signature of the Parties:

_____ _____
YN3 Brasso S. Bird, USN Date
Accused

_____ _____
LT H. R. Rabb, JAGC, USN Date
Detailed Defense Counsel

The foregoing agreement is approved.

_____ _____
Commander, Date
Naval Surface Force, U.S. Pacific Fleet
General Court-Martial Convening Authority

NAVY-MARINE CORPS TRIAL JUDICIARY
SOUTHWEST JUDICIAL CIRCUIT
UNITED STATES NAVY

UNITED STATES	)	**GENERAL COURT-MARTIAL**
	)	
v.	)	**MEMORANDUM OF**
	)	**PRETRIAL AGREEMENT**
BRASSO S. BIRD	)	
YN3 USN	)	

PART II: MAXIMUM SENTENCE APPENDIX

MAXIMUM SENTENCE TO BE APPROVED BY THE CONVENING AUTHORITY:

1. Punitive Discharge: May be approved as adjudged.

2. Confinement or restraint: If a dismissal is awarded, all confinement will be suspended, unless sooner vacated, for a period of twenty-four (24) months from the date the sentence is announced, at which time, unless sooner vacated, it will be remitted without further action; if a dismissal is not awarded, all confinement may be approved, however, all confinement in excess of twelve (12) months will be suspended, unless sooner vacated, for a period of twenty-four (24) months from the date the sentence is announced, at which time, unless sooner vacated, it will be remitted without further action.

3. Forfeitures and/or Fines:

a. Adjudged fines or forfeitures: If a punitive discharge is awarded, forfeitures and/or fines may be approved as adjudged. If a dismissal is not awarded and adjudged confinement exceeds six months and prior to the sentence being announced, I execute an allotment to Ms. Wailua Bird, my lawful dependent, all adjudged fines and forfeitures will be suspended, for a period of twelve (12) months from the date of the Convening Authority's action, at which time, unless sooner vacated, the suspended fines and forfeitures will be remitted without further action.

This agreement constitutes a request by the accused for and approval by the Convening Authority of deferment of that portion of any adjudged forfeitures which is to be suspended pursuant to the terms of this agreement. The period of deferment will run from the date adjudged fines and forfeitures would otherwise become effective, until the date the Convening Authority acts on the sentence.

b. Automatic forfeitures: If a dismissal is not awarded, automatic forfeitures, if applicable, will be deferred, provided that the accused executes and maintains an allotment in favor of his wife, Ms. Wailua S. Bird, prior to the announcement of sentence. This agreement constitutes a request by the accused for and approval by the convening authority of deferment of automatic forfeitures pursuant to Article 58b, UCMJ. The period of deferment will run from the date automatic forfeitures would otherwise become effective under Article 58b until the date the Convening Authority acts on the sentence.

This agreement constitutes a request by the accused for and approval by the convening authority of waiver of all automatic forfeitures. The period of waiver will commence on the date automatic forfeitures become payable and will run for six (6) months. The waived forfeitures shall be paid to the wife of the accused, Ruthellen Rose Larson, who is a lawful dependent of the accused.

4. Any other lawful punishment: May be approved as adjudged.

5. It is expressly understood that the commission of any offense cognizable under the UCMJ from the date sentence is adjudged to the date of the Convening Authority's action will be grounds for vacation of the suspension in accordance with R.C.M. 1109.

6. This agreement does not effect the provisions of UCMJ Article 57.

7. This agreement constitutes a request by the accused for, and approval by the convening authority of, deferment of the portion of any confinement to be suspended pursuant to the terms of this agreement. The period of deferment will run from the date the accused is released from confinement pursuant to this agreement, or the date that the sentence is announced if all confinement is to be suspended pursuant to this agreement, until the date the convening authority acts on the sentence.

8. As further consideration for this agreement, I agree that if I should be ordered to show cause at a Board of Inquiry which includes as a basis for processing, in part or in whole, the misconduct to which I have agreed to plead guilty per this pretrial agreement, I agree to WAIVE my right to a hearing before a Board of Inquiry, doing so with a full understanding of the consequences of waiving such a board, as explained to me by my defense counsel. I acknowledge that 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;

Signature of the Parties:

_____ _____
YN3 Brasso S. Bird USN Date
Accused

_____ _____
LT H. R. Rabb, JAGC, USN Date
Detailed Defense Counsel

The foregoing agreement is approved.

_____ _____
Commander, Date
Naval Surface Force, U.S. Pacific Fleet
General Court-Martial Convening Authority

CHAPTER 11

The Sentencing Case

A. Introduction. The Government's case in aggravation and the defense's case in extenuation and mitigation are both limited by the same concept: rarely, if ever, will the true extent and nature of the actual harm to the national security caused by the accused's misconduct be known. The victims in such cases are easy to identify - all U.S. citizens. The traditional concept of victim impact, however, is difficult to apply because of the difficulty in quantifying or describing the harm. Further, any such evidence is likely to be classified, and is subject to Mil. R. Evid. 505. Under Mil. R. Evid. 505, the standard for admissibility of classified information in sentencing is stricter than for the case on the merits. Mil. R. Evid. 505(i)(4)(B) provides that in presentencing proceedings, classified evidence, if found to be relevant and material, is only admissible if no unclassified version of that evidence is available.

B. Case In Aggravation. In the sentencing stage, the trial counsel can typically argue a theory of general deterrence. The nature of a national security case -- the deliberate divulging of national secrets -- is among the most serious to the Government and arouses intense passion. The compromise of classified material, at the very least, reveals highly sensitive sources and methods to unauthorized persons. At the worst, it places the lives of Navy personnel or others directly in jeopardy. In either case, the special trust that the Government has placed in the servicemember has been breached. The protection of classified material is a personal responsibility. Our nation's security is dependent upon the special confidence placed in those who have been granted access to classified information.

In developing a case in aggravation, the trial counsel should be prepared to present witnesses who can testify as to the degree of damage to national security caused by the offenses. In many cases, very senior officers and/or officials from the intelligence agency are the best individuals to testify as sentencing witnesses. If they are unavailable to provide live testimony, affidavits can be substituted. Code 17 can assist in identifying and obtaining appropriate witnesses and affidavits.

In addition, the trial counsel can present the non-disclosure agreements signed by the servicemember when he or she was first granted access to classified material. In these agreements the servicemember recognizes that a special trust is being place in him or her, and acknowledges that severe penalties will be incurred if that trust is breached. The presentation of these agreements at sentencing is an effective way to show that the servicemember was put on notice as to the confidence that was being placed in him or her, and the harm that could result from the compromise of classified material. The security manager or security office for the classified programs into which the servicemember has been cleared maintains these non-disclosure agreements.

C. Case in Extenuation and Mitigation. The defense counsel can typically argue that a lesser sentence should be adjudged based upon the servicemember's difficult personal circumstances. The service member's dire financial situation, youth and inexperience, or his or her lack of familiarity with classified material or the Intelligence Community could be examples of such circumstances.

In addition, the defense may be able to present evidence to suggest that the compromise of the classified material did not pose as severe a harm to the national security as the prosecution argues. It is also possible that authors or public policy analysts may testify that the classified information that was compromised is available to the public in open-source publications. In this circumstance, two things must be remembered: 1) the classification level of the material is not at issue because the classification review conducted early on has already settled that question, and 2) the publication of classified material in an open-source venue does not make the material unclassified.

D. Remitting and Suspending Sentences. Per JAGMAN 0159, only the Secretary of the Navy may remit or suspend any part of amount of the approved sentence in cases involving national security. All other officials in the Department of the Navy are prohibited from taking such action.

CHAPTER 12

Special Procedures for Post-Trial documents

A. Classified Records of Trial. When a record of trial contains classified information, the trial counsel must ensure the record is properly classified, marked, and stored. This means that the record as a whole is assigned the proper security classification, and each page of the record that contains classified information is marked properly. Too often, these important post-trial responsibilities do not receive adequate attention. The trial counsel must work closely with the Court Security Officer (CSO) to ensure security procedures are followed. Therefore, it is important that trial counsel not allow the CSO to be detached too soon from his or her responsibilities. Post-trial classification review and portion marking of the record of trial require close attention and strict adherence to procedures.

If the military judge orders information to be withheld from the accused pursuant to Mil. R. Evid. 505 and the accused objected to such action and was convicted, the relevant documents as well as the Government's motion to the withhold the information and any supporting materials must be attached to the record as a sealed exhibit. Mil. R. Evid. 505(g)(4).

B. Special Provisions. JAGMAN 0150c describes procedures for classified records of trial. If the record contains Sensitive Compartmented Information (SCI), then it is essential that the trial counsel/CSO ensure that the handling and storage procedures comply with SCI requirements, including the requirement that it be stored in an SCI Facility (SCIF) and transported by a special courier. If a record of trial includes SCI material, it is essential to contact Code 17 before forwarding it to the Navy-Marine Corps Appellate Review Activity to coordinate the use of the SCIF at Naval Criminal Investigative Service Headquarters for storage of the record. Do not excuse the CSO until all of these procedures are accomplished.

TAB A

STAFF JUDGE ADVOCATE/TRIAL COUNSEL CHECKLIST
FOR
NATIONAL SECURITY CASES

A. Notification of Investigation

____1. Identify cognizant NSCDA; notify SJA for NSCDA.

____2. Advise OJAG Code 17 of the case status (DSN 325-5464/5; (202) 685-5464/5; FAX DSN 325-5467; (202) 685-5467)

____3. Identify prospective TC at earliest stage of investigation.

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. Comm: 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.

____5. Remind investigators of speedy trial implications of apprehension when other investigative techniques and avenues remain to be explored.

____6. Insist upon joint determinations of what information, witnesses, or evidence will be made available for use at trial.

____7. Adhere strictly to the "third agency rule" (E.O. 12958, Part 4.2(h)) when dealing with non-DOD intelligence agencies (must have permission of originating agency).

____8. Request assistance from Code 17 to resolve any problems

____9. If the accused has agreed to speak to investigators, verify his or her understanding of the classification level of the information.

____10. Determine what classified information is likely to be involved.

____11. 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?

____12. Obtain a decision from the NSCDA about the proper disposition of the case.

____13. Determine if sensitive compartmented information is involved.

____14. Contact Program Manager in special access programs to determine special access requirements.

____15. Consider speedy trial implications and the existence of possible exclusions under RCM 707 or case law for the time required to complete classification reviews.

____16. 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.

____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 Code 17.

E. Security Clearances

____1. Confirm 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

____2. Obtain appointment of an investigation security officer in writing 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.

____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 Code 17, request CNO (OP-09N) issue a Limited Access Authorization for civilian defense counsel, if required.

____2. If request is denied, coordinate with Code 17 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 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 may also be requested to do this in 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.

____6. Make sure 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).

____7. Do not allow the accused or defense counsel to disclose classified material until notice occurs and judicial determination is made regarding such disclosure under M.R.E. 505.

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

J. Immunity

____1. Draft grants of immunity to apply only to court-martial.

____2. Alternatively, obtain permission from DOJ/DODGC 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

K. Protective Orders/Courtroom Security

____1. Include requirements for handling and disclosure of classified information in a protective order.

____2. Demonstrate a full understanding and an aggressive employment of M.R.E. 505 to counsel and operational staffs of intelligence agencies with which you work to ensure 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

____4. Where evidence is collected under a warrant issued pursuant to the Foreign Intelligence Surveillance Act, 50 U.S.C. 1801-1811, immediately contact 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 not to disclose 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.

____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 an appeal is not to occur, promptly so 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 Code 17 on significance of the accused's actions.

____3. Obtain witnesses/affidavits via 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.

____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. If the record of trial contains Sensitive Compartmented Information, follow procedures set forth in the Memorandum of Agreement between OJAG and NCIS.

____6. 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

TAB B

Military Judge Overview

A. JAGMAN Provisions.

1. National Security Case Disposition Authority (JAGMAN 0126). These listed commands decide if a case involving classified information is a national security case. In the Navy, the lowest level authority for this decision is the type commanders. In the Marine Corps, it is the Commanding General, Marine Corps Bases, Japan, Camp Lejeune, and Camp Pendleton. After that determination, the case can be sent to any convening authority for resolution, including court-martial, if the designated convening authority so chooses.

2. Definition of National Security Case (JAGMAN 0159a). Also limits subsequent clemency actions after the convening authority takes action on the sentence. A National Security Case is a case that involves to any serious degree, the compromise of a military or defense advantage over any foreign nation; involves an allegation of willful compromise of classified information; or affects our military or defense capability to successfully resist hostile or destructive action, overt or covert; and, acts of terrorism. Such cases include the attempt or conspiracy to commit such offenses, as well as aiding and abetting in the commission of the offenses.

3. Pretrial agreements (JAGMAN 0137c). In national security cases, the Secretary of the Navy must personally approve any pretrial agreement the convening authority may want to enter.

4. Grants of immunity (JAGMAN 0138d). All grants of immunity in national security cases must be approved by DOJ.

5. Spectators at proceedings (JAGMAN 0143). In cases involving classified information (including Article 32 investigations since 1996), application of this provision is subject to Mil. R. Evid. 505 and case law. *United States v. Hershey*, 20 M.J. 433, 435 (CMA 1985); *United States v. Grunden*, 2 M.J. 116 (CMA 1977); *MacDonald v. Hodson*, 19 U.S.C.M.A. 582, 42 C.M.R. 184 (1970); *United States v. Brown*, 7 U.S.C.M.A. 251, 256, 22 C.M.R. 41 (1956). *Press-Enterprise Co. v. Superior Court of California, Riverside County*, 464 U.S. 501, 509, 104 S. Ct. 819, 78 L. Ed. 2d 629 (1984); *see also Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 581, 100 S. Ct. 2814, 2829-30, 65 L. Ed. 2d 973 (1980)("Absent an overriding interest articulated in findings, the trial of a criminal case must be open to the public.").

B. Mil. R. Evid. 505. Classified information rules involve disclosure (discovery), disclosure (use at trial), and closure of proceedings.

1. Privilege from disclosure. Is claimed or asserted by SECNAV as head of the agency concerned for Navy or Marine Corps courts-martial, but not limited to SECNAV. Other heads of executive or military departments or government agencies may be concerned and involved as well.

2. Classification review. Necessary to ensure level of classified information involved in the case. Also necessary to obtain Secretary of the Navy exercise of Mil. R. Evid 505 privilege. This is NOT a declassification review under E.O. 12958, Sec 3.6. A declassification review is NOT conducted for classified information which is the subject of litigation. E.O. 12958, Sec. 3.6(3). *See also*, SECNAVINST 5510.36.

3. Protective Order. When classified information is disclosed (discovery) to the accused, all defense counsel and the accused should be required to sign a protective order to guard against compromise of the information disclosed. If not requested by Government counsel, consider it *sua sponte*. Just because counsel had classified information disclosed (discovery) to them, doesn't mean it can be *disclosed* (used) at court-martial. TC should have copies of sample protective orders.

4. Discovery twist. The military rules and culture favoring liberal discovery do not apply to classified information. Rule for Courts-Martial 701 (Discovery-information "material to preparation") defers to Mil. R. Evid. 505 (No 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 and the judge must so find in writing). Do not apply a Freedom of Information Act analysis that places a heavy burden on the Government to justify non-disclosure. Instead, the case law applying the Classified Information Procedures Act (CIPA) should be reviewed. *United States v. Yunis*, 76 U.S. App. D.C. 1; 867 F.2d 617 (D.C. Cir. 1989) (interpreting the Classified Information Procedures Act (CIPA) used in civilian court. 18 U.S.C. App.).

5. Notice by accused. The defense must notify trial counsel in writing, with a copy to the judge, of any intent to disclose (use) classified information prior to arraignment or as otherwise scheduled by the judge.

6. Invocation of the privilege.

7. In-camera proceedings. Preliminary session closed to the public used to determine whether information may be disclosed at the court-martial proceeding. By comparison with *United States v. Grunden*, 2 M.J. 116 (CMA 1977), you see that it also serves to lay the foundation for closing portions of the court-martial on the merits to the public.

a. Motion by the Government for *ex parte* examination by the judge. Government provides an affidavit demonstrating harm by any disclosure of the privileged information and provides the classified information. (Note: Mil. R. Evid. 104 provides that the rules of evidence don't apply to determination of the existence of a privilege, so no testimony is needed, documents suffice).

b. If judge finds disclosure could reasonably be expected to cause harm, judge orders *in camera* proceeding and Government provides the accused with some notice of the information at issue.

c. Following briefing and argument (notice again, there is no mention of

witnesses), unless the judge states in writing that the information is relevant and necessary to an element of the offense or a legally cognizable defense and is otherwise admissible in evidence, the information may not be disclosed or otherwise elicited at court-martial.

8. Alternatives to disclosure: Redaction or unclassified summaries. Judge's ruling that the evidence must be disclosed can limit the form of the evidence by allowing alternatives.

9. Sanctions when Government resists disclosure include:

a. Strike or preclude testimony of witness;

b. Declare a mistrial;

c. Find against the Government on any issue to which evidence is relevant and material to the defense;

d. Dismiss charges with or without prejudice; or

e. Dismiss the charges or specifications to which the information relates.

f. **NOTE: The judge does not have the authority to order production of classified information.**

C. Closed sessions. Used when necessary to prevent harm from the disclosure (use) of classified material. Before a trial judge can order the exclusion of the public (really, anyone without proper clearance and a need-to-know) on the basis of national security, the judge must be satisfied from all the evidence and circumstances that there is a reasonable danger that presentation of the classified information before the public will expose military matters which, in the interest of national security, should not be divulged. Additionally, the judge must limit the closed sessions to only those closed sessions necessary. Finally, the judge should state the rulings on the record, i.e., disclosure would harm the national defense and describe what will be closed. *United States v. Hershey*, 20 M.J. 433 (CMA 1985); *United States v. Terry,* 52 M.J. 574 (N.M.Ct.Crim.App. 1999). Although Mil. R. Evid. 505 goes a long way in fulfilling these requirements, *United States v. Grunden*, 2 M.J. 116 (CMA 1977) is a must read. Also, it bears emphasis that the judge is not determining if the classified material is accurately classified or should be classified, only that it was classified through the proper procedure. The judge does not review the actual decision to classify the material. Interestingly, *Grunden* also states that:

> As a general rule, the public shall be permitted to attend open sessions of courts-martial. Unless otherwise limited by directives of the Secretary of a Department, the convening authority, the military judge, or the president of a special court-martial without a military judge may, for security or other good reasons, direct that the public or certain portions thereof be excluded from a trial. However, all spectators may be excluded from an entire trial, over the accused's objection, only to prevent the disclosure of classified information. The authority to exclude should be cautiously exercised, and the right of the accused to a trial completely

open to the public must be weighed against the public policy considerations justifying exclusion.

Grunden, 2 M.J. at 121**.** Query: Does this allow the convening authority to dictate closed sessions?

D. National Security Case. JAGMAN states, or will state, that a National Security Case is a case that involves to any serious degree, the compromise of a military or defense advantage over any foreign nation; involves an allegation of willful compromise of classified information; or affects our military or defense capability to successfully resist hostile or destructive action, overt or covert; and, acts of terrorism. Such cases include the attempt or conspiracy to commit such offenses, as well as aiding and abetting in the commission of the offenses. Therefore, national security cases can involve, but are not limited to, offenses within the purview of:

1. Article 81, UCMJ (conspiracy);

2. Article 92, UCMJ (failure to obey order or regulation), when the conduct violates a general order or regulation relating to willful compromise (possible or confirmed) or willful disclosure of national defense information, including, but not limited to, violations of Article 1121(2), U.S. Navy Regulations, 1990, (disclosure and publication of information) and SECNAVINST 5510.36 series (information security program regulation);

3. Article 104, UCMJ (aiding the enemy), Article 106, UCMJ (spies), or Article 106a, UCMJ (espionage);

4. Article 107, UCMJ (false official statements), where the false official statement concerns the actual or prospective commission of, or knowledge of any person's actual or prospective commission of a crime against national security;

5. Article 131, UCMJ (perjury), where the perjury concerns the actual or prospective commission of, or knowledge of any person's actual or prospective commission of a crime against national security or concerns an attempt to commit such an act;

6. Article 134, UCMJ, when the conduct charged is:

a. A violation of a United States Code section specified in this section, including:

(1) section 1001, title 18, United States Code (false statements), when the falsification or concealment concerns the actual or prospective commission of, or knowledge of any person's actual or prospective commission of, a crime against national security or concerns an attempt to commit such an act;

(2) sections 792 (harboring or concealing persons), 793 (gathering, transmitting, or losing defense information), section 794 (gathering or delivering defense information to aid foreign government), or 798 (disclosure of classified information), title 18, United States Code;

(3) chapter 105 (sabotage), title 18, United States Code;

(4) chapter 113B (terrorism), title 18, United States Code;

(5) 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), or 2390 (enlistment to serve against the United States), title 18, United States Code;

(6) 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), or 2277 (disclosure of restricted data), title 42, United States Code, insofar as the offense is committed with intent to injure the United States or with the intent to secure an advantage to a foreign nation;

(7) section 783 (conspiracy and communication or receipt of classified information), title 50, United States Code; and

(8) an earlier statute or article on which a punitive Article of the UCMJ or any other United States Code section specified in this section is based.

b. Solicitation to commit a crime against the national security;

c. False swearing concerning the actual or prospective commission of, or knowledge of any person's actual or prospective commission of a crime against national security or concerning an attempt to commit such an act; and

d. Subornation of perjury committed in connection with the false testimony of any person concerning the actual or prospective commission of a crime against national security or concerning an attempt to commit such an act.

E. Incident not designated National Security Case. A case may involve matters and/or materials relating to the security of the United States, yet need not be designated a National Security Case if, in the opinion of the officer exercising cognizance over the matter under subparagraph e, below, the offenses involved do not rise to a level constituting a serious degree of compromise of the military or defense advantage over a foreign nation, do not constitute willful compromise of classified information, or do not effect military or defense capability to resist hostile or destructive action successfully, either covert or overt in nature.

F. Impact of designation. Whether a case that involves classified information has been designated as a National Security Case is of little or no consequence to the judge. The legality of the JAGMAN provisions has been litigated and established. *United States v. Allen*, 31 M.J. 572 (NMCMR 1990). When a case is designated a National Security Case, the Secretary of the Navy must approve any pretrial agreement and there are special rules for grants of immunity to witnesses. The Secretary doesn't enter into the pretrial agreement. If the convening authority chooses to decline a pretrial agreement offer, the Secretary does not review that decision.

G. Trial Procedure.

1. DO NOT PROCEED unless you have at least one court-martial security officer (CSO). You should arrange to have alternates, these cases can last several weeks. The CSO is not the bailiff. Use R.C.M. 802 liberally, but carefully. Use the R.C.M. 802 to determine the level of pretrial preparation the parties have done regarding the classified information. Two-edged sword - these cases are not common, so counsel won't be experienced. They may need guidance in overall classified information handling and in trial and discovery procedures.

2. Ensure the CSO and alternate CSO are very knowledgeable in the particular classified material at issue, especially Sensitive Compartmented Information cases.

3. At an Art. 39(a) session, instruct the CSO and alternates on their responsibilities and the procedures to use. During closed court sessions, the CSO should approve of anyone in the courtroom. Have the CSO prepare a matrix of all parties with their security clearances. Judge and counsel should have copies. The CSO must verify the clearances through the person's security officer.

4. Make sure all involved personnel have proper clearances:

a. Military Judge.

b. Defense counsel and defense paralegal. This may require extra time if civilian counsel or paralegals or expert witnesses/assistants are without clearance. Failure by the defense to cooperate in obtaining a clearance is NOT a showstopper. In *United States v. Jolliff*, a case tried under CIPA in which 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 failure of counsel to cooperate in obtaining a security clearance for himself could lead to disqualification and dismissal from the case by the trial judge. S*ee 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).

c. Trial counsel and paralegal.

d. CSO and alternates.

e. Court reporter and alternates.

f. Bailiff and alternates.

g. Physical security personnel, if needed.

h. Equity holder observers.

5. In public sessions, position the CSO in the back of the courtroom and arrange some unobtrusive signal to you when the CSO thinks the case is moving into classified information.

6. The CSO is not a witness expert to aid any of the parties. The CSO ensures proper handling and protection of the classified information, in an effort to keep you and the counsel from sharing jail cells adjoining one another.

7. If defense counsel think they need an expert, they can request one from the convening authority under case law. *United States v. Garries*, 22 M.J. 288 (CMA 1986). A "tutor" for education in classified information handling can usually be arranged without a need for confidentiality.

8. Don't allow note taking by any observers during closed sessions. Equity holders frequently send observers, and the CSO will have to monitor their access to closed sessions.

9. Have the members "read in" by the CSO, on the record, and have the appropriate documents attached as appellate exhibits.

10. Give special instructions to the members on the "reading in" process, classified and unclassified sessions and the procedures for handling their notes.

11. Notes. Ensure the CSO provides the judge, counsel, and the members with folders that can be sealed for storage of notes. The CSO should maintain custody of these notes except when they are being used for preparation or during appropriate sessions of court.

12. Maximize open sessions. Even in highly classified cases, structure the proceedings to maximize open sessions. [Note. The judge's initial task is to determine whether the perceived need urged as grounds for the exclusion of the public is of sufficient magnitude so as to outweigh "the danger of a miscarriage of justice which may attend judicial proceedings carried out in even partial secrecy." *Stamicarbon, N.V. V. American Cyanamid Co., 506 F.2d 532, 539 (2d Cir. 1974).* This may be best achieved by conducting a preliminary hearing which is closed to the public at which time the government must demonstrate that it has met the heavy burden of justifying the imposition of restraints on this constitutional right. The prosecution to meet this heavy burden must demonstrate the classified nature, if any, of the materials in question. It must then delineate those portions of its case that will involve these materials. Consider the following quote from *Grunden*:

> Before a trial judge can order the exclusion of the public on this basis, he must be satisfied from all the evidence and circumstances that there is a reasonable danger that presentation of these materials before the public will expose military matters which in the interest of national security should not be divulged. *United States v. Reynolds, 345 U.S. 1, 73 S. Ct. 528, 97 L. Ed. 727 (1953).* The method used by the prosecution to satisfy this burden, as recognized in *United States v. Reynolds, supra,* will vary depending upon the nature of the materials in question and the information offered. It is important to realize that this initial review by the trial judge is not for the purpose of conducting a de novo review of the propriety of a given classification decision. All that must be determined is that the proper authorities in accordance with the appropriate regulations have classified the material in question. *Brockway v. Department of the Air force, 518 F.2d 1184 (8th Cir. 1975).* The ultimate questions of whether these materials "relat[ed] to

> the national defense" and could be used to the injury of the United States or the advantage of a foreign country must remain for resolution by the jury. *18 U.S.C. § 793*(d). The sole purpose of this review is to protect an accused's right to a public trial by preventing circumvention of that right by the mere utterance of a conclusion or blanket acceptance of the government's position without a demonstration of a compelling need. *United States v. Nixon, 418 U.S. 683, 94 S. Ct. 3090, 41 L. Ed. 2d 1039 (1974)*.
>
> He must further decide the scope of the exclusion of the public. The prosecution must delineate which witnesses will testify on classified matters, and what portion of each witness' testimony will actually be devoted to this area. Clearly, unlike the instant case, any witness whose testimony does not contain references to classified material will testify in open court.
>
> In excising the public from the trial, the trial judge employed an ax in place of the constitutionally required scalpel.

Grunden, 2 M.J. at 122-23 (emphasis added).

It's not impossible and you don't have to be cartoon crazy. The *Grunden* court continued:

> The Court recognizes that not every situation is easily "pigeon-holed" into testimony which is devoted to classified material and that which is not; as noted earlier in this opinion, we feel that trial judges should and must be capable of exercising sound discretion in their rulings. Clearly, therefore, the trial judge need not participate in so rigid a procedure as to turn his courtroom into a parade; continuity of testimony and the fact that a given witness' testimony deals virtually exclusively with classified material are certainly factors which could lead to the exclusion of the public from all of a given witness' testimony regardless of the fact that a portion was not concerned with such matters. The procedure we set forth is to protect an individual's rights under the Sixth Amendment and to prevent those rights from being ignored on the basis of unthinking acceptance of government claims of need without the appropriate demonstration of that need.

Grunden, 2 M.J. at 124.

Additionally, the Navy-Marine Corps Court of Military Review has stated:

> Appellate defense counsel, citing *United States v. Grunden, 2 M.J. 116 (C.M.A. 1977)* and *United States v. Hershey, 20 M.J. 433 (C.M.A. 1985),* contend that the military judge relinquished and delegated his responsibilities to the prosecution by refusing to make judicial findings justifying closure of the court-martial to the public each time such a closure occurred. Such judicial findings for each closed session are not required. Mil.R.Evid. 505 is directed towards the information sought to be exempted from disclosure at a public trial. See Mil.R.Evid. 505(i)(4)(A) and (C). As the information may be divulged by a number of witnesses or documents, or both, the focus of exclusion is upon that specific information. Consequently, the specificity required addresses the information to be protected, not through what method it is disclosed. In contrast, rights of privacy of individuals such as were involved in *Press-Enterprise Co. v. Superior Court, 464 U.S. 501, 104 S. Ct. 819, 78 L. Ed. 2d 629 (1984),* focus upon individual rights requiring particularized rulings as to each individual situation.

> To require a military judge to make specific findings each time a series of questions is to be asked of a witness, after the judge had already determined the responses were classified, would be to create unnecessary and disruptive bifurcation of the trial and constitute an exercise in redundancy. The confusion would make a difficult trial an incomprehensible one and would be the antithesis of a fair and orderly proceeding within the context of the facts of this case. n4
>
> n4 We note the appellant's counsel were the first to request a closed session (to cross-examine a prosecution witness who had just testified in open session) and then later concurred in a bifurcated presentation of a Government witness' testimony with direct and cross-examination in open session followed by a closed session composed of further direct and cross-examination.
>
> We do not believe *Grunden* mandated judicial findings for each closed session when the Court of Military Appeals stated that "limited portions" of a court-martial may be partially closed despite defense objection but in "each instance the exclusion must be used sparingly with the emphasis always toward a public trial." Rather, as we noted regarding Mil.R.Evid. 505, the Court was addressing individualized decision-making as to specific information which the Government asserts must be exempted from disclosure at a public trial whenever that information is presented during the course of the trial. Further, we find nothing in Hershey that delineates such a requirement.
>
> . . .
>
> We believe the closure procedure utilized in this case was the fairest and most practical that could be devised. The extent of the closures was determined by either Government or defense. The military judge had already determined which information, because of its classified status, would be presented in closed sessions. The fact that certain unclassified information was disclosed by individuals whose duties and identities could not be publicly matched-up was necessary to protect classified information. Further bifurcation of other witnesses' testimony, other than as occurred, was impracticable and would have created unnecessary chaos. In fact, the apparent inadvertent disclosure of classified information by both parties in public sessions occurred rather frequently despite the efforts of the court to ensure nondisclosure. The procedure utilized allowed both parties a reasonably normal context within which to pursue their respective positions.

Lonetree, 31 M.J. at 853-54 (citations omitted).

TAB C

Recommended Reading

A. List of Law Review Articles.

1. Eisenberg, Graymail and Grayhairs: The Classified and Official Information Privileges Under the Military Rules of Evidence, The Army Lawyer, March, 1981.

2. Maher, The Right to a Fair Trial in Cases Involving the Introduction of Classified Information, 120 Mil. L. Rev. 83 (1988).

3. Anderson, Spying in Violation of Article 106, UCMJ: The Offense and the Constitutionality of its Mandatory Death Penalty, 127 Mil. L. Rev. 1 (1990).

B. List of Cases.

1. Scarbeck v. United States, 315 F.2d 546 (U.S. App. D.C. 1962)

2. United States v. Grunden, 2 M.J. 116 (CMA) 1977)

3. Cooke v. Orser, 12 M.J. 335 (CMA 1982)

4. United States v. Horton, 17 M.J. 1131 (NMCMR 1984)

5. United States v. Yunis, 867 F.2d 617 (U.S. App. D.C. 1989)

6. United States v. Lonetree, 31 M.J. 849 (NMCMR 1990)

7. United States v. Allen, 31 M.J. 572 (NMCMR 1990)

8. United States v. Pruner, 33 M.J. 272 (CMA 1991)

9. United States v. Lonetree, 35 M.J. 396 (CMA 1992)

10. United States v. Anzalone, 40 M.J. 658 (NMCMR 1994)

11. United States v. King, 2000 CAAF LEXIS 321 (CAAF 2000)

C. Executive Order 12958, Classified National Security Information, released 17 Apr 95.