CHAPTER 6

Security Requirements

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

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

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

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

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

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

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

If the civilian defense counsel wants to represent an accused in a court-martial involving classified information, civilian defense counsel must cooperate with the process to obtain a clearance. In *United States v. Jolliff*, a case tried under CIPA, the defense counsel was reluctant to submit to a security clearance process. The court stated: "Although the Sixth Amendment grants an accused an absolute right to have assistance of counsel, it does not follow that his right to a particular counsel is absolute." *Jolliff*, 548 F.Supp. 227 (D. Md. 1981). This was a warning that counsel's failure to cooperate in obtaining a security clearance can lead to disqualification and dismissal from the case by the trial judge. 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).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

This page intentionally left blank

APPENDIX 6-A

Attorney Access Authorization Request

5510
23 Nov 04

From:
To: Chief of Naval Operations (N09N2)
Via: Office of the Judge Advocate General (Code 17)

Subj: REQUEST FOR ACCESS AUTHORIZATION FOR ATTORNEY NAME, SSN

Ref: (a) SECNAVINST 5510.30A

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

a. NAME, SSN
U.S. citizen

b. Date and Place of Birth:

c. Security Clearance: None

d. Military Experience: None

e. Level requested: (Choose one) Secret / Top Secret

f. Duration of Access: until legal proceedings have concluded, approx. 1 yr

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

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

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

Very respectfully,

This page intentionally left blank

APPENDIX 6-B

Accused Access Request

5510
Ser __/
[Date]

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

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

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

1. For the purposes stated in reference (a), you are authorized access to national security information classified up to and including Secret.

2. Your access is limited to [matters related to preparation of your defense to the charges preferred on (DATE)] [discussion of the classified statement you provided to NCIS with your detailed and properly cleared defense counsel]. I reserve the right, in consultation with applicable original classification authorities, to limit your access in accordance with paragraph (d) of reference (b).

3. Physical custody and retention of classified material is not authorized. You are to comply with all rules and regulations regarding handling and safeguarding classified material. [Specifically, you are reminded of the terms of my previously issued protective order in this case, reference (c). **(NOTE: Should use this language and a protective order for post-preferral access; not necessary for limited, pre-preferral access)**]

4. You must complete the Classified Information Nondisclosure Agreement (SF-312) required by paragraph 9-4 of reference (d[c]) prior to receiving access to any classified information. Copies will be provided to my Staff Judge Advocate, trial counsel, the Office of the Judge Advocate General (Code 17), and, if applicable, the designated Investigation/Court Security Officer.

I. C. Onvene

This page intentionally left blank

APPENDIX 6-C

Sample Protective Order and MOU

5 Nov 05

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

f. Persons subject to this Order are admonished that any breach of the security procedures in this Order may result in the termination of their access to classified information. In addition, they are admonished that any unauthorized disclosure or possession of classified information may constitute violations of Untied 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 all persons who are attorneys, violations of this Order will be filed with their State Bar Association.

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

4. Personnel Security Investigations and Clearances

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6. Handling and Protection of Classified Information

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

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

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

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

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

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

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

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

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

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

j. The defense shall not disclose the contents of any classified documents or information to any person not named herein, except the members of this court-martial, if any, and the judge advocates for the United States identified by the Court Security Officer as having the appropriate clearances, and a need to know.

k. All persons given access to classified information pursuant to this Order are advised that all information to which they obtain access by the Order is now and will forever remain the property of the United States Government. They shall return all materials which may have come into their possession, or for which they are responsible because of such access, upon demand by the Court Security Officer.

l. A copy of this Order shall issue forthwith to defense counsel named herein, with a further order that said defense counsel advise the accused named herein of the contents of this Order, and furnish him a copy. The accused, through defense counsel, shall forthwith sign the statements set forth in paragraph 4.d of this Order, and counsel shall forthwith file an original with the Convening Authority and provide an original each to the Court Security Officer and the trial counsel. The signing and filing of this statement by the accused is a condition precedent to the disclosure of any classified information to the accused.

7. Nothing contained in these procedures shall be construed as a waiver of any right of the accused.

/S/

MEMORANDUM OF UNDERSTANDING

1. I, _____, understand that I may be the recipient of information and intelligence that concerns the present and future security of the United States and that belongs to the United States. This information and intelligence, together with the methods of collecting and handling it, are classified according to security standards set by the U.S. Government. I have read and understand the provisions of the espionage laws (sections 793, 794, and 798 of Title 18, United States Code) concerning the disclosure of information relating to the national defense and the provisions of the Intelligence Identities Protection Act (section 421 of Title 50, United States Code) and I am familiar with the penalties for the violation thereof. I have also read and understand the provisions of SECNAV Instruction 5510.36, concerning safeguarding, disseminating, transmitting and transporting, storage and destruction, and loss or compromise of classified information.

2. I have been advised that the unauthorized disclosure, unauthorized retention, and negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation or enemy of the United States. I herby agree that I will never divulge classified information to anyone unless (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive classified information: or (b) I have been given prior written notice of the authorization of the United States Government Department or Agency responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted; or (c) as ordered by the Convening Authority. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose the information, except as provided in (a), (b) or(c), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information. I have been advised and understand that any breach of this agreement may result in the termination of any access to classified information. I recognize that this agreement including its provision for the termination of access to classified information does not constitute a waiver of the United States' right to prosecute me for any statutory violation.

3. I understand that this agreement will remain binding on me after the conclusion of proceedings in _____.

4. I have received, read and understand the Protective Order entered by the Convening Authority on _____2004, in the case of _____, relating to classified information, and I agree to comply with the provisions thereof.

5. I understand that noncompliance with this Order will be reported to any State Bar where I am admitted to practice law.

_____ _____

Signature Date

Witnessed, sworn and subscribed to before me this __day of_____,2004

_____

Signature of Witness