

## CHAPTER 7

### Classification Reviews

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

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

**1. Distinction.** The “classification review” must be distinguished from other analytical processes such as the “damage assessment” and “declassification review.” It is neither a damage assessment nor a declassification review. The failure to properly understand and distinguish this difference frequently results in confusion, lost time, delay, and faulty products. “Classification review” was once defined and distinguished from these other processes in DODI 5240.11, “Damage Assessments” (Issued on 23 December 1991, and cancelled on 1 June 2005). While this instruction was cancelled without replacement, it remains informative on this issue, and is consistent with current language found in SECNAVINST 5510.36.<sup>2</sup> Enclosure (1) of DODI 5240.11 defined a classification review as “[a] formal finding that information subjected to loss or compromise is (was) legally classified at the time of compromise. The review usually includes an assessment of the probability (risk) of damage to national security resulting from disclosure of this information or material to an unauthorized person. A classification review is obtained in all national security cases and is necessary when a determination must be made on the use of classified information as trial evidence under the Classified Information Procedures Act or Military Rule of Evidence 505.” While originally required only in “national security cases,” classification reviews should be obtained in *all* cases involving classified information.

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

---

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

<sup>2</sup> SECNAV M-5510.36, paragraph 12-16 describes classification reviews which include:

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

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

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

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

**B. Components of a Classification Review Package.**

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

**FOR OFFICIAL USE ONLY**

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

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

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

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

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

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



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

**C. Role of the Affidavit at Trial.** The classification review package has three distinct purposes. Procedurally, it is required under M.R.E. 505 to assert the privilege and prevent the use of classified information at trial. The classification review also demonstrates that information is properly classified. This allows the government the opportunity to argue for a closed session during *Grunden* hearings. Finally, the classification review addresses an element of one or more charged offense because it sets forth the classification level of the information at the time of the offense<sup>3</sup> and describes the harm to national security<sup>4</sup> that would result from compromise of the information. Thus, the classification review is a critical part of pretrial proceedings and the trial itself.

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

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

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

---

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

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

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



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

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

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

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

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

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

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

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



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

**APPENDIX 7-A**

**Sample Classification Review Affidavit**

Declaration

I, LCDR \_\_\_\_\_, USN, declare and state:

BACKGROUND

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

PURPOSE OF DECLARATION

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

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

DESIGNATION OF INFORMATION

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

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

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

**FOR OFFICIAL USE ONLY**

**PROTECTION OF INFORMATION**

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

**CLASSIFICATION DETERMINATION**

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

**IMPACT ON NATIONAL SECURITY IF INFORMATION RELEASED**

Unauthorized disclosure of the classified material specified above would:

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

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

\_\_\_\_\_  
LCDR USN  
OPNAV N78  
ASW Sensors Requirements Officer

Executed this \_\_\_\_ day of \_\_\_\_\_ 2006.

**FOR OFFICIAL USE ONLY**

**APPENDIX 7-B**

**Sample OCA Cover Letter**

SECRET (UNCLASSIFIED upon removal of Enclosure (2))

From: Original Classification Authority  
To: Convening Authority

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

Ref: (a) Your ltr 5510 Ser x of 14 Oct 04, w/o encl  
(b) Military Rule of Evidence 505, Manual for Courts-  
Martial, 2005

Encl: (1) Affidavit of LCDR X of 14 Oct 04  
(2) Classified document in question

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

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

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

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

OCA

**7-B-1**

**FOR OFFICIAL USE ONLY**

**FOR OFFICIAL USE ONLY**

**This page intentionally left blank**

**7-B-2**

**FOR OFFICIAL USE ONLY**