IN A GENERAL COURT-MARTIAL
IN THE SECOND JUDICIAL CIRCUIT, U.S. ARMY TRIAL JUDICIARY
FORT BRAGG, NORTH CAROLINA

UNITED STATES	)	
	)	
v.	)	Government Response to Defense Motion
	)	for an Order Concerning Defense's
BERGDAHL, ROBERT BOWDRIE	)	Access to Classified Evidence in
(BOWE)	)	Possession of Trial Counsel
SGT, U.S. Army	)	
HHC, Special Troops Battalion	)	29 January 2016
U.S. Army Forces Command	)	
Fort Bragg, North Carolina 28310	)	

RELIEF SOUGHT

The Government first requests that the Court deny the Defense Motion for an Order Concerning Defense's Access to Classified Evidence in Possession of Trial Counsel (D APP #5) because the proposed order is contrary to the plain language of the applicable law and rules governing discovery and classified information, and would require this Court to sanction the unauthorized disclosure of classified information. The Government further requests the Court amend its Protective Order for Classified Information, or issue a supplemental order, specifying that the Defense must gain consent from all original classification authorities [hereinafter "OCAs"] who originally classified the particular information sought by the Defense before seeking access to classified information directly from any Government agency or department, any current or former Government employee, any Government information systems, or any other United States entity. Finally, the Government seeks leave of the Court to interview the Defense security officer and requests that the Court take judicial notice of Enclosures 5 and 6 to this Response. The Government requests oral argument.

BURDEN OF PERSUASION AND BURDEN OF PROOF

The Defense as the moving party bears the burden of persuasion on any factual issue whose resolution is necessary to decide this motion. The burden of proof is a preponderance of the evidence. Rule for Courts-Martial [hereinafter "R.C.M."] 905(c).

FACTS

On 30 June 2009, the Accused, an Infantryman (MOS 11B) deployed to Paktika Province, Afghanistan, as part of Task Force Yukon, Combined Joint Task Force-82/Regional Command-East, deserted from his place of duty at Observation Post Mest. The Accused was captured by enemy forces shortly after he departed. Over the following months, Task Force Yukon and other elements of the United States Armed

Forces engaged in extensive search and recovery operations to recover the Accused. The Accused was released back to the custody of the United States on 31 May 2014.

Court-martial charges were preferred against the Accused on 25 March 2015. The case was referred to a General Court-Martial on 14 December 2015. The Court issued a Protective Order for Classified Information on 14 January 2016, and the Defense provided its First Defense Discovery Request on 20 January 2016.[1]

To date, Trial Counsel have disclosed almost 6000 pages of unclassified documents and provided access to more than 900 pages of classified exhibits to a 2014 Army Regulation 15-6 administrative investigation regarding the circumstances of this case to Defense Counsel. Further, the Joint Personnel Recovery Agency [hereinafter "JPRA"] has allowed Defense Counsel to review all documents and media in its custody related to the Accused. Trial Counsel are currently preparing additional documents for Defense review, and have requests pending for OCA consent to allow the Defense to review more than 32,000 pages of classified documents.

The Government is willing to stipulate to the following from the Defense statement of facts for the limited purpose of obtaining a ruling on this motion: (1) the Government utilized ten Judge Advocates and e-discovery software to review classified information in this case as part of its due diligence efforts; (2) the Government is currently utilizing six Judge Advocates to review classified information in this case as part of its due diligence efforts (however, the Government does not agree these Judge Advocates have "enjoyed continuous access to all classified materials to aid their case preparation"); (3) the Government anticipates seeking OCA consent to allow Defense to review more than 25,000 documents estimated to consist of more than 300,000 pages; (4) Defense Counsel LTC Rosenblatt met with Trial Counsel on 13 January 2016 at the U.S. Army Forces Command headquarters (however, the Government does not agree with the Defense's recitation of the discussions between counsel during that meeting); (5) Defense Counsel and the Accused all have at least a SECRET security clearance, have signed the Standard Form 312 Classified Information Nondisclosure Agreement, and have acknowledged the Court's Protective Order for Classified Information; and (6) the trial is currently scheduled to commence on 8 August 2016.

WITNESSES/EVIDENCE

The Government encloses the following documents as evidence:

1. DA Form 2823, Sworn Statement of PFC Carolyn M. Byers, dated 11 December 2015.
2. Memorandum from LTC Franklin D. Rosenblatt, Subject: United States v. SGT Bergdahl, Request to Preserve Evidence, dated 7 April 2015.
3. Email Correspondence from LTC Franklin D. Rosenblatt, Subject: classified materials, dated 7 April 2015.

[1] The Defense appears to consider Enclosures 2 and 3, which were sent before the Defense was entitled to discovery, to also constitute a discovery request.

4. First Defense Discovery Request, dated 20 January 2016.

5. Department of Defense Manual 5200.01, Volume 3, DoD Information Security Program: Protection of Classified Information, Enclosure 2.

6. Army Regulation 380-67, Personnel Security Program, paragraph 3-23.

LEGAL AUTHORITY AND ARGUMENT

I. Defense is not Entitled to "Open File" Discovery

Both during oral argument on 12 January 2016, and in its motion, the Defense has asserted that it is entitled to see all documents in the Trial Counsel's possession based on Article 46 of the Uniform Code of Military Justice [hereinafter "UCMJ"] and the Sixth Amendment to the Constitution, and asks the Court to order the parties "to work cooperatively in implementing open-file discovery of both classified and unclassified materials."[2] This request disregards the plain language of the Rules for Courts-Martial and Military Rules of Evidence, and decades of precedent regarding the scope and regulation of discovery. Simply put: the Defense is not entitled to open file discovery, regardless of whether the information is classified or unclassified. With regard to the Defense's Constitutional arguments, the Supreme Court has been clear that "[w]e have never held that the Constitution demands an open file policy." *Kyles v. Whitley*, 514 U.S. 419, 437–41 (1995) (analyzing alleged *Brady* violations and explaining that it is the prosecution that determines whether potential evidence is disclosed to the defense). This is especially true in cases—like this one—where sensitive information is at issue. *See Pa. v. Ritchie*, 480 U.S. 39, 59 (1987) ("A defendant's right to discover exculpatory evidence does not include the unsupervised authority to search through the

[2] The Government disputes the Defense characterization that it has improperly imposed a "fanciful interpretation of its right to keep all classified evidence to itself and not disclose it to defense." Rather, the Government has only sought to ensure that all disclosures of classified information to the Defense are conducted in accordance with the requirements of M.R.E. 505(h), Executive Order 13526, and established procedures followed in other courts-martial with significant amounts of classified information. The Government is not seeking to withhold disclosable classified information from the Defense; it is only seeking to disclose that information consistent with the law and the rules.

The Government also disputes the Defense characterization of the information already made available to the Defense. The Defense asserted it has only been provided access to over 900 pages of classified materials in this case. This is incorrect. To date, the Government has provided Defense Counsel with almost 6000 pages of unclassified materials, and has provided Defense Counsel access to more than 900 pages of classified materials. Furthermore, JPRA has provided Defense Counsel with access to all materials regarding SGT Bergdahl in its possession at Fort Belvoir. The Government is currently preparing additional documents for Defense review, which can be scheduled with the reasonable notice required by Paragraph 1i(7) of the Protective Order for Classified Information. Finally, the Government has OCA consent requests pending for more than 32,000 pages of classified materials.

Of note, in the 14 December 2015 Government Motion for Article 39(a) Pretrial Conference and Docketing Order Pursuant to Military Rule of Evidence 505(f) (G APP #1), the Government proposed that the Defense review of classified information disclosable under Section III of the Military Rules of Evidence be conducted prior to arraignment (the Government made those documents available), and that the initial Defense review of classified information disclosable pursuant to the Rules for Courts-Martial and Military Rules of Evidence be conducted during the week of 22 February 2016 (approximately one month following the due date of the Defense discovery request). The Defense did not provide feedback on that proposed timeline or propose its own timeline, and instead came to Trial Counsels' office on 13 January 2016 and asked to see the classified information in this case without prior notice.

Commonwealth's files…. [T]his Court has never held—even in the absence of a statute restricting disclosure—that a defendant alone may make the determination as to the materiality of the information. Settled practice is to the contrary.").[3] The Defense here asks for precisely what the Supreme Court has repeatedly determined it is not Constitutionally entitled to: unsupervised authority to conduct its own search through Government files to determine what is disclosable.

In addition to not being Constitutionally required, the Defense's request is contrary to the plain language and intent of the disclosure and discovery provisions of the Rules for Courts-Martial and the Military Rules of Evidence. Indeed, the Defense argument would render R.C.M. 701(a), Section III of the Military Rules of Evidence, and the entire line of *Brady* cases, null. The Court of Appeals for the Armed Forces has acknowledged that even in military practice, there is no requirement for the Government to simply turn over all of its files to the Defense. *See U.S. v. Rivers*, 49 M.J. 434, 437 (C.A.A.F. 1998) ("[T]he defense is not entitled to unrestricted access to government information. Where a conflict arises between the defense search for information and the Government's need to protect information, the appropriate procedure is '*in camera* review' by a judge." (citations omitted)). Although the Defense has cited to Article 46 as support for open file discovery, there is a clear caveat in that Article: "The trial counsel, the defense counsel, and the court-martial shall have equal opportunity to obtain witnesses and other evidence *in accordance with such regulations as the President may prescribe*." 10 U.S.C. § 846 (emphasis added). Article 46 does not, as Defense asserts, support the conclusion that whenever Trial Counsel have access to information, the Defense Counsel must be given access to the same information.[4] Instead, just as Article 46 has provided, the President has prescribed rules to regulate the scope and procedure of discovery, including those found in R.C.M. 701, R.C.M. 703, and Military Rule of Evidence [hereinafter "M.R.E."] 505. As a result of these rules, the Government will always have greater access to its own information, just as the Defense will always have greater access to its own information. This is clear from a plain reading of R.C.M. 701(a), which details the *subset* of information the Trial Counsel must disclose, and R.C.M. 701(b), which details the narrower subset of information the Defense must disclose. *See Robinson v. Shell Oil Co.*, 519 U.S. 337, 340 (1997) (discussing statutory construction and stating that the court's inquiry must cease if the statutory language is unambiguous and the statutory scheme is coherent and consistent). There would be no need for these rules to establish left and right limits to discovery scope, or for specific discovery requests to be submitted as was ordered by the Court here, if we had an open file system where there were no limits to discovery anyway.

---

[3] The *Ritchie* Court also stated that "where a defendant makes only a general request for exculpatory material under *Brady v. Maryland*, 373 U.S. 83 (1963), it is the State that decides which information must be disclosed. Unless defense counsel becomes aware that other exculpatory evidence was withheld and brings it to the court's attention, the prosecutor's decision on disclosure is final. Defense counsel has no constitutional right to conduct his own search of the State's files to argue relevance." *Ritchie*, 480 U.S. at 59; *see U.S. v. Campa*, 529 F.3d 980, 995 (11th Cir. 2008) ("Ordinarily, the government alone determines whether material in its possession must be turned over to a defendant.").

[4] Under the Defense's reading of Article 46, the inverse would also have to be true: whenever the Defense Counsel has access to information, Trial Counsel must be given access to the same information.

The Government is not seeking to deprive the Defense access to information to which it is entitled. It is merely seeking to abide by the Rules for Courts-Martial, Military Rules of Evidence, and the precedent guiding execution of discovery. The Government is aware of its disclosure and discovery obligations, and will meet those requirements. There is no authority cited, Constitutional or otherwise, that would permit the Defense to double-check Government due diligence in this case, or allow it complete access to conduct a review of the Government's files.[5]

II. The Defense's Position Regarding Access to Classified Information Is Contrary to Law, and Warrants an Amendment or Supplement to the Protective Order

A. Defense Has no Need-to-Know Nondisclosable Classified Information

In addition to the plain reading of the rules for disclosure and discovery in courts-martial, the need-to-know and OCA consent requirements for disclosure of classified information to the Defense also preclude open file discovery in this case. Section 4.1(a) of Executive Order 13526, Classified National Security Information, states that a person can access classified information only if, among other requirements, the person has a need-to-know, which is defined as a "determination…that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function." E.O. 13526, sec. 6.1(dd). Here, the Defense seeks access to all classified information in the Government's possession, much of which has already been determined by Trial Counsel to be not disclosable under the Rules for Courts-Martial and Military Rules of Evidence, or in a significant number of cases, is totally irrelevant to this case. The Defense does not have a need-to-know gigabytes of classified information that is not material to this case under the disclosure and discovery rules.[6] Consequently, any order directing disclosure of such irrelevant

[5] Contrary to Defense's assertions, the Government does not lack authority for its position that the Defense is not entitled to open file classified discovery under Article 46 and the Sixth Amendment. *See Schmidt v. Boone*, 59 M.J. 841, 857 (A.F.C.C.A. 2004) ("We conclude R.C.M. 701 and 703, and Mil. R. Evid. 505, are entirely consistent with the rule-making authority granted to the President by Congress under Articles 36 and 46, UCMJ. The rules provide a reasonable process to assure 'equal opportunity to obtain witnesses and other evidence' under Article 46, UCMJ, while protecting the interests of both parties."), *vacated on other grounds*, *U.S. v. Schmidt*, 60 M.J. 1 (C.A.A.F. 2004); *U.S. v. Fuhrman*, 2006 CCA LEXIS 106, at *12–13 (N-M.C.C.A. 2006) (finding that M.R.E. 505 "adequately protects the appellant from government overreaching" and is not facially unconstitutional), *aff'd*, *U.S. v. Fuhrman*, 64 M.J. 437 (C.A.A.F. 2006); *U.S. v. Murphy*, 2008 CCA LEXIS 511, at *23–24 (A.F.C.C.A. 2008) (stating that M.R.E. 505 balances the interests of the accused who desires access to classified information for his defense and the interests of the Government in protecting that information); *see also* M.R.E. 505, analysis at A22-41 ("Rule 505 is based upon H.R. 4745, 96th Cong., 1st Sess. (1979), which was proposed by the Executive Branch as a response to what is known as the 'graymail' problem in which the defendant in a criminal case seeks disclosure of sensitive national security information, the release of which may force the government to discontinue the prosecution…. The rule attempts to balance the interests of an accused who desires classified information for his or her defense and the interests of the government in protecting that information.").

[6] There is significant precedent in Article III courts that Defense Counsel require both a security clearance and need-to-know before accessing classified information. The need-to-know is not met merely by being counsel to the accused. *See U.S. v. Amawi*, 2009 U.S. Dist. LEXIS 34476, at *2–5 (N.D. Ohio 2009) ("Getting clearance is not enough for access to classified information: there is, quite sensibly, also a

information would be directing the unauthorized disclosure of classified information, which is expressly prohibited by M.R.E. 505(a) ("Under no circumstances may a military judge order the release of classified information to any person not authorized to receive such information.").

B. OCA Consent is Required by Executive Order 13526

In addition to being inconsistent with the need-to-know requirement, the Defense position would also circumvent the OCA consent requirement under Executive Order 13526 and M.R.E. 505(h). As fully detailed in the Government Motion for Article 39(a) Pretrial Conference and Docketing Order Pursuant to Military Rule of Evidence 505(f), the Trial Counsel cannot simply turn over classified information to Defense Counsel. Any disclosure or dissemination of classified information must be done in accordance with Executive Order 13526, which establishes that classified information may not be freely distributed by an agency with access to that information. *See* E.O. 13526, sec. 4.1(i)(1) (permitting dissemination of information classified on or after 27 June 2010 only to another Executive Branch agency by any agency to which it has been made available and permitting the originating agency to require prior consent before any further dissemination); E.O. 13526, sec. 4.1(i)(3) (stating classified information created prior to 27 June 2010 cannot be disseminated outside any agency to which it has been made available without consent of the originating agency).[7]

The Defense has argued these limitations are not applicable in this case pursuant to section 4.1(i)(4), which states "the Department of Defense shall be considered one agency." It further argues all members of the Defense Team—including civilians with no status within the Department of Defense—should be considered within the Department, therefore any classified information obtained by the Defense can be shared throughout the team without limitation. This argument stretches section 4.1(i)(4) beyond its meaning. Although the Defense argues all members of the Defense Team should be considered within the Department of Defense due to their role in this court-martial, possession of security clearances, and the execution of forms, these persons' only interest in this case is as representatives of the Accused. *See* Army Regulation

---

'need-to-know' requirement…. Clearance simply qualifies counsel to view secret materials. It does not, however, *entitle* counsel to see anything and everything that the government has stamped classified even if it has something to do with a client."); *U.S. v. Libby*, 429 F. Supp. 2d 18, 24 (D.D.C. 2006) ("[T]he defendant is a former national security official and his attorneys possess security clearances, and they have already been provided with and permitted to view classified documents. These circumstances, however, do not lead to the inescapable conclusion that the defendant and his team of attorneys should be permitted to view every classified document associated with this case."); *U.S. v. Bin Laden*, 126 F. Supp. 2d 264, 287 n.27 (S.D.N.Y. 2000) ("Defense counsel's assertion that, given their security clearance, they ought to have access to the sensitive documents is not persuasive to the court. As the Government explains those security clearances enable El-Hage's attorneys to review classified documents, 'but they do not entitle them to see all documents with that classification.'"). These cases interpret provisions of the Classified Information Procedures Act, which is the federal corollary to M.R.E. 505. *See* M.R.E. 505, analysis at A22-41.

[7] Because the Accused's misconduct occurred on 30 June 2009, which is well before 27 June 2010, much of the classified information at issue in this case will likely be subject to the section 4.1(i)(3) requirement that further dissemination of classified information requires express consent of the OCA.

27-26, Rules of Professional Conduct for Lawyers, Rule 1.13 (stating Army lawyers represent the Army "*except* when representing an individual client" and "[a] lawyer who has been duly assigned to represent an individual who is subject to disciplinary action…has, for those purposes, a lawyer-client relationship with that individual" (emphasis added)). Indeed, the process for the Accused's civilian defense counsel to gain a security clearance pursuant to his role in this case is governed by Army Regulation 380-67, Personnel Security Program, paragraph 3-23, which is titled "Access by persons *outside* the executive branch" (emphasis added). The Defense has not cited any authority to extend the definition of the Department of Defense as an agency to all members of the Defense Team, particularly considering that personnel on the Defense Team are dedicated exclusively to representing the interests of the Accused in this case. Consequently, Executive Order 13526 does bar disclosure of classified information to the Defense Team without OCA consent.

C. The Classified Information Privilege Requires OCA Consent

But even more significant than the requirements of Executive Order 13526 in this case is the United States' classified information privilege as detailed in M.R.E. 505(h), which would be subverted if the Court enters the order proposed by the Defense. The Defense correctly notes that under M.R.E. 505(h)(1)(A), the Government may, through submission of a declaration signed by the head or designee of an executive agency or military department, invoke the United States' classified information privilege to delete, withhold, or otherwise limit the discovery of, or access to, classified information by the Defense. That declaration must be submitted to the Court by the Trial Counsel, who can further request an alternative to full discovery of the classified information by the Defense (i.e., redactions, a summary, or a stipulation). M.R.E. 505(h)(1)(B); M.R.E. 505(h)(2). In order to prevent the Defense from accessing or reviewing classified information over which privilege is invoked, the military judge must conduct an *in camera* review of the classified information upon request of the Trial Counsel, and may even conduct an *ex parte* discussion with Trial Counsel regarding the classified information. M.R.E. 505(h)(2)(B); M.R.E. 505(b)(5). The terms of this rule therefore anticipate a process in which the Trial Counsel and the Military Judge will have access to classified information, and even classified information disclosable to the Defense under the Rules for Courts-Martial and Military Rules of Evidence, that the Defense will never access or see in its complete form.

Defense argues that the invocation of privilege under M.R.E. 505(h) is the rule's only limitation on the Defense's discovery of, and access to, classified information, but then further concludes that there is otherwise no OCA consent requirement and all other classified information must therefore be disclosed immediately. This argument overlooks a critical step in the process: to allow a privilege holder a chance to invoke the privilege, someone has to let that holder know in advance that a party is seeking potentially privileged information. Indeed, there would be little reason for the classified information privilege to even exist if the Defense is allowed to circumvent the privilege by never giving the OCA concerned a meaningful opportunity to assert it in the first place. Quite simply, the Government argues that in accordance with the plain meaning

of the rule, prior to the Defense accessing information classified by an OCA, it must give that OCA a meaningful opportunity to determine whether it wishes to invoke its classified information privilege. The Defense's position, to the contrary, would allow it to comb through the SIPRNET[8] or JWICS[9] collecting classified information without ever talking to a human being, or speak with any current or former Government employee of any agency to collect classified information from those individuals without ever bothering to check whether the OCA wished to seek an invocation of privilege. The Defense's position would further allow it to direct Trial Counsel, contrary to their obligations to safeguard classified information, to provide all classified information in their possession to the Defense, whether or not Defense Counsel has a need-to-know, regardless of any limitation placed on disclosure of that information by the OCA,[10] and without any opportunity to check with the OCAs to determine whether they wish to seek invocation of the classified information privilege. The Defense, in short, is asking the Court to allow it to sidestep the OCAs in seeking classified information, effectively depriving the OCAs of their ability to invoke the classified information privilege.[11] This circumvention of OCAs is precisely what M.R.E. 505 was intended to prevent. *See Murphy*, 2008 CCA LEXIS 511, at *23–24 ("[T]he decision to release the classified material always belongs to the 'head of the executive or military department or government agency concerned' and the military judge may not compel the release of the information.").

As noted in the Government Request for Clarification filed on 21 January 2016 (G APP #7) and in the paragraphs above, the Defense's interpretation of its access to classified information in this case is contrary to Executive Order 13526, M.R.E. 505, and the basic concept of privilege, and greatly increases the risk of unauthorized disclosures of classified information. To protect against such unauthorized disclosure the Government respectfully requests that the Court deny the Defense's request for an order, and instead either amend or supplement the Protective Order for Classified Information with the following proposed language: "Pursuant to the requirements of M.R.E. 505(h) and Executive Order 13526, Defense Counsel and other members of the Defense Team may not seek access to classified information in furtherance of their representation of the Accused directly from any Government agency or department, any current or former Government employee, any Government information systems (including, but not limited to, SIPRNET and JWICS), or any other United States entity, except as previously authorized by all OCAs (as that term is defined in Executive Order

[8] The Secret Internet Protocol Router Network is the Department of Defense network for the exchange of classified information and messages at the SECRET level.
[9] The Joint Worldwide Intelligence Communications System is an information system certified to exchange or handle TOP SECRET material or Sensitive Compartmented Information.
[10] In addition to being classified at the CONFIDENTIAL, SECRET, or TOP SECRET level, information can be subject to originator control (ORCON), or be part of an Alternative Compensatory Control Measure (ACCM), that further restricts dissemination. E.O. 13526, sec. 4.1(i)(1); Department of Defense Manual 5200.01, v3, DoD Information Security Program: Protection of Classified Information, Encl. 2, para. 18.
[11] This interpretation of the classified information privilege could even prejudice the Accused later in these proceedings as "[e]vidence of a statement or other disclosure of privileged matter is not admissible against the holder of the privilege if disclosure was compelled erroneously or was made without an opportunity for the holder of the privilege to claim the privilege." M.R.E. 511(a).

13526 and the Protective Order for Classified Information) who have classified the particular information sought by the Defense."

III. The Defense's Proposed Sanctions Should be Rejected

The Defense notes that it will seek sanctions from the Court pursuant to M.R.E. 505(j)(4) "[i]f the prosecution does not comply with [the proposed Defense order] forthwith." Sanctions pursuant to this section are inappropriate for alleged discovery violations as they apply only if the Government continues to object to disclosure of classified information *in trial and pretrial proceedings* following a determination by the military judge that alternatives to full disclosure may not be used. M.R.E. 505(j)(4)(A); *see also* M.R.E. 505(j)(4)(B) (stating the Government can avoid sanctions "by permitting the accused to disclose the information at the pertinent court-martial proceeding"). Indeed, the section title of M.R.E. 505(j) is "Procedure for Use of Classified Information in Trial and Pretrial Proceedings" (as opposed to M.R.E. 505(h), which is titled "Discovery and Access by the Accused"). As these sanctions apply to a different stage of the proceedings, they should not be issued during discovery.

IV. The Government Seeks Leave of the Court to Interview the Defense Security Officer

The Defense listed Mr. Donald Gardner, the Defense Security Officer, as a potential witness on this motion. Paragraph 1e(2) of the Court's Protective Order for Classified Information states that the "Defense security officer is part of the Defense team and will maintain the confidentiality of all discussions with other members of the Defense team, and any observations made during Defense reviews or access to classified information." Notwithstanding this provision, the Government seeks leave of the Court to interview Mr. Gardner prior to any testimony he may give, regarding matters within the scope of his testimony. This action is permissible because the Defense has named him as a witness. *See U.S. v. Turner*, 28 M.J. 487, 488 (C.M.A. 1989) ("An expert may be of assistance to the defense in two ways. The first is as a witness to testify at trial. When serving in this capacity, he properly may be interviewed by the prosecutor.").

V. The Government Denies Production of the Trial Counsel as a Witness

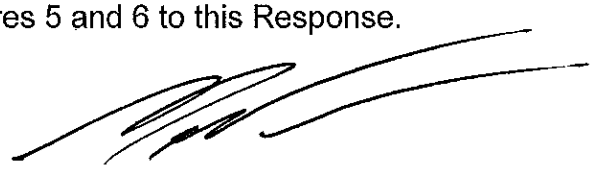
The Government denies production of the Trial Counsel as a witness on this motion. The Defense has made no showing pursuant to R.C.M. 703(c)(2) why testimony of the Trial Counsel who argued the initial motions regarding classified information in this case and would presumably argue this motion as well is "relevant and necessary." *See* R.C.M. 703(c)(2) (requiring that a witness list contain a synopsis of the expected testimony sufficient to show its relevance and necessity).

VI. The Government Requests Judicial Notice

On 8 January 2016, the Government requested that the Court take judicial notice pursuant to M.R.E. 202 of Executive Order 13526; Army Regulation 27-10, Military Justice, Chapter 6; and Army Regulation 27-26, Rules of Professional Conduct for Lawyers, Appendix B, Rule 1.13. In addition to these sources of domestic law, the Government further requests that the Court take judicial notice of the following domestic law pursuant to M.R.E. 202: Department of Defense Manual 5200.01, volume 3, DoD Information Security Program: Protection of Classified Information, Enclosure 2; and Army Regulation 380-67, Personnel Security Program, paragraph 3-23. "The military judge may take judicial notice of domestic law." M.R.E. 202. These documents are not subject to reasonable dispute because they can be accurately and readily determined from a source whose accuracy cannot be questioned.

CONCLUSION

Based on the above, the Government respectfully requests that the Court deny the Defense Motion for an Order Concerning Defense's Access to Classified Evidence in Possession of Trial Counsel. The Government further requests the Court amend its Protective Order for Classified Information, or issue a supplemental order, specifying the proposed language in Section II.C of this Response. Finally, the Government seeks leave of the Court to interview Mr. Gardner if he is called as a witness and requests that the Court take judicial notice of Enclosures 5 and 6 to this Response.



MICHAEL PETRUSIC
CPT, JA
Trial Counsel

I certify that I have served or caused to be served a true copy of the above Government Response to Defense Motion for an Order Concerning Defense's Access to Classified Evidence in Possession of Trial Counsel to Defense Counsel via email on 29 January 2016.

MICHAEL PETRUSIC
CPT, JA
Trial Counsel

SWORN STATEMENT

For use of this form, see AR 190-45; the proponent agency is PMG.

PRIVACY ACT STATEMENT

AUTHORITY: Title 10, USC Section 301; Title 5, USC Section 2951; E.O. 9397 Social Security Number (SSN).

PRINCIPAL PURPOSE: To document potential criminal activity involving the U.S. Army, and to allow Army officials to maintain discipline, law and order through investigation of complaints and incidents.

ROUTINE USES: Information provided may be further disclosed to federal, state, local, and foreign government law enforcement agencies, prosecutors, courts, child protective services, victims, witnesses, the Department of Veterans Affairs, and the Office of Personnel Management. Information provided may be used for determinations regarding judicial or non-judicial punishment, other administrative disciplinary actions, security clearances, recruitment, retention, placement, and other personnel actions.

DISCLOSURE: Disclosure of your SSN and other information is voluntary.

1. LOCATION	2. DATE *(YYYYMMDD)*	3. TIME	4. FILE NUMBER
Building 4700 Knox St., Fort Bragg, NC 28307	20151211	0940	

5. LAST NAME, FIRST NAME, MIDDLE NAME	6. SSN	7. GRADE/STATUS
Byers, Carolyn Marie		E3/AD

8. ORGANIZATION OR ADDRESS
HQ, FORSCOM

9. I, Carolyn M. Byers, WANT TO MAKE THE FOLLOWING STATEMENT UNDER OATH:

I am a paralegal currently assigned to the US Army Forces Command Headquarters. I have worked on the US v. Bergdahl case since January 2015. As of 11 December 2015, the Government Counsel has received documents related to the case from 26 agencies. I have personally been involved in the receipt, processing, and attorney review of those documents. As of the date of this statement more than 25,000 documents received via classified media have been marked disclosable by attorney reviewers.

I was also involved in processing classified information for Defense review in this case. The Defense has reviewed classified exhibits from MG Kenneth Dahl's AR 15-6 investigation, which was completed on 18 December 2014, and other classified material requested by Defense. These reviews occurred on 22 July 2015 and 2 September 2015 at Fort McNair, Washington D.C. and totaled approximately 926 pages.

----------Nothing Follows----------

10. EXHIBIT	11. INITIALS OF PERSON MAKING STATEMENT	PAGE 1 OF 2 PAGES
	CMB	

ADDITIONAL PAGES MUST CONTAIN THE HEADING "STATEMENT OF_____ TAKEN AT ____ DATED ____

THE BOTTOM OF EACH ADDITIONAL PAGE MUST BEAR THE INITIALS OF THE PERSON MAKING THE STATEMENT, AND PAGE NUMBER MUST BE INDICATED.

STATEMENT OF Carolyn M. Byers TAKEN AT Fort Bragg, NC DATED 20151211

9. STATEMENT *(Continued)*

AFFIDAVIT

I, Carolyn M. Byers, HAVE READ OR HAVE HAD READ TO ME THIS STATEMENT WHICH BEGINS ON PAGE 1, AND ENDS ON PAGE 2. I FULLY UNDERSTAND THE CONTENTS OF THE ENTIRE STATEMENT MADE BY ME. THE STATEMENT IS TRUE. I HAVE INITIALED ALL CORRECTIONS AND HAVE INITIALED THE BOTTOM OF EACH PAGE CONTAINING THE STATEMENT. I HAVE MADE THIS STATEMENT FREELY WITHOUT HOPE OF BENEFIT OR REWARD, WITHOUT THREAT OF PUNISHMENT, AND WITHOUT COERCION, UNLAWFUL INFLUENCE, OR UNLAWFUL INDUCEMENT.

(Signature of Person Making Statement)

WITNESSES:

Crystal J. Edwardsneal
4700 Knox St.
Fort Bragg, NC 28307
ORGANIZATION OR ADDRESS

ORGANIZATION OR ADDRESS

Subscribed and sworn to before me, a person authorized by law to administer oaths, this 11th day of December, 2015 at Fort Bragg, NC

(Signature of Person Administering Oath)

CPT Michael Petrusic
(Typed Name of Person Administering Oath)

Article 136, UCMJ
(Authority To Administer Oaths)

INITIALS OF PERSON MAKING STATEMENT CMB

DA FORM 2823, NOV 2006

APD LC v1.01ES

07 April 2015

MEMORANDUM FOR LTC Peter Q. Burke, Commander, Special Troops Battalion, United States Army Forces Command, Fort Bragg, North Carolina 28310

SUBJECT: United States v. SGT Bergdahl, Request to Preserve Evidence

1. Request: the Defense team requests that the U.S. military issue or seek orders to preserve evidence from the following organizations pertaining to SGT Bergdahl and his captivity:

a) Central Intelligence Agency

b) National Security Agency

c) Federal Bureau of Investigation

d) Naval Criminal Investigation Service

e) U.S. Army Criminal Investigation Command

f) United States Central Command

g) Defense Intelligence Agency

h) Joint Special Operations Command

i) Joint Personnel Recovery Agency

j) Combined Joint Task Force – 10

k) Regional Command East

l) Personnel Recovery Team, Kabul, Afghanistan

m) Joint Improvised Explosive Device Defeat Organization

n) United States Forces – Afghanistan

o) U.S. Army Intelligence and Security Command

2. Discussion

a) Based on media reports, finding Sergeant Bergdahl was a top priority intelligence requirement for several U.S. military organizations and agencies of the U.S. government from 2009 to 2014. As a result, it is possible that the U.S. government currently has a larger casefile on SGT Bergdahl than any other criminally accused person in the United States. The amount of evidence in possession of the government that is relevant to SGT Bergdahl's case might include tens of thousands of pages of additional documents.

b) SGT Bergdahl is charged with criminal conduct spanning a period from 2009 to 2014. Much of the evidence currently held by other U.S. military organizations and agencies will be relevant to SGT Bergdahl's defense. For example, classified intelligence gathered about his departure from his duty station and subsequent capture by the Taliban will be relevant to each charge. Signal intercepts, human intelligence, imagery, and classified operational reporting might reveal additional statements by SGT Bergdahl, statements by his captors about SGT Bergdahl, SGT Bergdahl's mental state, escape attempts, conditions of captivity and health, and SGT Bergdahl's conduct as a Soldier while in captivity. All of these will be relevant to the sentencing authority in a case for which the government can presently seek the UCMJ's most severe punishments of Death or confinement for life. Adding to the importance of this evidence is that there are currently no known available witnesses who can corroborate SGT Bergdahl's statements which might be admitted into evidence; such an uncorroborated account may be viewed as self-serving by a sentencing authority and result in a far more severe punishment.

c) Currently, it appears that very little or none of the relevant material held by other U.S. government and military organizations is in FORSCOM's possession. The FORSCOM trial counsel MAJ Kurz wrote to the defense on 07 April 2015 that no classified evidence in the possession of trial counsel negates or reduces degree of guilt for an offense charged. (The defense has not yet been provided access to these classified materials so cannot verify this). The absence of any relevant classified evidence described by the trial counsel is understandable given that the Army 15-6 investigation conducted by MG Dahl only asked for extremely narrow and specific responses from outside agencies, and did not seek any information about SGT Bergdahl's capture or five-year captivity. The evidence that defense will seek from these other agencies will be broader in order to obtain matters relevant to his defense.

d) Before the defense gains a power to seek to compel discovery of evidence later in the proceedings, potentially relevant evidence must necessarily first be preserved. MG Dahl's AR 15-6 investigation contains evidence that at least one organization (Personnel Recovery Team, Kabul, Afghanistan) has already destroyed evidence concerning SGT Bergdahl. Immediate preservation orders are the most appropriate means for the government to ensure that evidence held by government entities outside of FORSCOM is preserved and remains accessible.

FRANKLIN D. ROSENBLATT
LTC, JA
Individual Military Counsel for SGT Bergdahl

Beese, Christian E LTC USARMY HQDA TJAGLCS (US)

From: Rosenblatt, Franklin D LTC USARMY (US)
Sent: Tuesday, April 07, 2015 2:52 PM
To: Kurz, Margaret V MAJ USARMY FORSCOM (US); Beese, Christian E MAJ USARMY CAC (US)
Cc: eugene.fidell@yale.edu; Foster, Alfredo N Jr CPT USARMY IMCOM HQ (US)
Subject: classified materials

MAJ Kurz,

When can we expect to see the classified materials?

Respectfully,

Frank Rosenblatt

LTC, JA

phone: 808-477-9981

NIPR: franklin.rosenblatt@pacom.mil <mailto:franklin.rosenblatt@pacom.mil>

SIPR: franklin.rosenblatt@socom.smil.mil <mailto:franklin.rosenblatt@socom.smil.mil>

UNITED STATES	)	First Defense Discovery Request
	)	
v.	)	
	)	
ROBERT BOWDRIE (BOWE) BERGDAHL	)	
Sergeant (E-5), U.S. Army	)	
Headquarters and Headquarters Company	)	
Special Troops Battalion	)	
U.S. Army Forces Command	)	
Fort Bragg, NC 28310	)	20 January 2016

This is the defense's first discovery request, in accordance with the Pretrial Order. A written response to each numbered request is requested. Please Bates-stamp all disclosures to aid both sides in organizing the case. The inclusion of any matter in this request is without prejudice to any mandatory disclosure that trial counsel must make under the law, including R.C.M. 701(a)(1), 701(a)(3), 701(a)(4), and 701(a)(6) and Section III of the Military Rules of Evidence and that, even if such information is not specifically requested in this request, such information must still be disclosed to defense. The requests set forth below are continuing in nature. R.C.M. 701(d). All references to "trial counsel" are intended to extend to each and every judge advocate detailed or otherwise made available in fact to work on or assist the prosecution for any period and for any purpose, whether or not they are listed on any appointing order or personally appear during any session of the court-martial. The information requested herein is material to the preparation of the accused's defense. Counsel's ability to render the required effective assistance may be compromised without it. As trial counsel is not in a position to know what may or may not be material to the defense, trial counsel should apply a liberal standard of relevance when determining whether information will be disclosed. *United States v. Roberts*, 59 M.J. 323, 326 (C.A.A.F. 2004) (noting liberal mandate in discovery and holding specifically that evidence of a of witness's credibility was relevant to the defense and was therefore material to the defense for the purpose of discovery); *see also United States v. Webb*, 66 M.J. 89, 92 (C.A.A.F. 2008) (noting that the discovery mandate includes information that may not be admissible before trial and includes information that may assist the defense in formulating a strategy). This request is not limited to trial counsel's personal knowledge but extends to information known to others who may be acting on the government's behalf. *United States v. Jackson*, 59 M.J. 330, 334 (C.A.A.F. 2004) (discussing the trial counsel's duty to exercise due diligence in discovering other favorable evidence). If trial counsel contends that the requested information need not (or cannot) be disclosed or that the requested information does not exist, a written statement to that effect is requested. If no response to any request is received, the defense will assume that trial counsel has denied that request and may move for an order compelling discovery. R.C.M. 701(g)(1)(3).

1. In accordance with R.C.M. 701(a)(1), any paper that accompanied the charges when they were referred, the convening order and any orders amending it, and any signed or sworn statement that relates to an offense charged in this matter.

2. In accordance with R.C.M. 701(a)(2)(A), any book, paper, document, photograph, or tangible object and the opportunity to inspect any building or place that is within the control of military

authorities and that is material to the preparation of the defense or that trial counsel intends to use in the prosecution's case-in-chief or that was obtained from or belonged to the accused. By way of illustration and not limitation to this general request, defense specifically requests:

3. Video of SGT Bergdahl while in captivity from approximately November 2013. This video shows SGT Bergdahl in a state of near-death during a time covered by each of the charges. It was offered as a "proof of life" video by the Taliban in order to continue negotiations for SGT Bergdahl's release. This video is in the possession of the Department of State Special Representative for Afghanistan and Pakistan. There are no known copies within control of DoD.

4. SGT Bergdahl's complete enlistment file of source documents at, from or to Human Resources Command, including all documents, of whatever description, including both hard copy and email communications and memoranda of telephone conversations relating in any way to the extension(s) of his enlistment as well as concerning the defense's efforts to obtain these documents. HRC officials told defense that these source documents are normally given to the Soldier upon request, but that they would not provide them to SGT Bergdahl due to the "sensitivity" of his case.

5. All documents, including emails to or from HRC officials, concerning whether to award or withhold military decorations to SGT Bergdahl at any time from June 2014 through January 2016 and ongoing.

6. All flag paperwork on SGT Bergdahl from May 2009 to present.

7. The complete Afghanistan diary of then-LT John Billings.

8. Any statements of the accused not disclosed to the defense in the government's Section III disclosure.

9. All correspondence about SGT Bergdahl between the Department of Defense (DoD) and any component or office thereof and the House Armed Services Committee (HASC), to include its members and staff. On 14 June 2014 the Chairman Buck McKeon asked DoD for ongoing disclosure of all intelligence reports relating to SGT Bergdahl, all final recommendations of reports concerning SGT Bergdahl, and all non-disclosure agreements signed by members of the armed forces relating to SGT Bergdahl.

10. All correspondence about SGT Bergdahl between the DoD or any component or office thereof and the Senate Armed Services Committee (SASC), to include its leadership, members, staff, and congressional fellows.

11. Name, rank, and contact information of any military personnel who worked at OCLL or as Congressional Fellows (including, but not limited to, JAG officers) who fielded congressional inquiries about SGT Bergdahl. Copies of all inquiries from Congress or any committee or member thereof about SGT Bergdahl from 2009 to present, and copies of all responses from Department of Defense or any component or office thereof to these inquiries.

12. Appointment calendars for TJAG, DJAG, Director of Army Staff, and Chief of Staff of Army from June 2014 to January 2016.

13. Any grant or offer of immunity or leniency given to any potential government witness, including any persons who committed unauthorized disclosures or mishandling of classified information.

14. Documents concerning the detailing of LTC Christian Beese and MAJ Margaret Kurz to this case and to FORSCOM before any convening authority had decided whether preferral of charges was warranted. Name(s) of person(s) who coordinated this detailing.

15. All documents concerning the detailing of 10 additional attorneys to the prosecution team in or about October 2015, and the addition of an unknown number of mobilized reservist attorneys to the prosecution team in or about January 2016. In order to assist the defense in safeguarding sensitive and classified case information, and also to ensure we have adequate resources to defend the case, we request a current roster of all members of the prosecution team and notification when team members change, including experts, paralegals, warrant officers, and investigators.

16. All materials concerning SGT Bergdahl that were presented to President Obama in 2014 in advance of his decision to release five detainees in order to secure SGT Bergdahl's release.

17. All briefing materials provided to GEN Mark Milley concerning SGT Bergdahl's case in preparation for his confirmation hearing as Chief of Staff of the Army, and copies of any information exchanged between DoD officials and the SASC or any member of staffer thereof concerning SGT Bergdahl's case in advance of this confirmation hearing.

18. The 2015 CID investigation into the conduct of members of SGT Bergdahl's platoon regarding the treatment of human remains in Afghanistan, including the battalion's policy concerning how human remains should be treated. This request seeks both the investigation and all agent investigative materials.

19. All documents or other evidence the prosecution intends to use concerning whether any military members died in efforts to find SGT Bergdahl.

20. All classified and unclassified emails sent to or from LTC Peter Q. Burke, GEN Mark Milley, or GEN Robert Abrams concerning SGT Bergdahl and his case during the period that each served as his court-martial convening authority.

21. All documents and investigations relating to the military members the prosecution contends were wounded searching for SGT Bergdahl, to include names and contact information, complete medical records, LOD investigations, JAGMAN or AR 15-6 investigations, and classified or unclassified storyboards.

22. Form DD214 for Senator John S. McCain. This is required to determine whether he is a military retiree who is subject to the UCMJ for purposes of art. 37, UCMJ.

23. Documents and communications about SGT Bergdahl's restoration to full duty from June to August 2014.

24. All documents related to MG Scaparrotti's grant of testimonial immunity to then-PFC Bergdahl in the summer of 2009 in Afghanistan.

25. Copies of all rights advisals and warnings given to SGT Bergdahl. Notice of any oral rights warnings or advisals.

26. The USFOR-A classified "tactical directive" published in the summer of 2009.

27. Documents pertaining to unsuccessful negotiations to secure SGT Bergdahl's release in 2009, including names and contact information of persons involved in the negotiations.

28. Diplomatic cables, notes, documents, or messages in the possession of the Department of State pertaining to SGT Bergdahl from U.S. embassies in Islamabad or Kabul from 2009 to 2014.

29. Following MG Dahl's investigation, the Director of Army Staff on 22 December 2014 directed the Deputy Chief of Staff, G-1 (DCS, G-1) to provide within 90 days recommendations related to the finding in Part IV, paragraph 2a on whether the Army should request DoD to: (a) modify the coding on separation documents related to behavioral health concerns to make them more specific and standardize them; and (b) mandate access to prior service records to review the separation actions of prior service applicants before granting a waiver. We request to see the DCS G-1's submissions responsive to this order. The Director of Army Staff also directed DCS, G-1 to advise the Director of Army Staff within 90 days what actions have been taken related to the findings in Part V, paragraphs 1(c)(2)-(6), 2(a)(1), and 2(a)(2). We request to see the DCS G-1's response. We request notice if DCS G-1 amended or caused to be amended any regulations, policies, guidance, or doctrine as a result.

30. Bates page 3629 includes the following CID agent investigative activity on 10/07/2009 at 16:39 by Jesus R. Rodriguez: "Received confidential roll-up reports for two individuals captured and detained by U.S. forces. The detainees related significant information on the whereabouts and condition of PFC BERGDAHL." Please provide the referenced reports and the names and contact information of the two individuals.

31. Information on any persons including detainees within de facto or effective U.S. control, or under the control of proxies, who have personal knowledge of SGT Bergdahl in captivity. We also request information on how we can speak with these individuals.

32. Names and contact information for any persons who are not under U.S. control but are known by U.S. officials to have personal knowledge of SGT Bergdahl's captivity.

33. SGT Bergdahl's current complete military health record, with care taken so that it does not include any mental health examination or assessment matters that are subject to the M.R.E. *513 privilege*.

34. Any written instructions or regulations that were in effect in 2009 used by Recruiting Command officials in the approval of enlistment waivers.

35. Any law enforcement investigation that relates to this matter. By way of illustration and not limitation, this request incorporates all agent-activity summaries; all agent-investigation reports; any enclosures to those reports; any statement taken by any law enforcement agent from any person regardless of how that statement is recorded and any evidence of any advice of that

person's rights under art. 31, UCMJ or the Constitution; any interview worksheet, including any administrative information that is taken before a law enforcement interview occurs; any case note; any agent summary; any interim, final, and supplemental report; any photograph or slide or diagram or sketch or drawing; any evidence or property-custody document (*e.g.*, DA Form 4137); any consent to search or any affidavit regarding any request for a warrant or search authorization and any such warrant or search authorization or any denial of the same; and any electronic file of any type and content.

36. Any investigation that relates to this matter that was not conducted by a law enforcement agent regardless of whether that investigation was a formal or informal investigation. By way of illustration and not limitation, this request includes any AR 15-6 (or equivalent) investigation, inspector general investigation, LOD investigation, after-action report, collateral safety investigation, and any Commander's inquiry under M.R.E. 303 and includes any appointing order; any evidence that was received by the investigator regardless of whether that item of evidence was received formally, considered, or credited; any statement that was taken by the investigator; any interim findings or recommendations regardless of whether those findings or recommendations were incorporated into the final report; any legal review of the investigation; the final findings and recommendations of the investigation regardless of whether those findings or recommendations were approved, disapproved, or modified; the approval, disapproval, or modification of those findings and recommendations; and any supplemental report concerning the investigation.

37. A complete copy of any recording of the Article 32 preliminary hearing.

38. Any evidence that trial counsel intends to mark as an exhibit during the government's case-in-chief, rebuttal, if any, or any pre-sentencing proceeding.

39. For each witness to the events described in the charges that are now pending against the accused or whom the trial counsel intends to call during the government's case-in-chief or rebuttal or at any pre-sentencing proceeding:

(a) A complete copy of the witness's personnel file. By way of illustration and not limitation, this request includes the Army Human Resources Record (formerly known as the Official Military Personnel File or a service equivalent) and the Officer Record Brief or Enlisted Record Brief or service equivalent; the civilian personnel file, if any, for each witness; the so-called "local file" for each witness; the accreditation file for each law enforcement witness; any record of any non-judicial punishment against or discharge before the expiration of term of service for any witness; the curriculum vitae of any expert; and any adverse administrative action against any witness, including any letter of reprimand or GOMOR however filed.

(b) A copy of any National Crime Information Center or Crime Records Center record, any Case Review Committee record, and any police record, including CID reports, Military Police reports, or civilian police reports. To the extent that trial counsel has not already requested this information, this request also constitutes an express request of the trial counsel to conduct such a search.

(c) Any investigation into the conduct of that witness regardless of whether that investigation is pending formal initiation or is ongoing or concluded and regardless of whether

the investigation resulted in a favorable or unfavorable finding with respect to the witness's conduct.

(d) Any record of non-judicial punishment that was considered or imposed on the witness; any record of any "titling," arrest, or apprehension of the witness; any charge, complaint, information, or indictment against the witness; and any judgment of criminal conviction involving the witness, including any result of trial or initial or final promulgating order of trial by court-martial or record of trial in a summary court-martial that involved the witness.

(e) Any medical or mental health record of any witness that may show that the witness may have misrepresented the events at issue or is biased or prejudiced or has a motive to misrepresent or that, due to a medical or mental-health issue, may have misperceived the events at issue or may fail to accurately recall those events. *See* M.R.E. 608 (discussing impeachment evidence). To the extent that the government claims that a medical record is protected from disclosure, defense notes that the military does not recognize a "doctor-patient" privilege. M.R.E. 501(d); *see also United States v. Clark*, 62 M.J. 195, 198 (C.A.A.F. 2005) (stating there is generally no doctor-patient privilege in the military). If trial counsel asserts that these records are privileged under the psychotherapist-patient or victim-advocate-victim privilege or any other privilege recognized by military law, defense requests written evidence that the privilege has been claimed by its holder or written evidence of specific authorization for trial counsel to assert that privilege on the holder's behalf. *See* M.R.E. 513(c) (noting that counsel may be authorized to claim the privilege on behalf of a holder but not incorporating counsel into the list of persons whose authority to claim the privilege is presumed); 514(c) (stating also that counsel may claim the privilege but not including trial counsel in the list of persons who have presumptive authority to claim the privilege).

40. Any written notice, including any invoice, purchase agreement, purchase order, or contract, of any result or report of any physical or mental examination or of scientific test or experiment regardless of whether the actual result or report is within the possession, custody, or control of military authorities.

41. Any report of any error, whether ultimately founded or not, of any expert who conducted any physical or mental examination or scientific test or experiment in this matter or any information that may call into question the practices or procedures of that expert or any laboratory in which such a test was conducted. This request includes the quality-assurance or quality-control reports for any applicable laboratory for the 24 months preceding any test and any such reports for the period between the test and the trial in this matter.

42. Any document used by a witness to prepare for trial, including any document that was used by the witness to refresh that witness's recollection before testifying. *See* M.R.E. 612.

43. Any statement made by any Commander or Convening Authority, or their assigned judge advocates, that provides guidance to any person concerning the appropriate disposition of or punishment for any offense, expresses any form of disfavor toward any person who may testify or has testified on behalf of any other person in any case or expresses any opinion regarding the guilt or innocence of the accused, or that may show that the officer has any interest other than an official interest in this matter.

44. Any evidence that any officer or law enforcement agent who has taken action in this case has violated or is suspected of violating the UCMJ or other criminal law.

45. Any materials that were furnished to or considered by the Convening Authority, including any written advice by the Staff Judge Advocate, when the Convening Authority selected the panel members detailed to this court-martial. VISGER.

46. Any response to any questionnaire that was submitted to any panel member in accordance with R.C.M. 912(a)(1), each member's signed acknowledgment of GEN Abrams's December 2015 order to them, and all panel members' Officer Record Briefs.

47. Any certification of any document that is provided in accordance with any portion of this discovery request. *E.g.*, M.R.E. 901(b)(10), 902.

48. Any evidence that is material to the preparation of the defense, including evidence that may be offered by the prosecution in rebuttal. *See United States v. Luke,* 69 M.J. 309 (C.A.A.F. 2009) (stating rebuttal evidence falling under R.C.M. 701(a)(2) is material to preparation of the defense and must be disclosed); *see also United States v. Trimper,* 28 M.J. 460 (C.M.A. 1989).

49. In accordance with R.C.M. 701(a)(5), any document trial counsel intends to present at any pre-sentencing proceeding and the names and addresses of all witnesses whom the trial counsel intends to call at any such proceeding.

50. In accordance with the Fifth Amendment and R.C.M. 701(a)(6), defense respectfully notes the obligation to disclose (and it requests the disclosure of) the existence of any evidence that is either known by trial counsel or should be known to trial counsel through the exercise of due diligence (*see United States v. Williams,* 50 M.J. 436 (C.A.A.F. 1999) (outlining scope of the prosecutor's duty to search for *Brady* evidence beyond prosecutor's own files)) that reasonably tends to negate the guilt of the accused of an offense that is charged, reduce the degree of guilt of the accused of an offense that is charged, or reduce the punishment. *Brady v. Maryland*, 373 U.S. 83, 87 (1963) (holding that the suppression by the prosecution of evidence that is favorable to the accused violates due process when the evidence is material to either guilt or punishment and irrespective of the good or bad faith of the prosecutor). Without limitation to this general requirement to disclose, that requirement also includes:

(a) Any evidence that relates to the credibility of any witness. *Giglio v. United States*, 405 U.S. 150, 154 (1972) (holding that when the reliability of a witness "may well be determinative of guilt or innocence," the nondisclosure of evidence affecting credibility falls within the *Brady* disclosure requirement).

(b) Any grant of immunity or leniency, of any type, granted or promised to any witness by the government (including civilian, state, and foreign authorities) in exchange for that witness's testimony. *See* M.R.E. 301(c)(2) (stating that once a grant of immunity or leniency has been made, that grant must be reduced to writing and served on defense).

51. Under M.R.E. 404(b), the defense requests notice of the general nature of any evidence of other crimes, wrongs, or acts that the government intends to introduce at trial.

52. Under M.R.E. 613(a), the defense requests disclosure of any prior statement of a witness, whether written or not, that trial counsel intends to examine the witness concerning.

53. Blotter entries or operational reporting for all DUSTWUNs in Afghanistan from 2008 to 2010.

54. A copy of the request sent by the prosecutors for SGT Bergdahl's medical records which resulted in the HIPAA violation and wrongful disclosure of privileged mental health records by government officials.

55. To aid in the preparation of the defense's case and to ensure that the defense has an equal opportunity to obtain witnesses and other evidence, the defense requests contact information for any witness that the trial counsel may possess, including telephone numbers and e-mail addresses. *See* art. 46, UCMJ (equal-opportunity rule for courts-martial); *see also* R.C.M. 701(a)(3) (providing that before trial, the trial counsel shall disclose the names and addresses of the witnesses who the trial counsel intends to call in the prosecution's case-in-chief).

EUGENE R. FIDELL
Civilian Defense Counsel

FRANKLIN D. ROSENBLATT
LTC, JA
Military Defense Counsel

Department of Defense

MANUAL

NUMBER 5200.01, Volume 3
February 24, 2012
Incorporating Change 2, March 19, 2013

USD(I)

SUBJECT: DoD Information Security Program: Protection of Classified Information

References: See Enclosure 1

1. PURPOSE

a. Manual. This Manual is composed of several volumes, each containing its own purpose. The purpose of the overall Manual, as authorized by DoD Directive (DoDD) 5143.01 (Reference (a)) and DoD Instruction (DoDI) 5200.01 (Reference (b)), is to reissue DoD 5200.1-R (Reference (c)) as a DoD Manual to implement policy, assign responsibilities, and provide procedures for the designation, marking, protection, and dissemination of controlled unclassified information (CUI) and classified information, including information categorized as collateral, sensitive compartmented information (SCI), and Special Access Program (SAP). This guidance is developed in accordance with Reference (b), Executive Order (E.O.) 13526, E.O. 13556, and part 2001 of title 32, Code of Federal Regulations (CFR) (References (d), (e), and (f)). This combined guidance is known as the DoD Information Security Program.

b. Volume. This Volume:

(1) Provides guidance for safeguarding, storage, destruction, transmission, and transportation of classified information.

(2) Identifies security education and training requirements and processes for handling of security violations and compromise of classified information.

(3) Addresses information technology (IT) issues of which the security manager must be aware.

(4) Incorporates and cancels Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandums (References (g) and (h)).

2. APPLICABILITY. This Volume:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereinafter referred to collectively as the "DoD Components").

b. Does not alter existing authorities and responsibilities of the Director of National Intelligence (DNI) or of the heads of elements of the Intelligence Community pursuant to policies issued by the DNI. Consistent with Reference (b), SCI shall be safeguarded in accordance with the policies and procedures issued by the DNI, as implemented by DoD 5105.21-M-1 (Reference (i)) and other applicable guidance.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy, in accordance with Reference (b), to:

a. Identify and protect national security information and CUI in accordance with national-level policy issuances.

b. Promote information sharing, facilitate judicious use of resources, and simplify management through implementation of uniform and standardized processes.

c. Employ, maintain and enforce standards for safeguarding, storing, destroying, transmitting, and transporting classified information.

d. Actively promote and implement security education and training throughout the Department of Defense.

e. Mitigate the adverse effects of unauthorized access to classified information by investigating and acting upon reports of security violations and compromises of classified information.

5. RESPONSIBILITIES. See Enclosure 2 of Volume 1.

6. PROCEDURES. See Enclosures 2 through 7.

7. INFORMATION COLLECTION REQUIREMENTS. All inspections, investigations, notifications, and audits required by this Volume are exempt from licensing according to paragraphs C4.4.1, C4.4.2, C4.4.7 and C4.4.8 of DoD 8910.1-M (Reference (j)).

8. RELEASABILITY. UNLIMITED. This Volume is approved for public release and is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

9. EFFECTIVE DATE. This Volume:

a. Is effective February 24, 2012.

b. Must be reissued, cancelled, or certified current within 5 years of its publication in accordance with DoD Instruction 5025.01 (Reference (ck)). If not, it will expire effective February 24, 2022 and be removed from the DoD Issuances Website.

Michael G. Vickers
Under Secretary of Defense
for Intelligence

Enclosures
1. References
2. Safeguarding
3. Storage and Destruction
4. Transmission and Transportation
5. Security Education and Training
6. Security Incidents Involving Classified Information
7. IT Issues for the Security Manager

Glossary

ENCLOSURE 2

SAFEGUARDING

1. CONTROL MEASURES. DoD Components shall have a system of control measures that ensure access to classified information is limited to authorized persons. The control measures shall be appropriate to the environment in which access occurs and to the nature and volume of the information. The system shall include technical, physical, and personnel control measures. Administrative control measures, which may include records of internal distribution, access, generation, inventory, reproduction, and disposition, shall be required when technical, physical, and personnel control measures are insufficient to deter and detect access by unauthorized persons. Except as otherwise specified, requests for waivers to the provisions of this Volume shall be submitted in accordance with section 16 of Enclosure 3 of Volume 1.

2. PERSONAL RESPONSIBILITY FOR SAFEGUARDING. Everyone who works with classified information is personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to classified information. Everyone granted access to classified information is personally responsible for protecting the classified information they know, possess, or control and for complying with the pre-publication security review processes specified in DoDD 5230.09 (Reference (k)). Classified information shall be protected at all times either by storing it as this Volume prescribes or by having it under the personal observation and control of an authorized individual.

3. ACCESS TO CLASSIFIED INFORMATION. Except as provided in sections 5 and 6 of this enclosure and in accordance with section 11 of Enclosure 3 of Volume 1, no person may have access to classified information unless that person has a security clearance in accordance with DoD 5200.2-R (Reference (l)) and has signed a Standard Form (SF) 312, "Classified Information Non-Disclosure Agreement" (NDA), and access is essential to the accomplishment of a lawful and authorized Government function (i.e., has a need to know).

4. DETERMINING NEED FOR ACCESS. The individual with authorized possession, knowledge, or control of the information has the final responsibility for determining whether a prospective recipient's official duties requires them to possess or have access to any element or item of classified information, and whether that prospective recipient has been granted the appropriate security clearance by proper authority.

5. EMERGENCY AUTHORITY. In emergencies in which there is an imminent threat to life or in defense of the homeland, the Heads of the DoD Components may authorize the disclosure of classified information, including information normally requiring the originator's prior authorization, to an individual or individuals who are otherwise not routinely eligible for access. The disclosing authority shall:

a. Limit the amount of classified information disclosed to the absolute minimum to achieve the purpose.

b. Limit the number of individuals who receive classified information.

c. Transmit the classified information through approved Federal government channels by the most secure and expeditious method consistent with this Volume, or by other means deemed necessary when time is of the essence.

d. Provide instructions about what specific information is classified and how it should be safeguarded. Information disclosed shall not be deemed declassified as of result of such disclosure or subsequent use by a recipient. Physical custody of classified information must remain with an authorized Federal government entity in all but the most extraordinary circumstances.

e. Provide appropriate briefings to the recipients on their responsibilities not to disclose the information to unauthorized individuals and obtain a signed SF 312.

f. Notify the agency or DoD Component originating of the information and the Deputy Under Secretary of Defense for Intelligence, and Security (DUSD(I&S)) within 72 hours of the disclosure of classified information, or at the earliest opportunity that the emergency permits but no later than 30 days after the release, by providing:

(1) A description of the disclosed information.

(2) Identification of individuals to whom the information was disclosed.

(3) How the information was disclosed and transmitted.

(4) Reason for the emergency release.

(5) How the information is being safeguarded.

(6) A description of the briefings provided.

(7) A copy of the signed SF(s) 312.

6. ACCESS BY INDIVIDUALS OUTSIDE THE EXECUTIVE BRANCH. Classified information may be made available to individuals or agencies outside the Executive Branch, as provided in this section, if such information is necessary for performance of a lawful and authorized function, and such release is not prohibited by the originating department or agency. The Heads of DoD Components shall designate officials to ensure the recipient's eligibility for access, prior to the release of classified information. (See Volume 1, Enclosure 3, section 11 for requirements for access by individuals inside the Executive Branch.)

a. Congress. DoDI 5400.04 (Reference (m)) provides rules for access to classified information or material by Congress, its committees, members, and staff representatives. Members of Congress, by virtue of their elected position, are not investigated or cleared by the Department of Defense.

b. Government Printing Office (GPO). Collateral documents and material of all classifications may be processed by the GPO, which protects the information according to a DoD/GPO Security Agreement (Reference (n)).

c. Representatives of the Government Accountability Office (GAO). DoDI 7650.01 (Reference (o)) sets forth rules for granting GAO representatives access to classified information that the Department of Defense originates and possesses when such information is relevant to the performance of the statutory responsibilities of that organization. Certifications of security clearances and the basis therefore, shall be accomplished under arrangements between the GAO and the relevant DoD Component. Personal recognition or presentation of official GAO credential cards are acceptable for identification purposes, but not for access to classified information.

d. Historical Researchers. Persons outside the Executive Branch who are engaged in historical research projects may be authorized access to classified information provided that the DoD Component Head or senior agency official with classification jurisdiction over the information:

(1) Determines, in writing, that such access is clearly consistent with the interests of national security in view of the intended use of the material to which access is granted by certifying that the requester has been found to be eligible for access pursuant to Reference (l) and section 3 of this enclosure.

(2) Limits access to specific categories of information over which the DoD Component has classification jurisdiction or for which the researcher has the written consent of the DoD Component or non-DoD agency with classification jurisdiction. The information contained within or revealed by the specified categories must be within the scope of the research.

(3) Maintains custody of the classified material at a DoD installation or activity or authorizes access to documents held by the National Archives and Records Administration (NARA).

(4) Obtains the requester's agreement to safeguard the information and to submit any notes and manuscripts intended for public release for review by all DoD Components or non-DoD departments or agencies with classification jurisdiction to determine whether classified information is contained therein. The agreement shall be documented by execution of a statement substantially similar to that in Figure 1.

Figure 1. Conditions Governing Access to Official Records by Historical Researchers

To Whom It May Concern:

I understand that the classified information to which I have requested access for historical research purposes is concerned with the national defense or foreign relations of the United States. Unauthorized disclosure could reasonably be expected to cause damage, serious damage, or exceptionally grave damage to the national security depending on whether the information is classified Confidential, Secret, or Top Secret, respectively. If granted access, I therefore agree to the following conditions governing access to the [insert Component or activity] files:

1. I will abide by any rules and restrictions issued in your letter of authorization, including those of other Agencies whose information is interfiled with that of the [insert Component or activity].

2. I agree to safeguard the classified information to which I gain possession or knowledge in a manner consistent with Part 4 of Executive Order 13526, "Classified National Security Information," and the applicable provisions of the DoD regulations concerning safeguarding classified information, including Volumes 1, 2, and 3 of DoD Manual 5200.01, "DoD Information Security Program."

3. I agree not to reveal to any person or Agency any classified information obtained because of this access except as authorized in the terms of your authorization letter or a follow-on letter. I further agree that I shall not use the information for purposes other than those set forth in my request for access.

4. I agree to submit my research notes for review to determine if classified information is contained in them before their removal from the specific area assigned to me for research. I further agree to submit my manuscript(s) for a security review before its publication or presentation. In each of these reviews, I agree to comply with any decision of the reviewing official in the interests of the security of the United States, including the retention or deletion of any classified parts of such notes and manuscript whenever the Federal Agency concerned deems such retention or deletion necessary.

5. I understand that failure to abide by the conditions in this statement shall constitute sufficient cause for canceling my access to classified information and for denying me any future access and may subject me to criminal provisions of Federal Law as referred to in Item 6.

6. I have been informed that provisions of title 18 of the United States Code impose criminal penalties, under certain circumstances, for the unauthorized disclosure, loss, copying, or destruction of defense information.

THIS STATEMENT IS MADE TO THE UNITED STATES GOVERNMENT TO ENABLE IT TO EXERCISE ITS RESPONSIBILITY FOR THE PROTECTION OF INFORMATION AFFECTING THE NATIONAL SECURITY. I UNDERSTAND THAT ANY MATERIAL FALSE STATEMENT THAT I MAKE KNOWINGLY AND WILLFULLY SHALL SUBJECT ME TO THE PENALTIES OF TITLE 18, U.S. CODE, SECTION 1001.

Signature:

Witness's Signature:

Date:

(5) Authorizes access, in writing, for no more than 2 years from the date of issuance. The DoD Component may renew access for 2-year periods in accordance with DoD Component-issued regulations.

e. Presidential or Vice Presidential Appointees and Designees. Persons who previously occupied senior policy-making positions to which they were appointed or designated by the President or Vice President may not remove classified information upon departure from office, as all such material shall remain under the U.S. Government's security control. Such persons may be authorized access to classified information they originated, reviewed, signed, received, or that was addressed to them while serving as an appointee or designee, provided that the DoD Component Head or senior agency official with classification jurisdiction for such information:

(1) Determines, in writing, that such access is clearly consistent with the interests of national security in view of the intended use of the material to which access is granted and by certifying that the requester has been found to be eligible for access pursuant to section 3 of this enclosure.

(2) Limits access to items that the person originated, reviewed, signed, or received while serving as a Presidential or Vice Presidential appointee or designee.

(3) Retains custody of the classified material at a DoD installation or activity or authorizes access to documents in the custody of the NARA.

(4) Obtains the requestor's agreement (SF 312) to safeguard the information and to submit any notes and manuscript for pre-publication review by all DoD Components and non-DoD departments or agencies with classification jurisdiction to determine that no classified information is contained therein.

f. Use of Classified Information in Litigation. DoDD 5405.2 (Reference (p)) governs the use of classified information in litigation.

g. Special Cases. When necessary in the interests of national security, the Heads of the DoD Components or their senior agency official may authorize access to classified information by persons outside the Federal government, other than those enumerated in section 5 of this enclosure and paragraphs 6.a through 6.f of this section. Prior to authorizing access, such official must determine that the recipient is reliable, loyal, and trustworthy for the purpose of accomplishing a national security objective; meets the requirements of section 3 of this enclosure; and can and will safeguard the information from unauthorized disclosure. The national security objective shall be stated in the authorization, which shall be in writing. This authority may not be further delegated.

7. VISITS. The Heads of the DoD Components shall establish procedures to accommodate visits to their Component facilities involving access to, or disclosure of, classified information. As a minimum, these procedures shall include verifying the identity, personnel security clearance, access (if appropriate), and need to know for all visitors.

a. Visit requests shall be processed and security clearance and access level verified using the Joint Personnel Adjudication System (JPAS) for DoD civilian, military, and contractor personnel whose access level and affiliation are reflected in JPAS. Fax, telephone, or other appropriate method shall be used for those personnel whose access level and affiliation are not reflected in JPAS.

b. Visits by foreign nationals to DoD Components and facilities, except for activities or events that are open to the public, shall be handled in accordance with DoDD 5230.20 (Reference (q)) and documented in the Foreign Visits System Confirmation Module.

8. PROTECTION WHEN REMOVED FROM STORAGE. An authorized person shall keep classified material removed from storage under constant surveillance. Classified document cover sheets (SF 703, "Top Secret (Cover sheet);" SF 704, "Secret (Cover sheet);" or SF 705 "Confidential (Cover sheet)") shall be placed on classified documents not in secure storage. The cover sheets show, by color and other immediately recognizable format or legend, the applicable classification level.

9. END OF DAY SECURITY CHECKS. The heads of activities that process or store classified information shall establish a system of security checks at the close of each duty and/or business day to ensure that any area where classified information is used or stored is secure. SF 701, "Activity Security Checklist," shall be used to record such checks. An integral part of the security check system shall be the securing of all vaults, secure rooms, and containers used for storing classified material. SF 702, "Security Container Check Sheet," shall be used to record such actions. SFs 701 and 702 shall be retained and disposed of as required by Component records management schedules.

10. EMERGENCY PLANS. Plans shall be developed to protect, remove, or destroy classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action, to minimize the risk of compromise, and for the recovery of classified information, if necessary, following such events. The level of detail and the amount of testing and rehearsal of these plans shall be determined by assessing the risk of hostile action, foreign intelligence threats, natural disaster, or terrorist activity that may place the information in jeopardy.

a. Use the requirements of Committee on National Security Systems (CNSS) Instruction 4004 (Reference (r)) when developing plans for the emergency protection (including emergency destruction under no-notice conditions) of classified communications security (COMSEC) material.

b. When preparing emergency plans, consider:

(1) Reducing the amount of classified material on hand.

(2) Storing less frequently used classified material at other secure locations.

(3) Creating regular back up copies of information in electronic formats for off-site storage.

(4) Transferring as much retained classified information to removable electronic media as possible, thereby reducing its bulk.

11. USE OF SECURE COMMUNICATIONS. In accordance with the requirements of Enclosure 4, classified information shall be transmitted only over secure communications circuits approved for transmission of information at the specified level of classification. This includes communication by telephone, facsimile, e-mail and other forms of electronic communications (e.g., messages, websites). See Volume 2 of this Manual for guidance on required markings.

12. REMOVAL OF CLASSIFIED INFORMATION FOR WORK AT HOME. When it is mission critical for individuals to remove classified information and materials (e.g., IT equipment and associated storage media) for work at home, specific security measures and approvals are required. Security measures appropriate for the level of classification must be in place to provide adequate protection and security-in-depth and to prevent access by unauthorized persons. Compliance with section 13 of Enclosure 4 of this Volume is also required.

a. Top Secret. Only the Secretary of Defense, the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commanders, or the senior agency officials appointed pursuant to section 5.4(d) of Reference (d) may authorize the removal of Top Secret information from designated working areas for work at home. Such officials may also authorize removal of information for work at home for any lower level of classification.

b. Secret and Confidential. The Heads of the DoD Components may authorize removal of Secret and Confidential information from designated working areas for work at home. This authority shall not be delegated below the major command or equivalent level.

c. Residential Storage Equipment. A General Services Administration (GSA)-approved security container shall be furnished for residential storage of classified information. Written procedures shall be developed to provide for appropriate protection of the information, including a record of the classified information that has been authorized for removal for work at home.

d. Classified IT Systems. See section 7 of Enclosure 7 of this Volume when classified IT equipment will be used. All residential classified network connections must be certified and accredited in accordance with DoDI 8510.01 (Reference (s)) requirements.

e. Foreign Country Restriction. Work at home may be authorized in foreign countries only when the residence is in a specific location where the United States enjoys extraterritorial status (e.g., on the embassy, chancery, or consulate compound) or on a U.S. military installation.

13. WORKING PAPERS. Working papers are documents (e.g., notes, drafts, prototypes) or materials (e.g., printer ribbons, photographic plates), regardless of the media, created during development and preparation of a finished product. Working papers and materials are not intended or expected to be disseminated. Working papers and materials containing classified information shall be:

a. Dated when created.

b. Marked with the highest classification of any information contained therein.

c. Safeguarded as required for the assigned classification.

d. Conspicuously marked "Working Paper" on the cover and/or first page of the document or material (or comparable location for special types of media) in letters larger than existing text.

e. Destroyed in accordance with chapter 33 of title 44, U.S.C. (Reference (t)) as implemented by DoDD 5015.2 (Reference (u)) and appropriate DoD Component implementing directives and records schedules when no longer needed.

f. Marked and controlled the same way as this Manual requires for finished products of the same classification when retained more than 180 days from date of origin (30 days for SAPs), filed permanently, e-mailed within or outside the originating activity, or released outside the originating activity, except as provided in paragraph 13.g. of this section.

g. Shared between action officers, either physically or electronically, without controlling them as permanent documents only when:

(1) The working materials are shared informally (e.g., collaborative documents or coordinating drafts) in the development process.

(2) Transfer or transmission of the material is via secure means and, if electronic, by means other than e-mail.

(3) All copies held by other than the originator are marked and controlled as required for finished products when retained more than 180 days of origin (30 days for SAPs). Consult with the originator for correct markings.

14. EQUIPMENT USED FOR PROCESSING CLASSIFIED INFORMATION. The Department of Defense has a variety of non-COMSEC-approved equipment that is used to process classified information. This includes copiers, facsimile machines, computers and other IT equipment and peripherals, display systems, and electronic typewriters. Activities shall identify those features, parts, or functions of equipment used to process classified information that may retain all or part of the information. Activity security procedures shall prescribe the appropriate safeguards to:

a. Prevent unauthorized access to that information, including by repair or maintenance personnel.

b. Ensure that repair procedures do not result in unauthorized dissemination of or access to classified information. Where equipment cannot be properly sanitized or appropriately knowledgeable escort provided, cleared maintenance technicians shall be used. Electronic repair or diagnostic equipment shall be maintained as classified material by the DoD Component if there is the potential for classified data transmission from the equipment being serviced. Use of remote diagnostic or repair capabilities shall be specifically approved and authorized in writing by the activity security manager; if the equipment retains or stores any classified information appropriate physical and logical protection must be provided on the remote end and secure communications are required.

c. Replace and destroy equipment parts in the appropriate manner when classified information cannot be removed. Removable disk drives, memory chips and boards, and other electronic components of copiers, fax machines, etc. may be sanitized or destroyed in the same manner as used for comparable computer equipment. Alternatively, the equipment shall be designated as classified and be retained and protected accordingly.

d. Ensure that appropriately knowledgeable, cleared personnel inspect equipment and associated media used to process classified information before the equipment is removed from protected areas to ensure there is no retained classified information. Classification markings and labels shall be removed from sanitized equipment and media after inspection, prior to removal from protected areas.

e. Ensure computers and other equipment used to process classified information or to transmit classified information across a network are certified and accredited in accordance with Reference (s) as required by DoDD 8500.01E (Reference (v)). Measures to protect against compromising emanations shall be implemented in accordance with DoDD C-5200.19 (Reference (w)).

15. REPRODUCTION OF CLASSIFIED MATERIAL. Paper copies, electronic files, and other material containing classified information shall be reproduced only when necessary for accomplishing the organization's mission or for complying with applicable statutes or Directives. Use of technology that prevents, discourages, or detects unauthorized reproduction of classified information is encouraged.

a. Unless restricted by the originating agency, Top Secret, Secret, and Confidential information may be reproduced, including by e-mailing, scanning, and copying, to the extent operational needs require.

b. The DoD Components shall establish procedures that facilitate oversight and control of the reproduction of classified information and the use of equipment for such reproduction, including controls that ensure:

(1) Reproduction is kept to a minimum consistent with mission requirements.

(2) Personnel reproducing classified information are knowledgeable of the procedures for classified reproduction and aware of the risks involved with the specific reproduction equipment being used and the appropriate countermeasures they are required to take.

(3) Reproduction limitations originators place on documents and special controls applicable to special categories of information are fully and carefully observed.

(4) Reproduced material is placed under the same accountability and control requirements as applied to the original material. Extracts of documents will be marked according to content and may be treated as working papers if appropriate.

(5) Reproduced material is conspicuously identified as classified at the applicable level and copies of classified material are reviewed after the reproduction process to ensure that the required markings exist.

(6) Waste products generated during reproduction are protected and destroyed as required.

(7) Classified material is reproduced only on approved and, when applicable, properly accredited systems. Section 14 of this enclosure provides additional guidance.

(8) Foreign government information (FGI) is reproduced and controlled pursuant to guidance and authority granted by the originating government.

16. CLASSIFIED MEETINGS AND CONFERENCES. Meetings and conferences involving classified information present special vulnerabilities to unauthorized disclosure. The Heads of the DoD Components shall establish specific requirements for protecting classified information at DoD Component-sponsored meetings and conferences, to include seminars, exhibits, symposia, conventions, training classes, workshops, or other such gatherings, during which classified information is disseminated.

a. DoD Component approval processes shall ensure that the following requirements are met:

(1) The meeting or conference serves a specified U.S. Government purpose.

(2) Use of other approved methods or channels for disseminating classified information or material are insufficient or impractical.

(3) The meeting or conference, or classified sessions thereof, takes place only at an appropriately cleared U.S. Government facility or a U.S. contractor facility that has an appropriate facility security clearance and, as required, secure storage capability, unless an exception is approved, in writing, in advance by the DoD Component Head or senior agency

official. Such exception authority shall not be delegated below the senior agency official. Requests for exceptions to permit use of facilities other than appropriately cleared U.S. Government or U.S. contractor facilities shall be submitted to the DoD Component Head or senior agency official in accordance with Component procedures. The request shall include a security plan that describes how the requirements of paragraphs 16.b and 16.d of this section shall be met.

(a) If classified meetings or conferences occur at a cleared U.S. contractor location, the contractor shall comply with all applicable portions of DoD 5220.22-M (Reference (x)) and parts 120 through 130 of title 22, CFR (Reference (y)) (also known as "The International Traffic in Arms Regulations"). DoD approval for the conduct of the meeting does not constitute authorization for presentation of export-controlled information when foreign nationals attend.

(b) The conduct of classified meetings or conferences at foreign installations and contractor sites is often subject to the rules and regulations of the host country, thus presenting additional security risks. Prior to approval of the conduct of such meetings, the DoD Component shall obtain assurances, in writing, that the responsible foreign government will agree to use security measures and controls that are at least as stringent as those required by this Manual. The provisions of paragraph 16.d. also shall be satisfied. To this end, assistance can be provided by the Director, International Security Programs, Defense Technology Security Administration, Office of the Under Secretary of Defense for Policy (OUSD(P)).

(c) Routine day-to-day meetings and gatherings of DoD officials shall be conducted only at an appropriately cleared U.S. Government or contractor facility. Exceptions shall not be granted for routine meetings.

(d) The provisions of this section do not apply to operational meetings conducted in combat situations, classes conducted by DoD schools, or gatherings of personnel of a DoD Component and foreign government representatives or U.S. and/or foreign contractor representatives on a matter related to a specific U.S. Government contract, program, or project.

(4) Classified sessions are segregated from unclassified sessions.

(5) Access to the meeting or conference, or specific sessions thereof, where classified information may be discussed or disseminated is limited to persons who possess an appropriate security clearance and need to know.

(6) Any participation by foreign nationals or foreign representatives complies with requirements of Reference (q) and DoDD 5230.11 (Reference (z)) (e.g., the responsible U.S. Government foreign disclosure office(s) assures, in writing, that the information to be presented has been approved for disclosure to the represented foreign countries).

(7) Announcement of the meeting or conference is unclassified and limited to a general description of topics expected to be presented, names of speakers, logistical information, and administrative and security instructions.

(8) Procedures shall ensure that classified information, documents, recordings, audiovisual material, information systems, notes, and other materials created, distributed, or used during the meeting are controlled, safeguarded, and transported as provisions of this Manual require. Recording or taking notes, including notes on classified electronic devices, during classified sessions shall be permitted only when it is determined that such action is necessary to fulfill the U.S. Government purpose for the meeting.

(9) Information systems used during the meeting or conference to support creation or presentation of classified information shall meet all applicable requirements for processing classified information, including as appropriate considerations of technical security countermeasures (TSCM). Unclassified laptop computers, handheld information technologies (e.g., personal electronic devices (PEDs)), and other similar devices shall not be used for note taking during classified sessions. Use of classified computers and other electronic devices shall be permitted only when needed to meet the intent of the meeting or conference and appropriate protection and TSCM requirements have been met.

b. The DoD activity sponsoring a classified meeting or conference shall assign an official to serve as security manager for the meeting and be responsible for ensuring that, at a minimum, the following security provisions are met:

(1) Attendees are briefed on safeguarding procedures.

(2) Entry is controlled so that only authorized personnel gain entry to the area. Particular caution shall be taken to ensure that any individual who is not authorized to attend the classified session(s) is denied entry thereto.

(3) The perimeter is controlled to ensure unauthorized personnel cannot overhear classified discussions or introduce devices that would result in the compromise of classified information.

(4) Escorts are provided for uncleared personnel who are providing services to the meeting or conference (e.g., setting up food or cleaning) when classified presentations and/or discussions are not in session.

(5) Use of cell phones, PEDs, 2-way pagers, and other electronic devices that transmit is prohibited.

(6) Classified notes and handouts are safeguarded in accordance with Enclosure 3.

(7) Classified information is disclosed to foreign nationals only in accordance with the provisions of Reference (z).

(8) An inspection of the room(s) is conducted at the conclusion of the meeting or conference (or at the end of each day of a multi-day event) to ensure all classified materials are properly stored.

c. Appropriately cleared U.S. Government contractor personnel may provide administrative support and assist in organizing a classified meeting or conference, but the DoD Component sponsoring the gathering remains responsible for all security requirements.

d. Facilities other than appropriately cleared U.S. Government or U.S. contractor facilities proposed for use for classified meetings and conferences shall:

(1) Not be open to the public and access shall be controlled by the U.S. Government or cleared contractor through a 100 percent identification card check at the perimeter point. For a military installation or comparably protected Federal government compound, this can be at the perimeter fence of the installation or compound.

(2) Have the room(s) where the classified sessions are to be held located away from public areas so that access to the room(s), walls, and ceiling(s) can be completely controlled during the classified sessions.

(3) Provide authorized means to secure classified information in accordance with Enclosure 3.

(4) Meet the DoD antiterrorism standards specified by DoDI 2000.16 (Reference (aa)).

(5) Be subject to TSCM surveys in accordance with DoDI 5240.05 (Reference (ab)). When addressing this requirement, TSCM security classification guidance MUST be consulted to ensure proper classification of meeting details when associated with the use of TSCM.

e. Not later than 90 days following the conclusion of a classified meeting or conference for which an exception was granted, the sponsoring activity shall provide an after-action report to the DUSD(I&S) through the approving DoD Component Head or senior agency official. The after-action report shall be a brief summary of any issues or threats encountered during the event and actions taken to address the situation.

17. SAFEGUARDING FGI

a. North Atlantic Treaty Organization (NATO) Information. NATO classified information shall be controlled and safeguarded according to United States Security Authority for NATO Instruction 1-07 (Reference (ac)).

b. Other FGI. See the Glossary for the definition of FGI.

(1) To avoid inadvertent compromise, classified FGI shall be stored in a manner that will avoid commingling with other material. For small volumes of material, separate files in the same vault, container, or drawer will suffice.

(2) FGI shall be re-marked if needed to ensure the protective requirements are clear. FGI may retain its original classification if it is in English. However, when the foreign

government marking is not in English, or when the foreign government marking requires a different degree of protection than the same U.S. classification designation, a U.S. marking that results in a degree of protection equivalent to that required by the foreign government shall be applied. See Appendix 1 to Enclosure 4 of Volume 2 of this Manual for comparable U.S. classification designations.

(3) U.S. documents containing FGI shall be marked as required by section 9 of Enclosure 4 of Volume 2 of this Manual. The foreign government document or authority on which derivative classification is based must be identified on the "Derived from:" line, in addition to the identification of any U.S. classification authority. A continuation sheet should be used for multiple sources, if necessary. A U.S. document containing FGI cannot be declassified or downgraded below the highest level of FGI contained in the document without the written permission of the foreign government or international organization that originated the information.

(4) Security clearances issued by the U.S. Government are valid for access to classified FGI of a comparable level.

(5) The transmission of FGI within the United States among U.S. Government agencies and U.S. contractors and between U.S. contractors with a need to know must be in accordance with this Manual and Reference (x).

(6) The international transfer of foreign government classified information must be by government officials through government-to-government channels, or channels agreed upon in writing by the originating and receiving governments (collectively "government-to-government transfer"). See Enclosure 4 and its Appendix for further guidance on transfer of classified information.

(7) The receiving DoD Components shall protect FGI to at least a degree equivalent to that required by the foreign government or international organization that provided the information. FGI shall be controlled and safeguarded in the same manner as prescribed for U.S. classified information, except as described below. The control and safeguarding requirements for FGI may be modified as permitted by a treaty or international agreement, or, for foreign governments with which there is no treaty or international agreement, through formal written agreement between the responsible national security authorities or designated security authorities of the originating and receiving governments (hereafter referred to collectively as designated security authorities (DSAs)). The Under Secretary of Defense for Policy (USD(P)) serves as the DSA.

(a) Control of Foreign Government Top Secret Information. Maintain records for 5 years of the receipt, internal distribution, destruction, annual inventory, access, reproduction, and transmittal of foreign government Top Secret information. Reproduction requires the consent of the originating government. Destruction shall be witnessed.

(b) Control of Foreign Government Secret Information. Maintain records for 3 years of the receipt, distribution, external dispatch, reproduction, and destruction of material

containing foreign government Secret information. Other records may be necessary if the originator requires. Secret FGI may be reproduced to meet mission requirements.

(c) Control of Foreign Government Confidential Information. Maintain records for 2 years for the receipt and external dispatch of Confidential FGI. Do not maintain other records for foreign government Confidential information unless required by the originating government. Confidential FGI may be reproduced to meet mission requirements.

(d) Foreign Government Restricted Information and Information Provided in Confidence. In order to ensure the protection of Restricted FGI or foreign government unclassified information provided in confidence, such information shall be classified in accordance with Reference (d) which states that unauthorized disclosure of FGI is presumed to cause damage to the national security. If the foreign protection requirement is lower than the protection required for U.S. Confidential information, the information shall be marked "CONFIDENTIAL-Modified Handling" as described in Volume 2, Enclosure 4, paragraph 4.c of this Manual and the following requirements shall also be met:

1. The information shall be provided only to those individuals who have an established need to know, and where access is required by official duties.

2. Individuals given access shall be notified of applicable handling instructions. This may be accomplished by a briefing, written instructions, or by applying specific handling requirements to an approved cover sheet.

3. Documents shall be stored to prevent unauthorized access (e.g., a locked desk or cabinet or a locked room to which access is controlled).

4. DoD Components and contractors performing on DoD contracts shall handle documents bearing the marking "UK RESTRICTED" as classified in accordance with subparagraph 17.b.(7)(d). The provision in the U.S./United Kingdom (UK) Security Implementing Arrangement (Reference (ad)) that allows documents marked "UK RESTRICTED" to be handled in a manner similar to For Official Use Only (FOUO) information applies ONLY to DoD contactors operating under COMMERCIAL contracts with the UK and, pursuant to the agreement, the UK must include in the applicable contract its requirements for the marking and handling of the information. The provision does NOT apply to, nor permit, such handling of UK RESTRICTED information by DoD Components or by contractors when performing on DoD contracts.

(8) FGI shall not be disclosed to nationals of third countries, including foreign nationals who are protected individuals or permanent resident aliens, or to any other third party, or used for other than the purpose for which the foreign government provided it without the originating government's written consent. Questions regarding releasability or disclosure should be directed to the U.S. originator, who will consult with the foreign government as required. Contractors will submit their requests through the contracting U.S. Government agency for U.S. contracts and the Defense Security Service for direct commercial contracts. Approval from the originating government does not eliminate the requirement for the contractor to obtain an export

authorization as required by other regulations or policies.

18. ALTERNATIVE COMPENSATORY CONTROL MEASURES (ACCM). A Head of a DoD Component with original classification authority (OCA) may employ ACCM when he or she determines that the standard security measures detailed in this Manual are insufficient to enforce need to know for classified information and SCI or SAP protections are not warranted. The use of an unclassified nickname, obtained in accordance with Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3150.29C (Reference (ae)), together with a list of persons authorized access, and a specific description of information subject to the enhanced ACCM controls, are the three requisite elements of an ACCM.

a. DoD Proponents for ACCM. The DoD staff proponent for ACCM management, oversight and Congressional reporting is the OUSD(P). The proponent for ACCM security policy is the Office of the Under Secretary of Defense for Intelligence (OUSD(I)). Given this sharing of ACCM responsibilities, staff elements in OUSD(P) and OUSD(I) shall implement mechanisms that ensure transparency of all ACCM actions.

b. ACCM Approval. A Head of a DoD Component may approve ACCM use for classified information over which they have cognizance. Prior to approving the establishment of an ACCM, the criticality, sensitivity, and value of the information; analysis of the threats both known and anticipated; vulnerability to exploitation; and a countermeasures cost benefits analysis shall be assessed.

c. Guidance on ACCM Use. Use of ACCM must be consistent with the following guidance:

(1) ACCM may be used to assist in enforcing need to know for classified DoD intelligence matters. The DoD Component Head establishing or terminating any such ACCM shall provide written notification within 30 days to the Director of Security, OUSD(I), and the Director, Special Programs, OUSD(P), who shall maintain this information as long as the ACCM is in use.

(2) ACCM may be used to assist in enforcing need to know for classified operations, sensitive support, and other non-intelligence activities. The DoD Component Head establishing or terminating any such ACCM shall provide written notification within 30 days to the Director, Special Programs, OUSD(P), for review. The Director, Special Programs, OUSD(P), shall maintain this information as long as the ACCM is in use.

(3) ACCM shall not be used for acquisition programs or activities progressing through the acquisition process.

(4) DoD Components shall obtain an unclassified nickname consistent with Reference (ae) and coordinate with OUSD(P) to preclude duplication of nicknames.

(5) A roster or listing of all persons accessed to the ACCM shall be maintained by the ACCM control officer (see subparagraph 18.f.(1)(c) of this section). The access roster will differentiate between those persons actively accessed and those whose accesses are currently

inactive.

(6) ACCM documents and materials shall be marked as specified in Enclosure 4 of Volume 2 of this Manual.

(7) Heads of DoD Components must establish and maintain a system that provides for recurrent inspection of the ACCM they have approved. This mechanism shall ensure compliance with the provisions of this Manual. Each ACCM shall be overseen and inspected on a recurrent basis by the ACCM sponsor or OUSD(P).

d. Prohibited Security Measures. The application of the following security measures with ACCM material is prohibited:

(1) Using personnel security investigative or adjudicative standards that are more stringent than those normally required for a comparable level of classified information to establish access eligibility to ACCM-protected information.

(2) Using code words as defined in Reference (ae).

(3) Using trigraphs, digraphs, or other abbreviations of the approved nickname.

(4) Using specialized non-disclosure agreements or any certificates of disclosure or non-disclosure for ACCM access.

(5) Using a billet structure or system to control the position or numbers of persons afforded ACCM access.

e. Prohibited Uses of ACCM. The following uses of ACCM are prohibited:

(1) Using ACCM for NATO or non-intelligence FGI. For NATO, exceptions to this limitation can be granted only by the Secretary of Defense. For non-intelligence FGI, exceptions to this limitation can be granted only by the USD(P). Request for exceptions shall be forwarded to the Director, International Security Programs, Defense Technology Security Administration, OUSD(P), for action. Such approvals must be documented and retained by the sponsor.

(2) Using ACCM to protect classified information in acquisition programs as defined in DoDD 5000.01 (Reference (af)).

(3) Using ACCM to protect technical or operational requirements of systems in the acquisition process. Systems in operational use are not viewed as being in the acquisition process. Components of operational systems are fielded end items, not items in the acquisition process, and improvements to fielded items are eligible for ACCM status if properly justified.

(4) Using ACCM to protect Restricted Data (RD), Formerly Restricted Data (FRD), COMSEC, SCI, SAP, or Nuclear Command and Control Extremely Sensitive Information.

(5) Using ACCM to protect unclassified information.

(6) Using ACCM to preclude or impede congressional, OSD, or other appropriate oversight of programs, command functions, or operations.

(7) Using ACCM to justify funding to procure or maintain a separate ACCM communication system.

f. Documentation

(1) Use of ACCM must be approved in writing by the cognizant DoD Component Head. The correspondence establishing the ACCM shall be signed by the DoD Component Head and shall include the following information:

(a) Unclassified nickname assigned in accordance with Reference (ae).

(b) Designation of the ACCM sponsor. As a minimum, the sponsor shall be a general or flag officer, or senior executive equivalent, who has OCA at the level of or higher than the information protected by the ACCM.

(c) Designation of an ACCM control officer who shall be the organization's point of contact for all matters concerning the ACCM. Subsequent changes in designated personnel shall be provided, in writing, to the Special Programs Office, OUSD(P).

(d) Description of the essential information to be protected by the ACCM.

(e) Effective activation date and expected ACCM duration.

(f) Any planned participation by foreign partners.

(2) The ACCM sponsor shall develop and distribute a program security plan, security classification guide, and program participant briefing to all participating organizations prior to the activation of the ACCM. As a minimum, the briefing will address the specific information that is subject to ACCM security measures.

(3) The Special Programs Office, OUSD(P), shall maintain a central repository of records for all DoD ACCM.

g. Annual Reports of ACCM Use. Not later than December 15 of each year, the DoD Components shall provide a report to OUSD(P) on all ACCM usage during the previous year. The exact format for this report shall be provided annually by OUSD(P), however, the general data elements include: ACCM nickname; purpose and/or description of the ACCM program; expected duration; and ACCM sponsor and ACCM control officer(s).

h. Sharing ACCM-Protected Information. ACCM-protected information may be shared with

other DoD Components and/or other Federal government departments and agencies only when the recipient organization agrees to abide by the ACCM security requirements stipulated in this enclosure.

i. Contractor Access to ACCM. DoD contractors may participate in ACCMs, or be directed to participate, only when such access and the associated security plan are identified in the DD Form 254, "Contract Security Classification Specification." Care must be taken to ensure identification of the security plan does not disclose ACCM-protected data.

j. Program Maintenance

(1) ACCM sponsors shall maintain an updated listing of primary and alternate ACCM control officers for each organization to which they have extended their program.

(2) Each organization's ACCM control officer shall maintain an updated ACCM access control list for their organization.

(3) Initial contact between organizations will be between each organization's ACCM control officers. ACCM control officers may authorize action officer to action officer contact once access control lists have been exchanged between organizations.

(4) Personnel requiring access to ACCM-protected information shall receive specialized training upon initial access to the program and annually thereafter. Training, as a minimum, shall address the procedures for access, control, transmission, storage, and marking. Individuals may be required to sign an acknowledgement of training should the security plan so specify.

(5) ACCM documentation (i.e., program security plan and security classification guide) must be updated a minimum of once every 5 years.

(6) ACCM sponsors shall provide the following information, through the DoD Component Head, to OUSD(P) concurrently with the ACCM annual report:

(a) A listing of primary and alternate ACCM control officers for each organization managing an ACCM.

(b) Any updated ACCM documentation or confirmation that program documentation has been reviewed and is current.

k. Safeguarding ACCM Information. The provisions of this Manual regarding the safeguarding of classified information are modified with respect to use of ACCM as follows:

(1) Top Secret, Secret, and Confidential cover sheets (i.e., SFs 703, 704, and 705, respectively) used to cover ACCM material shall be over stamped or marked with "ACCM" and the appropriate nickname. Cover sheets specifically designated by the DoD Components for use with ACCM must be approved by the Director of Security, OUSD(I), prior to use.

(2) ACCM material should be handled and stored based on the security classification of the information contained therein and in a manner that separates it from non-ACCM classified information. Separate GSA approved storage containers are not required so long as everyone with access to container is also approved for access to the ACCM material stored within, but the measures used (e.g., segregated files, separate folders, drawers labeled for ACCM) shall prevent the commingling of ACCM material with other classified documents.

(3) ACCM information shall be transmitted in the same manner as other classified information at the same classification level with the following exceptions:

(a) ACCM information packaged for transmission shall have the inner envelope marked with the appropriate classification, the caveat "ACCM," and the assigned nickname, and shall be addressed to the attention of an individual authorized access to the ACCM information.

(b) The ACCM nickname shall be used in the text of message traffic and on cover sheets accompanying secure facsimile transmissions to assist in alerting the recipient that the transmission involves ACCM-protected information. Senders shall ensure that an authorized recipient is awaiting the transmission when sending via secure facsimile. When using the Defense Message System (DMS), the material must also be marked as "SPECAT" (Special Category) in accordance with the requirements and procedures in CJCSM 5720.01B (Reference (ag)). Due to limits in DMS processing, only one ACCM nickname should be used in a DMS message.

(c) Automated information systems or electronic files containing ACCM protected information shall be configured with appropriate discretionary access controls to ensure that access is restricted to individuals with authorized access.

(d) Secret Internet Protocol Router Network (SIPRNET) or other secure transmission methods authorized for processing information at the required level of classification may be used to transmit ACCM information. Each such transmission must be marked with the caveat "ACCM" and the authorized nickname in accordance with the marking guidance in Volume 2 and transmitted only to those authorized access to the ACCM information.

(e) The method of transmission selected for ACCM information, whether in hardcopy or electronic form, shall be consistent with the security classification assigned. Designation of information as requiring ACCM protection does not, in and of itself, require the transmission of the information by methods usually reserved for a higher level of classified information.

l. Security Incidents. Compromise of ACCM program information can present an immediate and real threat to national security and those personnel involved in mission execution. Anyone finding ACCM material out of proper control shall take actions to safeguard the material and shall immediately notify the local ACCM control officer, if known, or the local security manager.

(1) All reporting, inquiry, investigation, and damage assessment will be conducted per

the guidelines contained in Enclosure 6 of this Volume. Any reports containing ACCM information shall be handled in accordance with the requirements of this Manual as modified by this section.

(2) Section 13 of Enclosure 6 of this Volume states the actions to take if unauthorized personnel are inadvertently afforded access to ACCM information. Inadvertent disclosure forms, commonly used with compartmented information, are not authorized for use with ACCM information.

(3) Because ACCM program information is not SCI or SAP, reasonable risk management procedures should be followed when ACCM program information is incorrectly placed on non-approved electronic processing systems or electronically transmitted to non-authorized personnel and/or systems. Deleting the file or material from all affected systems is normally a sufficient action unless the material in question is classified at a higher level of classification than that for which the system is accredited.

(4) The ACCM sponsor should be notified when the local inquiry and investigation is completed. Resolution will be in accordance with current guidance contained in Enclosure 6 of this Volume and must consider the guidance contained in the ACCM program security plan. Responsibility for the damage assessment remains with the ACCM sponsor. Any additional action will be as directed by the ACCM sponsor and the local security manager.

m. ACCM Termination. ACCM shall be terminated by the establishing DoD Component when ACCM security measures are no longer required. Notification of ACCM termination must be submitted, in writing, as required by paragraphs 18.c.(1) and 18.c.(2) of this enclosure.

n. Transitioning an ACCM to a SAP. If, at any point in time, the DoD Component Head determines that information protected by ACCM requires further protection as a SAP, authorization to establish a DoD SAP must be requested in accordance with DoD Directive 5205.07 (Reference (ah)).

Army Regulation 380–67

Security

Personnel Security Program

Headquarters
Department of the Army
Washington, DC
24 January 2014

UNCLASSIFIED

SUMMARY of CHANGE

AR 380–67
Personnel Security Program

This rapid action revision, dated 24 January 2014--

- Revises criteria for application of security standards (para 2-4*q*).
- Incorporates the provisions to provide procedural benefits to afford individuals an opportunity to appeal a final adjudicative decisions to a higher level authority (para 8-6*d*).
- Adds performance measures (para 11-5).
- Rescinds appendix on reporting of nonderogatory cases (app E).
- Deletes appendix on guidelines for conducting prenomination personal interviews (app G).
- Deletes appendix on the list of designated countries (app H).
- Updates the National Adjudicative Guidelines (app I).
- Adds internal control evaluation (app M).

Headquarters
Department of the Army
Washington, DC
24 January 2014

*Army Regulation 380–67

Effective 24 February 2014

Security

Personnel Security Program

By Order of the Secretary of the Army:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

GERALD B. O'KEEFE
Administrative Assistant to the Secretary of the Army

History. This publication is a rapid action revision. The portions affected by this rapid action revision are listed in the summary of change.

Summary. This regulation implements the DOD and Department of the Army Personnel Security Program and takes precedence over all other departmental issuances affecting these programs. It contains the policies and procedures for access to classified information and assignment in a sensitive position. It also prescribes the investigative scope and adjudicative standards and criteria that are necessary prerequisites for such access or employment. It includes due process procedures for appealing adverse administrative actions rendered in accordance with the provisions of this regulation. This regulation contains all of DOD 5200.2–R and includes all recommendations of the Commission to Review DOD Security Policies and Practices (Stilwell Commission) approved for implementation. Army implementing instructions in this regulation are set in boldface type.

Applicability. This regulation applies to the active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. Also, it applies only to Army contractor personnel who require access to sensitive compartmented information in the performance of their duties.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff, G–2. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Army internal control process. This regulation contains internal control provisions in accordance with AR 11–2 and identifies key internal controls that must be evaluated (see appendix M).

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Deputy Chief of Staff, G–2, 1000 Army Pentagon, Washington, DC 20310–1000.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Deputy Chief of Staff, G–2, 1000 Army Pentagon, Washington, DC 20310–1000.

Distribution. This regulation is available in electronic media only and is intended for command levels A, B, C, D, and E for the active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

*This regulation supersedes AR 380–67, dated 9 September 1988.

e. If geographical and political situations prevent the full completion of the BI (and/or counterintelligence-scope polygraph), issuance of an LAA shall not be authorized; exceptions to the policy may only be authorized by the DUSD(P).

f. A report on all LAAs in effect, including the data required in paragraphs *b*(l) through (6), above, shall be furnished to the DUSD(P), **DCSINT (DAMI–CIS),** within **30** days after the end of each fiscal year (See para 11–102.)

3–23. Access by persons outside the executive branch

a. Access to classified information by persons outside the executive branch shall be accomplished in accordance with chapter VII, DOD 5200.1–R **(AR 380–5)**. The investigative requirement shall be the same as for the appropriate level of security clearance, except as indicated below.

b. Members of the U.S. Senate and House of Representatives do not require personnel security clearances, They may be granted access to DOD classified information which relates to matters under the jurisdiction of the respective committees to which they are assigned and is needed to perform their duties in connection with such assignments.

c. Congressional staff members requiring access to DOD classified information shall be processed for a security clearance in accordance with DODD 5142.1 and the provisions of this regulation. The Director, Washington Headquarters Services (WHS), will initiate the required investigation (initial or reinvestigation) to DIS, adjudicate the results and grant, deny or revoke the security clearance, as appropriate. The Assistant Secretary of Defense (Legislative Affairs) will be notified by WHS of the completed clearance action.

d. State Governors do not require personnel security clearances. They may be granted access to specifically designated classified information, on a"need-to-know" basis, based upon affirmation by the Secretary of Defense, **the Secretary of the Army (SA), or the Deputy Chief of Staff, G–2 (DCS, G–2)** that access, under the circumstances, serves the national interest. Staff personnel of a Governor's office requiring access into classified information shall be investigated and cleared in accordance with the prescribed procedures of this regulation when the head of a DOD component or single designee, **the SA, or the DCS, G–2** affirms that such clearance serves the national interest. Access shall also be limited to specifically designated classified information on a"need-to-know" basis. **Requests for access by State Governors and/or the staff of a Governor's office will be submitted to HQDA (DAMI–CIS.)**

e. Members of the U.S. Supreme Court, the Federal judiciary and the Supreme Courts of the individual States do not require personnel security clearances. They may be granted access to DOD classified information to the extent necessary to adjudicate cases being heard before these individual courts.

f. Attorneys representing DOD military, civilian or contractor personnel, requiring access to DOD **or DA** classified information to properly represent their clients, shall normally be investigated by DIS and cleared in accordance with the prescribed procedures in paragraph 3–19. This shall be done upon certification of the General Counsel of the DOD component involved in the litigation **or Office of The Judge Advocate General** that access to specified classified information, on the part of the attorney concerned, is necessary to adequately represent their client. In exceptional instances, when the exigencies of a given situation do not permit timely compliance with the provisions of paragraph 3–19, access may be granted with the written approval of an authority designated in **paragraph F–1,** appendix F, provided that as a minimum: (a) a favorable name check of the FBI and the DCII has been completed, and (b) a DOD Non-Disclosure Agreement has been executed. **Requests for access for attorneys representing DA military, civilian, or contractor personnel will be submitted through the Office of The Judge Advocate General (DAJA–AL), Washington, DC 20310–2212 to the Office of The Deputy Chief of Staff for Intelligence (DAMI–CIS), Washington, DC 20310–1056.** In postindictment cases, after a judge has invoked the security procedures of **PL 96–456, Stat. 2025,** the Classified Information Procedures Act (CIPA), the Department of Justice may elect to conduct the necessary BI and issue the required security clearance, in coordination with the affected DOD component **or the DA.**

3–24. Restrictions on issuance of personnel security clearances

Personnel security clearances must be kept to the absolute minimum necessary to meet mission requirements. Personnel security clearances shall *not* be issued:

a. To persons in nonsensitive positions.

b. To persons whose regular duties do not require authorized access to classified information.

c. For ease of movement of persons within a restricted, controlled, or industrial area, whose duties do not require access to classified information.

d. To persons who may only have inadvertent access to sensitive information or areas, such as guards, emergency service personnel, firemen, doctors, nurses, police, ambulance drivers, or similar personnel.

e. To persons working in shipyards whose duties do not require access to classified information.

f. To persons who can be prevented from accessing classified information by being escorted by cleared personnel.

g. To food service personnel, vendors and similar commercial sales or service personnel whose duties do not require access to classified information.

h. To maintenance or cleaning personnel who may only have inadvertent access to classified information unless such access cannot be reasonably prevented.