

AMERICAN CIVIL LIBERTIES UNION)
AND AMERICAN CIVIL LIBERTIES)
UNION FOUNDATION,)
)
Petitioners,) U.S.C.M.C.R. Case No. 13-003
)
v.)
)
UNITED STATES OF AMERICA,)
)
Respondent.) DATE: March 7, 2013

APPENDIX TO RESPONSE TO PETITION FOR A WRIT OF MANDAMUS

TABLE OF CONTENTS

Tab	Description	App. Pages
1	AE 013 - Government Motion To Protect Against Disclosure of National Security Information (Apr. 26 2012)	1-46
2	AE 013A - Motion of the American Civil Liberties Union for Public Access to Proceedings and Records (May 2, 2012)	47-82
3	AE 013D - Government's Response To the American Civil Liberties Union Motion for Public Access to Proceedings and Records (May 16, 2012)	83-97
4	AE 013F - Response/Opposition by 14 News Organizations to Government's Motion to Protect Against Disclosure of National Security Information (AE013) and Cross-Motion to Enforce Public Access Rights (May 16, 2012)	98-125
5	AE 013H - Reply of the American Civil Liberties Union to the Government's Response to the Motion for Public Access to Proceedings and Records (May 23, 2012)	126-137
6	AE 013L - Government's Supplemental Motion For Modified Order To Protect Against Disclosure of National Security Information (Sept. 26, 2012)	138-163
7	AE 013N - Response of the American Civil Liberties Union to Government's Supplemental Motion for Modified Order to Protect Against Disclosure of National Security Information (Oct. 12, 2012)	164-170
8	Excerpt of Unofficial/Unauthenticated Transcript (Oct. 17, 2012)	171-315
9	AE 013O – Ruling on Government Motion To Protect Against Disclosure of National Security Information (Dec. 6, 2012)	316-320
10	AE 013P – Protective Order #1 (Dec. 6, 2012)	321-340
11	AE 013Z – Supplemental Ruling on Government Motion To Protect Against Disclosure of National Security Information (Feb. 9, 2013)	341-344
12	AE 013AA – Amended Protective Order #1 (Feb. 9, 2013)	345-362
13	Modified Protective Order Pertaining to Classified Information, <i>United States v. Ghailani</i> , No. 98 CR 1023 (S.D.N.Y. July 21, 2009)	363-383
14	Executive Order No. 13,526, 75 Fed. Reg. 707 (Dec. 29, 2009)	384-409

Tab 1

MILITARY COMMISSIONS TRIAL JUDICIARY
GUANTANAMO BAY, CUBA

<p>UNITED STATES OF AMERICA</p> <p>v.</p> <p>KHALID SHAIKH MOHAMMAD, WALID MUHAMMAD SALIH MUBARAK BIN ATTASH, RAMZI BINALSHIBH, ALI ABDUL AZIZ ALI, MUSTAFA AHMED ADAM AL HAWSAWI</p>	<p>AE013</p> <p>Government Motion To Protect Against Disclosure of National Security Information</p> <p>26 April 2012</p>
---	--

1. **Timeliness.** This motion is timely filed under Rule for Military Commissions (R.M.C.) 905(b) and Military Commissions Trial Judiciary Rule of Court 3.6.a.
2. **Relief Sought.** The Government respectfully requests that the Military Judge issue the attached proposed Protective Order to protect classified information in connection with this case. *See* 10 U.S.C. § 949p-3; Military Commission Rule of Evidence (M.C.R.E.) 505(e).
3. **Overview.** This military commission will involve classified information that must be protected throughout all stages of the proceedings, including the upcoming arraignment of the Accused. As discussed in the attached declarations from the Central Intelligence Agency (CIA), the Department of Defense (DoD), and the Federal Bureau of Investigation (FBI), filed herewith under seal, the substance of the classified information in this case deals with the sources, methods, and activities by which the United States defends against international terrorist organizations. Attachment A, Classified Declaration of David H. Petraeus, Director, Central Intelligence Agency, dated 7 April 2012 (Petraeus Decl.); Attachment B, Classified Declaration

UNCLASSIFIED//FOUO WHEN SEPARATED FROM CLASSIFIED
ATTACHMENTS A THROUGH D (FILED UNDER SEAL)

of Information Review Officer, Central Intelligence Agency, dated 12 April 2012 (CIA Decl.); Attachment C, Classified Declaration of General Douglas M. Fraser, United States Air Force, Commander, United States Southern Command, dated 24 October 2011 (SOUTHCOM Decl.); Attachment D, Classified Declaration of Mark F. Giuliano, Assistant Director, Counterterrorism Division, Federal Bureau of Investigation, dated 7 September 2011 (FBI Decl.). The Military Commissions Act, 10 U.S.C. § 948a, *et seq.* (M.C.A.), specifically protects classified information, the disclosure of which would be detrimental to national security. 10 U.S.C. § 949p-1. The Government moves the Military Judge, pursuant to the M.C.A., to enter the attached proposed Protective Order to protect classified information in this case. *See* Attachment E.

4. **Burden of Proof.** As the moving party, the Government bears the burden of demonstrating by a preponderance of the evidence that the requested relief is warranted. R.M.C. 905(c); M.C.R.E. 505(e) (“Upon motion of the trial counsel, the military judge shall issue an order to protect against the disclosure of any classified information that has been disclosed by the United States to any accused or counsel, regardless of the means by which the accused or counsel obtained the classified information, in any military commission [under the M.C.A.] or that has otherwise been provided to, or obtained by, any such accused in any such military commission”).

5. **Facts**

a. This case involves classified information that deals with the sources, methods, and activities by which the United States defends against international terrorist organizations, including al Qaeda and its affiliates. *See, e.g.*, [REDACTED] SOUTHCOM Decl. ¶ 12; FBI Decl. ¶ 10.

b. On 11 September 2001, a group of Al Qaeda operatives hijacked four civilian airliners in the United States. After the hijackers killed or incapacitated the airline pilots, a pilot-

hijacker deliberately slammed American Airlines Flight 11 into the North Tower of the World Trade Center in New York, New York. A second pilot-hijacker intentionally flew United Airlines Flight 175 into the South Tower of the World Trade Center. Both towers collapsed soon thereafter. Hijackers also deliberately slammed a third airliner, American Airlines Flight 77, into the Pentagon in Northern Virginia. A fourth hijacked airliner, United Airlines Flight 93, crashed into a field in Shanksville, Pennsylvania, after passengers and crew resisted the hijackers and fought to reclaim control of the aircraft. A total of 2,976 people were murdered as a result of Al Qaeda's 11 September 2001 attacks on the United States. Numerous other civilians and military personnel were also injured. Al Qaeda leadership praised the attacks, vowing that the United States would not "enjoy security" until al Qaeda's demands were met. The United States Congress responded on 18 September 2001 with an Authorization for Use of Military Force.

c. On 31 May 2011 and 26 January 2012, pursuant to the Military Commissions Act of 2009, charges in connection with the 11 September 2001 attacks were sworn against Khalid Shaikh Mohammad (Mohammad), Walid Muhammad Salih Bin Attash (Bin Attash), Ramzi Binalshibh (Binalshibh), Ali Abdul Aziz Ali (Ali), and Mustafa Ahmed Adam al Hawsawi (Hawsawi). These charges were referred jointly to this capital Military Commission on 4 April 2012. The accused are each charged with Conspiracy, Attacking Civilians, Attacking Civilian Objects, Intentionally Causing Serious Bodily Injury, Murder in Violation of the Law of War, Destruction of Property in Violation of the Law of War, Hijacking an Aircraft, and Terrorism.

(1) More specifically, Mohammad is alleged, among other things, to be the architect of the 9/11 concept. Once Usama bin Laden approved his plan, Mohammad oversaw its development and logistical progress to fruition. Mohammad also is accused of providing personal training and guidance to the hijackers. He is further charged with

attending a meeting in late 2001, during which Osama bin Laden confirmed al Qaeda's involvement in the 9/11 attacks in a videotaped message.

(2) Bin Attash, in part, is accused of being instrumental in establishing the means by which the al Qaeda hijackers ultimately were able to smuggle weapons onboard civilian airliners. Bin Attash also is alleged to have facilitated the transit of two hijackers into the United States, as well as provide them personal training in hand-to-hand combat. Bin Attash is further accused of attempting to apply for a visa that would allow him to travel to the United States.

(3) After leaving Hamburg, Germany, Binalshibh is alleged to have traveled to Afghanistan to attend an al Qaeda training camp and attempted, on multiple occasions, to become a pilot-hijacker along with co-conspirators Mohammed Atta (Atta), Marwan al Shehhi (Shehhi), and Ziad Jarrah (Jarrah). Binalshibh, among other things, is also alleged to have ultimately become the primary coordinator and communications hub between Mohammad and Atta.

(4) Ali, in part, is charged with having transferred more than \$100,000 to hijackers located within the United States for their living expenses and flight training. Ali also is alleged to have attempted to obtain a United States visa in order to become a hijacker for the 9/11 operation. He further is accused of facilitating travel to the United States for many of the hijackers as well as obtaining flight training materials for their use.

(5) Hawsawi, among other things, is accused of having facilitated the travel of many of the hijackers into the United States, as well as handling financial transactions directly associated with the 9/11 attacks.

d. The overall 9/11 conspiracy is alleged to have begun in 1996 when Mohammad met with Usama Bin Laden in Afghanistan and discussed the operational concept of hijacking commercial airliners and crashing them into buildings in the United States and elsewhere. This became known among al Qaeda leadership as the "Planes Operation." Surveillance of airline security, hand-to-hand combat training, and transit of hijackers to the United States began in earnest starting in 1999. Financial transactions and the creation of "martyr wills" relating to the "Planes Operation" continued in 2000. Flight training for the pilot-hijackers extended into 2001. Additional hijackers streamed into the United States during the summer of 2001, and weapons and equipment for use in the attacks were also purchased during this time. In late August 2001, a message to the conspirators allegedly informed them that Atta had chosen 11 September 2001 as the date of the operation. After the attacks, a video featuring Usama bin Laden, Binalshibh, Hawsawi, and other al Qaeda operatives allegedly documented a post-9/11 meeting, which was later released by al Qaeda for propaganda purposes.

e. In response to the terrorist attacks on 11 September 2001, the United States instituted a program run by the CIA to detain and interrogate a number of known or suspected high-value terrorists, or "high-value detainees" ("HVDs"). This CIA program involves information that is classified TOP SECRET / SENSITIVE COMPARTMENTED INFORMATION (SCI), the disclosure of which would be detrimental to national security. [REDACTED]

f. Mohammad and Hawsawi were captured on or about 1 March 2003; Bin Attash and Ali were captured on or about 29 April 2003; and Binalshibh was captured on or around 11 September 2002. After their captures, the Accused were detained and interrogated in the CIA program.

g. Because the Accused were detained and interrogated in the CIA program, they were exposed to classified sources, methods, and activities. Due to their exposure to classified information, the Accused are in a position to reveal this information publicly through their statements. Consequently, any and all statements by the Accused are presumptively classified until a classification review can be completed. [REDACTED]

h. On 6 September 2006, President George W. Bush officially acknowledged the existence of this program and announced that a group of HVDs had been transferred by the CIA to DoD custody at Joint Task Force – Guantanamo (JTF-GTMO). *See* President George W. Bush, *President Discusses Creation of Military Commissions to Try Suspected Terrorists*, Remarks from the East Room of the White House, Sep. 6, 2006, available at <http://georgewbush-whitehouse.archives.gov/news/releases/2006/09/20060906-3.html>. The five Accused were among the group of HVDs transferred to JTF-GTMO, and have remained in detention at JTF-GTMO since that time.

i. Since 6 September 2006, a limited amount of information relating to the CIA program has been declassified and officially acknowledged, often directly by the President. This information includes a general description of the program; descriptions of the various “enhanced interrogation techniques” that were approved for use in the program; the fact that the so-called “waterboard” technique was used on three detainees; and the fact that information learned from HVDs in this program helped to identify and locate al Qaeda members and disrupt planned terrorist attacks. *See id.*; *see also* CIA Inspector General, *Special Review: Counterterrorism Detention and Interrogation Activities (September 2001 – October 2003)*, May 7, 2004, available at http://media.washingtonpost.com/wp-srv/nation/documents/cia_report.pdf.

j. Other information related to the program has not been declassified or officially acknowledged, and therefore remains classified. This classified information includes allegations involving (i) the location of its detention facilities, (ii) the identity of any cooperating foreign governments, (iii) the identity of personnel involved in the capture, detention, transfer, or interrogation of detainees, (iv) interrogation techniques as applied to specific detainees, and (v) conditions of confinement [REDACTED]. The disclosure of this classified information would be detrimental to national security. [REDACTED]

k. Information relating to DoD sources, methods, and activities at JTF-GTMO also remains classified. This classified information includes (i) force protection information, (ii) foreign government information, (iii) intelligence sources and methods, (iv) military and intelligence operational information, (v) certain detainee information, and (vi) derivatively classified information. SOUTHCOM Decl. ¶¶ 12-29. The disclosure of this classified information would be detrimental to national security. *See id.*

l. Certain FBI documents involved in this case also contain classified information, the disclosure of which would be detrimental to national security. FBI Decl. ¶ 10.

6. Discussion

The M.C.A. mandates that the protection of classified information is paramount. *See* 10 U.S.C. § 949p-1. Recognizing the equities at stake when balancing the need for a system to prosecute terrorism-related offenses and the need to conduct ongoing counterterrorism operations, the M.C.A. includes unambiguous protections for classified information, including the sources, methods, and activities by which the United States acquires information. *See generally* 10 U.S.C. §§ 949p-1 through 949p-7. The rules in this area provide that the protection of classified information “applies to all stages of the proceedings.” M.C.R.E. 505(a)(1).

The protections elaborated under the M.C.A. and M.C.R.E. establish well-defined pretrial, trial, and appellate procedures to govern the discovery, handling, and use of classified information in military commissions. Such protections and procedures include protective orders; *ex parte, in camera* presentations and proceedings; alternatives for disclosure of classified information; pretrial conferences and hearings; notice requirements; and protections for courtroom proceedings. *See generally* 10 U.S.C. §§ 949p-1 through 949p-7; M.C.R.E. 505. In analyzing these rules, it is also helpful to examine case law interpreting similar provisions under the Classified Information Procedures Act, 18 U.S.C. App. 3 (CIPA), upon which the M.C.A.'s provisions are patterned. *See* 10 U.S.C. § 949p-1(d) (making the judicial construction of CIPA authoritative under the M.C.A. where not inconsistent with specific M.C.A. provisions); 10 U.S.C. §§ 949p-2(b), 949p-4(b)(2), 949p-7(c)(2) (providing that conferences, presentations, and proffers take place *ex parte* as necessary, in accordance with federal court practice under CIPA); 155 Cong. Rec. S7947, 7987-89 (July 23, 2009) (Senate floor debate on M.C.A. amendments to adopt CIPA procedures).

Due to the classified information involved with this case, and the harm to national security that its disclosure reasonably could be expected to cause, the M.C.A. allows for certain protective measures to be adopted in this military commission. To that end, the Government submits the attached proposed Protective Order (Attachment F) as a means of protecting the classified information involved in this case.

a. CLASSIFIED INFORMATION RELATING TO THE SOURCES, METHODS, AND ACTIVITIES OF THE UNITED STATES MUST BE PROTECTED FROM DISCLOSURE IN THIS MILITARY COMMISSION.

In support of this motion, the Government submits declarations from representatives of the CIA, DoD, and FBI invoking the classified information privilege and explaining how disclosure

of the classified information at issue would be detrimental to national security. [REDACTED]

[REDACTED] SOUTHCOM Decl. ¶ 10-29; FBI Decl. ¶ 10. Due to the extremely sensitive nature of the classified information they contain, the Government files these declarations under seal, respectfully requests that they be considered by the Military Judge *in camera*, and further requests that the Petraeus Declaration and the CIA Declaration be considered *ex parte*. See 10 U.S.C. §§ 949p-2(b), 949p-4(b)(2), 949p-6(a)(3), 949p-6(d)(4); M.C.R.E. 505(d)(2), 505(f)(2)(B), 505(h)(3)(A).¹

As these declarations describe, the classified information involved in this case relates to the sources, methods, and activities by which the United States defends against international terrorism and terrorist organizations, and the disclosure of such information would be detrimental to national security. [REDACTED] SOUTHCOM Decl. ¶ 12; FBI Decl. ¶ 10. This information is therefore properly classified by the executive branch pursuant to Executive Order 13526, as amended, or its predecessor Orders, and is subject to protection in connection with this military commission. 10 U.S.C. §§ 948a(2)(A), 949p-1(a); M.C.R.E. 505(a)(1), (c); M.C.R.E. 505(f), Discussion. See also *Dep't of the Navy v. Egan*, 484 U.S. 518, 527 (1988) (“[T]he protection of classified information must be committed to the broad discretion of the agency responsible, and this must include broad discretion to determine who may have access to it.”);

¹ In addition to being allowed under the military commission rules, *ex parte*, *in camera* inspection of national security information is routinely conducted by federal courts under the similar CIPA provisions upon which the M.C.A.'s classified information provisions are modeled. See, e.g., *United States v. Mejia*, 448 F.3d 436, 457 (D.C. Cir. 2006) (finding that when “the government is seeking to withhold classified information from the defendant, an adversary hearing with defense knowledge would defeat the very purpose of the discovery rules”) (quoting H.R. Rep. No. 96-831, pt. 1, at 27 n.22 (1980)), *cert. denied*, 549 U.S. 1137 (2007); *Stillman v. CIA*, 319 F.3d 546, 548 (D.C. Cir. 2003) (“Precisely because it is often difficult for a court to review the classification of national security information, we anticipate that *in camera* review of affidavits, followed if necessary by further judicial inquiry, will be the norm.”) (internal quotation marks and citation omitted); *United States v. Klimavicius-Viloria*, 144 F.3d 1249, 1261 (9th Cir. 1998) (recognizing that “*ex parte*, *in camera* hearings in which government counsel participates to the exclusion of defense counsel are part of the process that the district court may use,” particularly “if the court has questions about the confidential nature of the information or its relevancy”).

Bismullah v. Gates, 501 F.3d 178, 187-88 (D.C. Cir. 2007) (“It is within the role of the executive to acquire and exercise the expertise of protecting national security.”) (citations omitted).

The protection of such sources, methods, and activities relating to counterterrorism and other intelligence operations predates the enactment of the M.C.A. and is firmly rooted in federal law. In *United States v. Yunis*, 867 F.2d 617 (D.C. Cir. 1989), for example, the Court of Appeals for the D.C. Circuit upheld a protective order that protected not only the contents of a defendant hijacker’s recorded conversations, but also the intelligence-gathering methods used to collect them. *Yunis*, 867 F.2d at 623. The court recognized that in some instances the national security interest “lies not so much in the contents of the conversations, as in the time, place and nature of the government’s ability to intercept the conversations at all.” *Id.*

Even when classified information has been leaked to the public domain, it remains classified and cannot be further disclosed unless it has been declassified or “officially acknowledged,” which entails that it “must already have been made public through an official and documented disclosure.” *Wolf v. CIA*, 473 F.3d 370, 378 (D.C. Cir. 2007) (internal quotations and citations omitted); *see also Fitzgibbon v. CIA*, 911 F.2d 755, 765 (D.C. Cir. 1990) (“[I]n the arena of intelligence and foreign relations, there can be a critical difference between official and unofficial disclosures.”); *United States v. Moussaoui*, 65 Fed. Appx. 881, 887 n.5 (4th Cir. 2003) (“[I]t is one thing for a reporter or author to speculate or guess that a thing may be so or even, quoting undisclosed sources, to say that it is so; it is quite another thing for one in a position to know of it officially to say that it is so.”) (quoting *Alfred A Knopf, Inc. v. Colby*, 509 F.2d 1362, 1370 (4th Cir. 1975)).

Indeed, even false allegations about classified information related to this case must be protected from disclosure because, otherwise, the Government would be in the untenable position

of having to deny false information and yet ignore true information, which would implicitly confirm the very information the Government seeks to protect. [REDACTED] Any disclosure of classified information—which the Defense and the Accused are in a particularly credible position to confirm or deny—can have a significant impact on national security, even if that information is attributed to public sources. See *Wolf*, 473 F.3d at 378 (recognizing that “the fact that information exists in some form in the public domain does not necessarily mean that official disclosure will not cause [cognizable] harm” to government interests); *Afshar v. Dep’t of State*, 702 F.2d 1125, 1130 (D.C. Cir. 1983) (“[E]ven if a fact . . . is the subject of widespread media attention and public speculation, its official acknowledgement by an authoritative source might well be new information that could cause damage to the national security.”).

Accordingly, the Government’s proposed protective order precludes the Defense and the Accused from making public or private statements confirming, contradicting, or otherwise commenting on classified information, including information obtained from the public domain. To allow the Defense or the Accused to comment on such information would amount to an authoritative disclosure of classified information. Because the Government cannot predict whether the Accused intends to disclose classified information at arraignment or during subsequent public proceedings in this case, the Government requests that the Military Judge immediately implement the protective measures set forth in the proposed Protective Order.

b. PURSUANT TO THE M.C.A., VARIOUS PROTECTIVE MEASURES SHOULD BE ADOPTED TO PROTECT CLASSIFIED INFORMATION FROM DISCLOSURE IN THIS CASE.

The M.C.A. and M.C.R.E. authorize the Military Judge to issue protective orders governing the storage, use, and handling of classified information, however it was obtained. 10 U.S.C. § 949p-3; M.C.R.E. 505(e). The attached proposed Protective Order therefore seeks to

protect *all currently and properly classified information* in this case, including classified information that may be obtained in the public domain. See Attachment F. As discussed below, the Government requests that the Military Judge issue the proposed Protective Order and take such additional steps as it deems appropriate to protect against the improper disclosure of classified information during this military commission, including arraignment, discovery, pretrial litigation, trial, and at all other stages of the proceedings.

(1) Commission Security Officer

The Government requests that the Military Judge appoint a Commission Security Officer (CSO), and authorize the CSO to appoint Alternate Commission Security Officers (ACSOs) as necessary, to ensure the proper storage, handling, and use of classified information by the parties in this case. This CSO will serve as the liaison between the owners of the classified information and those who are provided access to such information, and will ensure that the classified information is handled and treated appropriately.² The CSO will be available to advise the Commission on issues regarding classified information, and will assist the Defense and the Government regarding the handling and use of classified information, including pleadings, filings, and documents produced during discovery. The CSO will also assist in enforcing and implementing various protections and procedures designed to avoid harm to national security, including during open proceedings.

(2) Authorized Access to Classified Information

MCRE 505(a)(1), provides that “under no circumstances may a military judge order the release of classified information to any person not authorized to receive such information.” The

² The CSO will work in conjunction with representatives of the originating agencies to make determinations on the appropriate classification status of particular materials; however, the CSO does not have classification authority and will not be in a position to interpret legal or procedural issues relating to the disclosure of such information.

protections for classified information found in MCRE 505 are designed to ensure that at all stages of the proceedings the prosecution is able to weigh the risk of disclosing classified information and reflect the understanding that determining whether an individual is granted access to classified information is inherently an Executive Branch function.

Authorized access to classified information involves several steps. First, an individual must obtain the necessary security clearance which simply allows that person to view classified material. It does not, however, entitle someone to access all classified information. *U.S. v. Bin Laden*, 126 F. Supp.2d 264, 287 n.27 (S.D.N.Y. 2000) (security clearances enable "attorneys to review classified documents, "but do not entitle them to see all documents with that classification.") (citing *United States v. Ott*, 827 F.2d 473, 477 (9th Cir. 1987)). Second, an individual must demonstrate a "need to know" the classified information in question. Exec. Order No. 13,292, § 6.1(z), 68 Fed.Reg. 15,315, 15,332 (Mar. 28, 2003). See *Badrawi v. Dep't of Homeland Security*, 596 F. Supp. 2d 389, 2009 U.S. Dist. LEXIS 2245, 2009 WL 103361, *9 (D.Conn.) (counsel without need to know properly denied access to classified information despite security clearance); *United States v. Ott*, 827 F.2d 473 at 477 (District Court unpersuaded that defense counsel's security clearance entitled them to review FISA material, noting that Congress has a legitimate interest in ensuring that sensitive security information is not unnecessarily disseminated regardless of whether an individual holds the appropriate security clearance.) In the current case, the Accused clearly fall into the category of persons "not authorized to receive" classified information. See MCRE 505(a)(1). Similarly, counsel for other detainees do not have the requisite "need to know" that would enable them to view classified information that the Accused's counsel may have in their possession. Nor would counsel representing the Accused in

a forum other than the current military commission have a “need to know” the classified information at issue in this case.

Accordingly, the Government’s proposed protective order precludes the Defense from providing any classified information obtained during this case, outside the immediate parameters of these military commission proceedings. Further, the proposed protective order precludes the Defense from using classified information obtained as a result of their participation in commission proceedings in any other forum, or in a military commission proceeding involving another detainee.

(3) Clearances

Because the statements of the Accused are presumptively classified as TOP SECRET / SCI, all personnel with whom the Accused have or will have substantive contact must have a TOP SECRET / SCI clearance and be briefed into the appropriate SCI component. Section 4.1 of Executive Order 13526 outlines the requirements that must be met in order to have access to classified information: (1) a favorable determination of eligibility for access by an agency head; (2) a signed, approved nondisclosure agreement; and (3) a need-to-know the information. Under these rules, all members of the Defense, Government, and courtroom personnel, including the clerk, reporter, and CSO, must have the requisite clearances, as set forth in the proposed Protective Order limiting courtroom access to appropriately cleared personnel. The Government also requests that the Defense execute and file the Memorandum of Understanding attached to the Proposed Protective Order (Attachment E) as a precondition to receiving classified information in connection with this case.

(4) Storage, Handling, and Use of Classified Information

In addition to ensuring appointment of a CSO, the Government's proposed Protective Order details specific procedures that it requests the Commission to adopt for maintaining and operating secure areas in which to store and handle classified information. Approved Secure Compartmented Information Facilities (SCIFs) are provided at GTMO and elsewhere for use by the Military Judge, the Defense, and the Government during pretrial and trial proceedings, in order to ensure the proper handling and storage of classified information. The Government's proposed Protective Order details the procedures for maintaining and operating such secure areas and otherwise properly handling classified information in connection with this case. Under the terms of the proposed Protective Order, if there are any questions regarding the treatment or handling of classified information, the parties must seek guidance from the CSO, who will consult as necessary with the owners of the classified information at issue.

(5) Notice Requirements for Introducing Classified Information During Proceedings

The M.C.A. requires the Defense to give advance notice to the Government and the Military Judge whenever it reasonably expects to disclose classified information at a proceeding. M.C.R.E. 505(g)(1)(A). This rule allows both the Government and the Military Judge the opportunity to be fully apprised ahead of time of the classified information at issue, to ascertain the potential harm full disclosure could cause to national security, and to consider whether there are alternatives to disclosure that could minimize that harm. *See United States v. Badia*, 827 F.2d 1458, 1465 (11th Cir. 1987), *cert. denied*, 485 U.S. 937 (1988).

This notice requirement has three critical steps. *See* M.C.R.E. 505(g)-(h). First, the Defense must provide a detailed, written description of the specific classified information it reasonably expects to disclose. M.C.R.E. 505(g)(1)(A), Discussion. Courts interpreting the similar requirement under CIPA Section 5(a) have held that such descriptions "must be

particularized, setting forth specifically the classified information which the defendant reasonably believes to be necessary to his defense.” *United States v. Collins*, 720 F.2d 1195, 1199-1200 (11th Cir. 1983); *see also United States v. Smith*, 780 F.2d 1102, 1105 (4th Cir. 1985) (*en banc*). This notice requirement applies equally to information the Defense intends to introduce through documentary exhibits and to information it intends to elicit through testimony on direct or cross-examination. *See Collins*, 720 F.2d at 1195; *United States v. Wilson*, 750 F.2d 7 (2d Cir. 1984), *cert. denied*, 479 U.S. 839 (1986).

Second, the Defense must provide its notice sufficiently in advance of the proceeding to provide the Government with a reasonable opportunity to (1) invoke the classified information privilege, (2) move for an *in camera* hearing to discuss the information-at-issue, (3) obtain a ruling on the issue from the Military Judge, (4) propose any alternatives to disclosure, and (5) determine whether to pursue an interlocutory appeal for any ruling allowing the disclosure of classified information. M.C.R.E. 505(g)(1), 505(h). Thus, this timing requirement, similar to the one imposed under CIPA Section 5(a), takes into account the lengthy process that can ensue between the initial notice from the Defense and the proceeding at which the disclosure of classified information is expected to occur.

Third, as stated above, once the Defense has provided notice of its intent to disclose classified information in a proceeding, the Government may move for an *in camera* hearing to address the classified information privilege and the use of any classified information. M.C.R.E. 505(h). In connection with this *in camera* hearing, the Military Judge must determine whether the classified information is “relevant and necessary to an element of the offense or a legally cognizable defense and is otherwise admissible.” M.C.R.E. 505(h)(1)(C). If so, the Government can seek alternatives to full disclosure for the classified information, which must be used by the

Defense unless use of the classified information itself is necessary to afford the Accused a fair trial. M.C.R.E. 505(h)(1), 505(h)(3)-(4); *see also United States v. North*, 910 F.2d 843, 899 (D.C. Cir. 1990) (finding that under CIPA, the trial court must grant the Government's substitution "if it finds that the admission or summary would leave the defendant in substantially the same position as would disclosure").

Unless the Defense meets this notice requirement, and affords the Government a reasonable opportunity to seek the available protections discussed above, the Defense is prohibited from disclosing the classified information. M.C.R.E. 505(g). This prohibition pertains to both the introduction of the classified information at issue and the examination of any witness with respect to that information. M.C.R.E. 505(g)(2).

(6) Disclosure of Classified Information During Proceedings

The Government's proposed protective order provides that the Government may seek to limit the direct or cross-examination of a witness to protect against the public disclosure of classified information. *See* M.C.R.E. 505(e). To that end, Trial Counsel may object to any line of questioning during witness testimony that may require disclosure of inadmissible classified information. *See* M.C.R.E. 505(i)(3). Following such an objection, the Military Judge should determine whether the witness' response is admissible and, if so, take additional steps as necessary to protect against the public disclosure of any classified information.

To prevent the disclosure of classified information through physical or documentary evidence, the Military Judge may admit a portion of a document, recording, or photograph into evidence, or proof of the contents thereof, without requiring the introduction of the original classified item into evidence. M.C.R.E. 505(i)(2). The Military Judge also may permit the Government to introduce otherwise admissible evidence while protecting the classified sources,

methods, and activities by which the United States acquired the evidence, so long as the evidence is deemed reliable. M.C.R.E. 505(h)(3). Regardless of the manner in which such evidence is introduced, however, the evidence remains classified at its original classification level. M.C.R.E. 505(i)(1).

Finally, to protect against disclosure of classified information, including intelligence or law enforcement sources, methods, or activities, the Military Judge may order that the public be excluded from any portion of a proceeding in which such information will be disclosed, or take other lesser measures as necessary to protect against disclosure of information during open proceedings. *See* 10 U.S.C. § 949d(c); R.M.C. 806(b), Discussion. This express authorization to close proceedings to the public during the military commission process recognizes the national security interests at stake when handling or presenting classified information in connection with pretrial or trial proceedings.

(7) Delayed Audio Feed to the Public Gallery

In accordance with M.C.R.E. 505, certain safeguards have already been instituted in the courtroom used by this military commission, including a glass partition separating the public gallery from the courtroom itself, which is connected by an audio-video broadcast.³ The Government requests a forty-second delay in the broadcast to the gallery so that if classified information is disclosed, inadvertently or otherwise, in open court, the Government will have the opportunity to prevent it from being publicly disclosed. If any of the Accused testify, for example, the delayed-broadcast mechanism is vital to the protection of classified information since the Accused's statements are presumed classified until a classification review is completed. Because the Government cannot predict what an Accused will say during open proceedings or

³ This broadcast may also connect the courtroom to a remote viewing area.

whether he will comply with orders from the Military Judge, the time delay is the only effective means of preventing any intentional or inadvertent disclosure of classified information to the public. Additionally, the time delay will prevent the public disclosure of classified information by other witnesses, who may reveal such information inadvertently during their testimony in open proceedings.

This measure, which is much less restrictive than closing the courtroom entirely, is necessary to protect classified information during open proceedings. In the event that classified information is disclosed during open proceedings, the forty-second delay would allow the Military Judge, the CSO, or the Government to take action to suspend the broadcast before the information is publicly disclosed. The Government can then consult with the equity holder of the classified information to determine what, if any, actions must be taken to limit its disclosure. *See* M.C.R.E. 505(i)(3). If classified information is disclosed during the proceeding, and the broadcast is suspended to prevent its public disclosure, then that portion of the proceeding will not be broadcast, but will remain part of the classified record of the proceeding. If the Military Judge determines, after consultation with the CSO, that the Government will not assert any privilege, or that classified information was not disclosed and is not at risk of disclosure, then the proceedings and the broadcast, with the time delay, will resume upon the Commission's order.

c. CONCLUSION

In light of the classified information at issue in this case, and the harm to national security that its disclosure reasonably could be expected to cause, the Government requests that the Military Judge enter the proposed Protective Order (Attachment E) and the proposed Order placing classified Attachments A through D under seal (Attachment F).

UNCLASSIFIED//FOR PUBLIC RELEASE

UNCLASSIFIED//FOR OFFICIAL USE ONLY

7. **Oral Argument.** The Government does not request oral argument. The Government requests that the proposed Protective Order be issued prior to any commission proceeding.
8. **Certificate of Conference.** The Defense has been notified of this motion and objects to the requested relief.
9. **Attachments**
 - A. Classified Declaration of David H. Petraeus, Director, Central Intelligence Agency, dated 7 April 2012 (filed *ex parte, in camera*, and UNDER SEAL)
 - B. Classified Declaration of Information Review Officer, Central Intelligence Agency, dated 12 April 2012 (filed *ex parte, in camera*, and UNDER SEAL)
 - C. Classified Declaration of General Douglas M. Fraser, United States Air Force, Commander, United States Southern Command, dated 24 October 2011 (filed *in camera* and UNDER SEAL)
 - D. Classified Declaration of Mark F. Giuliano, Assistant Director, Counterterrorism Division, Federal Bureau of Investigation, dated 7 September 2011 (filed *in camera* and UNDER SEAL)
 - E. Proposed Protective Order and Memorandum of Understanding
 - F. Proposed Order placing Attachments A through D under seal
 - G. Certificate of Service

Respectfully submitted,

//s//

Joanna P. Baltes
Deputy Trial Counsel
Mark Martins
Chief Prosecutor
Office of the Chief Prosecutor
Office of Military Commissions
1610 Defense Pentagon
Washington, D.C. 20301

UNCLASSIFIED//FOR PUBLIC RELEASE

**MILITARY COMMISSIONS TRIAL JUDICIARY
GUANTANAMO BAY, CUBA**

<p>UNITED STATES OF AMERICA</p> <p>v.</p> <p>KHALID SHEIKH MOHAMMAD, WALID MUHAMMAD SALIH MUBARAK BIN ATTASH, RAMZI BINALSHIBH, ALI ABDUL AZIZ ALI, MUSTAFA AHMED ADAM AL HAWSAWI</p>	<p>FILED <i>EX PARTE</i></p> <p>FILED <i>IN CAMERA</i></p> <p>FILED UNDER SEAL</p>
--	---

ATTACHMENT A – CLASSIFIED DECLARATION OF DAVID H. PETRAEUS,
DIRECTOR, CENTRAL INTELLIGENCE AGENCY, DATED 7 APRIL 2012

Filed with TJ
26 April 2012

Attachment A
Page 1 of 6

Appellate Exhibit 013- (KSM et al.)
Page 21 of 130

UNCLASSIFIED//FOR PUBLIC RELEASE

UNCLASSIFIED//FOR PUBLIC RELEASE

**MILITARY COMMISSIONS TRIAL JUDICIARY
GUANTANAMO BAY, CUBA**

<p>UNITED STATES OF AMERICA</p> <p>v.</p> <p>KHALID SHEIKH MOHAMMAD, WALID MUHAMMAD SALIH MUBARAK BIN ATTASH, RAMZI BINALSHIBH, ALI ABDUL AZIZ ALI, MUSTAFA AHMED ADAM AL HAWSAWI</p>	<p>FILED <i>EX PARTE</i></p> <p>FILED <i>IN CAMERA</i></p> <p>FILED UNDER SEAL</p>
--	---

ATTACHMENT B – CLASSIFIED DECLARATION OF INFORMATION REVIEW
OFFICER, CENTRAL INTELLIGENCE AGENCY, DATED 12 APRIL 2012

UNCLASSIFIED//FOR PUBLIC RELEASE

UNCLASSIFIED//FOR PUBLIC RELEASE

**MILITARY COMMISSIONS TRIAL JUDICIARY
GUANTANAMO BAY, CUBA**

<p>UNITED STATES OF AMERICA</p> <p>v.</p> <p>KHALID SHEIKH MOHAMMAD, WALID MUHAMMAD SALIH MUBARAK BIN ATTASH, RAMZI BINALSHIBH, ALI ABDUL AZIZ ALI, MUSTAFA AHMED ADAM AL HAWSAWI</p>	<p>FILED <i>IN CAMERA</i></p> <p>FILED UNDER SEAL</p>
--	---

ATTACHMENT C – CLASSIFIED DECLARATION OF GENERAL DOUGLAS M. FRASER,
UNITED STATES AIR FORCE, COMMANDER, UNITED STATES SOUTHERN
COMMAND, DATED 24 OCTOBER 2011

Filed with TJ
26 April 2012

Attachment C
Page 1 of 22

Appellate Exhibit 013- (KSM et al.)
Page 63 of 130

UNCLASSIFIED//FOR PUBLIC RELEASE

UNCLASSIFIED//FOR PUBLIC RELEASE

**MILITARY COMMISSIONS TRIAL JUDICIARY
GUANTANAMO BAY, CUBA**

<p>UNITED STATES OF AMERICA</p> <p>v.</p> <p>KHALID SHEIKH MOHAMMAD, WALID MUHAMMAD SALIH MUBARAK BIN ATTASH, RAMZI BINALSHIBH, ALI ABDUL AZIZ ALI, MUSTAFA AHMED ADAM AL HAWSAWI</p>	<p>FILED <i>IN CAMERA</i></p> <p>FILED UNDER SEAL</p>
--	---

ATTACHMENT D – CLASSIFIED DECLARATION OF MARK F. GIULIANO, ASSISTANT
DIRECTOR, COUNTERTERRORISM DIVISION, FEDERAL BUREAU OF
INVESTIGATION, DATED 7 SEPTEMBER 2011

Filed with TJ
26 April 2012

Attachment D
Page 1 of 24

Appellate Exhibit 013- (KSM et al.)
Page 85 of 130

UNCLASSIFIED//FOR PUBLIC RELEASE

**MILITARY COMMISSIONS TRIAL JUDICIARY
GUANTANAMO BAY, CUBA**

<p>UNITED STATES OF AMERICA</p> <p>v.</p> <p>KHALID SHAIKH MOHAMMAD, WALID MUHAMMAD SALIH MUBARAK BIN ATTASH, RAMZI BINALSHIBH, ALI ABDUL AZIZ ALI, MUSTAFA AHMED ADAM AL HAWSAWI</p>	<p>PROTECTIVE ORDER #1</p> <p>To Protect Against Disclosure of National Security Information</p> <p>_____ 2012</p>
--	---

Upon consideration of the submissions regarding the Government's motion for a protective order to protect classified information in this case, the Commission finds that this case involves classified national security information, including TOP SECRET / SENSITIVE COMPARTMENTED INFORMATION (SCI), the disclosure of which would be detrimental to national security, the storage, handling, and control of which requires special security precautions, and access to which requires a security clearance and a need-to-know. Accordingly, pursuant to authority granted under 10 U.S.C. §§ 949p-1 to 949p-7, Rules for Military Commissions (R.M.C.) 701 and 806, Military Commission Rule of Evidence (M.C.R.E.) 505, Regulation for Trial by Military Commissions (R.T.M.C.) ¶ 17-3, and the general supervisory authority of the Commission, in order to protect the national security, and for good cause shown, the following Protective Order is entered.

I. SCOPE

1. This Protective Order establishes procedures applicable to all persons who have access to or come into possession of classified documents or information in connection with this case,

regardless of the means by which the persons obtained the classified information. These procedures apply to all aspects of pretrial, trial, and post-trial stages in this case, including any appeals, subject to modification by further order of the Commission.

2. This Protective Order applies to all information, documents, testimony, and material associated with this case that contain classified information, including but not limited to any classified pleadings, written discovery, expert reports, transcripts, notes, summaries, or any other material that contains, describes, or reflects classified information.

3. Counsel are responsible for advising their clients, translators, witnesses, experts, consultants, support staff, and all others involved with the defense or prosecution of this case, respectively, of the contents of this Protective Order.

II. DEFINITIONS

4. As used in this Protective Order, the term "Defense" includes any counsel for the Accused in this case and any employees, contractors, investigators, paralegals, experts, translators, support staff or other persons working on the behalf of the Accused or his counsel in this case.

5. The term "Government" includes any counsel for the United States in this case and any employees, contractors, investigators, paralegals, experts, translators, support staff or other persons working on the behalf of the United States or its counsel in this case.

6. The words "documents" and "information" include, but are not limited to, all written or printed matter of any kind, formal or informal, including originals, conforming copies and non-conforming copies, whether different from the original by reason of notation made on such copies or otherwise, and further include, but are not limited to:

UNCLASSIFIED//FOR PUBLIC RELEASE

a. papers, correspondence, memoranda, notes, letters, cables, reports, summaries, photographs, maps, charts, graphs, inter-office and intra-office communications, notations of any sort concerning conversations, meetings, or other communications, bulletins, teletypes, telegrams, facsimiles, invoices, worksheets, and drafts, alterations, modifications, changes, and amendments of any kind to the foregoing;

b. graphic or oral records or representations of any kind, including, but not limited to: photographs, charts, graphs, microfiche, microfilm, videotapes, and sound or motion picture recordings of any kind;

c. electronic, mechanical, or electric records of any kind, including, but not limited to: tapes, cassettes, disks, recordings, electronic mail, instant messages, films, typewriter ribbons, word processing or other computer tapes, disks or portable storage devices, and all manner of electronic data processing storage; and

d. information acquired orally.

7. The terms “classified national security information and/or documents,” “classified information,” and “classified documents” include:

a. any classified document or information that was classified by any Executive Branch agency in the interests of national security or pursuant to Executive Order, including Executive Order 13526, as amended, or its predecessor Orders, as “CONFIDENTIAL,” “SECRET,” “TOP SECRET,” or additionally controlled as “SENSITIVE COMPARTMENTED INFORMATION (SCI)” and specifically designated by the United States for limited or restricted dissemination or distribution;

b. any document or information, regardless of its physical form or characteristics, now or formerly in the possession of a private party that was derived from United States

UNCLASSIFIED//FOR PUBLIC RELEASE

Government information that was classified, regardless of whether such document or information has subsequently been classified by the Government pursuant to Executive Order, including Executive Order 13526, as amended, or its predecessor Orders, as "CONFIDENTIAL," "SECRET," "TOP SECRET," or additionally controlled as "SENSITIVE COMPARTMENTED INFORMATION (SCI)";

c. verbal or non-documentary classified information known to the Accused or the Defense;

d. any document or information as to which the Defense has been notified orally or in writing that such document or information contains classified information, including, but not limited to the following:

(i) documents or information that would reveal or tend to reveal details surrounding the capture of the Accused other than the location and date;

(ii) documents or information that would reveal or tend to reveal the locations in which: Khalid Shaikh Mohammad (Mohammad) and Mustafa Ahmed Adam al Hawsawi (Hawsawi) were detained from the time of their capture on or about 1 March 2003 through 6 September 2006; Walid Muhammad Salih Bin Attash (Bin Attash) and Ali Abdul Aziz Ali (Ali) were detained from the time of their capture on or about 29 April 2003 through 6 September 2006; and Ramzi Binalshibh (Binalshibh) was detained from the time of his capture on or around 11 September 2002 through 6 September 2006.

(iii) documents or information that refer or relate to the names, identities, and descriptions of any persons involved with the capture, transfer, detention, or interrogation of the Accused or specific dates regarding the same, from on or around the aforementioned capture dates through 6 September 2006;

(iv) documents or information that refer or relate to classified sources, methods, or activities used by the United States to acquire evidence or information, including information describing any interrogation techniques as applied to the Accused from on or around the aforementioned capture dates through 6 September 2006;

(v) documents or information that refer or relate to the conditions of confinement of the Accused from on or around the aforementioned capture dates through 6 September 2006;

(vi) statements made by the Accused, which, due to these individuals' exposure to classified sources, methods, or activities of the United States, are presumed to contain information classified as TOP SECRET / SCI; and

e. any document or information obtained from or related to a foreign government or dealing with matters of U.S. foreign policy, intelligence, or military operations, which is known to be closely held and potentially damaging to the national security of the United States or its allies.

8. "National Security" means the national defense and foreign relations of the United States.

9. "Access to classified information" means having authorized access to review, read, learn, or otherwise come to know classified information.

10. "Secure area" means a physical facility accredited or approved for the storage, handling, and control of classified information.

11. "Unauthorized disclosure of classified information" means any knowing, willful, or negligent action that could reasonably be expected to result in a communication or physical transfer of classified information to an unauthorized recipient. Confirming or denying information, including its very existence, constitutes disclosing that information.

III. COMMISSION SECURITY OFFICER

12. A Commission Security Officer (CSO) has been appointed by the Commission for the purpose of providing security arrangements necessary to protect against unauthorized disclosure of any classified documents or information in connection with this case. The CSO is authorized to appoint Alternate Commission Security Officers (ACSOs) as necessary. All references to the CSO herein shall be deemed to refer also to any ACSOs appointed to this case.

13. The parties shall seek guidance from the CSO with regard to the appropriate storage, handling, and use of classified information. The CSO shall consult with the original classification authority (OCA) of classified documents or information, as necessary, to address classification decisions or other related issues.

14. The CSO shall not reveal to any person, including the Government, the content of any conversations the CSO hears by or among the Defense, nor reveal the nature of documents being reviewed by the Defense or the work generated by the Defense, except as necessary to report violations of this Protective Order to the Commission after appropriate consultation with the Defense or to carry out duties pursuant to this Protective Order. Additionally, the presence of the CSO shall not operate as a waiver of any applicable privilege under the Military Commissions Act, 10 U.S.C. § 948a, *et seq.* (M.C.A.), R.M.C., or M.C.R.E.

IV. ACCESS TO CLASSIFIED INFORMATION

15. Without authorization from the Government, no member of the Defense, including defense witnesses, shall have access to classified information in connection with this case unless that person has:

a. received the necessary security clearance from the appropriate Department of Defense (DoD) authorities and signed an appropriate non-disclosure agreement, as verified by the CSO;

b. signed the Memorandum of Understanding Regarding Receipt of Classified Information (MOU), attached to this Protective Order, agreeing to comply with the terms of this Protective Order; and

c. a need-to-know the classified information at issue, as determined by the OCA of that information.

16. In order to be provided access to classified information in connection with this case, each member of the Defense shall execute the attached MOU, file the executed originals of the MOU with the Commission, and submit copies to the CSO and counsel for the Government. The execution and submission of the MOU is a condition precedent to the Defense having access to classified information for the purposes of these proceedings.

17. The substitution, departure, or removal of any member of the Defense, including defense witnesses, from this case for any reason shall not release that person from the provisions of this Protective Order or the MOU executed in connection with this Protective Order.

18. Once the CSO verifies that counsel for the Accused have executed and submitted the MOU, and are otherwise authorized to receive classified information in connection with this case, the Government may provide classified discovery to the Defense, either directly or via the CSO, who will assist as necessary in ensuring the material is delivered to the Defense.

19. All classified documents or information provided or obtained in connection with this case remain classified at the level designated by the OCA, unless the documents bear a clear indication that they have been declassified. The person receiving the classified documents or

information, together with all other members of the Defense or the Government, respectively, shall be responsible for protecting the classified information from disclosure and shall ensure that access to and storage of the classified information is in accordance with applicable laws and regulations and the terms of this Protective Order.

20. No member of the Defense, including any defense witness, is authorized to disclose any classified information obtained during this case, outside the immediate parameters of these military commission proceedings. If any member of the Defense, the Accused, or any defense witness receives any summons, subpoena, or court order, or the equivalent thereof, from any United States or foreign court or on behalf of any criminal or civil investigative entity within the United States or from any foreign entity, the Defense, including defense witnesses, shall immediately notify the Commission, the CSO, and the Government so that appropriate consideration can be given to the matter by the Commission and the OCA of the materials concerned. Absent authority from the Commission or the Government, the Defense, the Accused, and defense witnesses are not authorized to disseminate or disclose classified materials in response to such requests. The Defense, the Accused, and defense witnesses and experts are not authorized to use or refer to any classified information obtained as a result of their participation in commission proceedings in any other forum, or in a military commission proceeding involving another detainee.

V. USE, STORAGE, AND HANDLING PROCEDURES

21. The Office of the Chief Defense Counsel, Office of Military Commissions, has approved secure areas in which the Defense may use, store, handle, and otherwise work with classified information. The CSO shall ensure that such secure areas are maintained and operated in a

manner consistent with this Protective Order and as otherwise reasonably necessary to protect against the disclosure of classified information.

22. All classified information provided to the Defense, and otherwise possessed or maintained by the Defense, shall be stored, maintained, and used only in secure areas. Classified information may only be removed from secure areas in accordance with this Protective Order and applicable laws and regulations governing the handling and use of classified information.

23. Consistent with other provisions of this Protective Order, the Defense shall have access to the classified information made available to them and shall be allowed to take notes and prepare documents with respect to such classified information in secure areas.

24. The Defense shall not copy or reproduce any classified information in any form, except in secure areas and in accordance with this Protective Order and applicable laws and regulations governing the reproduction of classified information.

25. All documents prepared by the Defense that are known or believed to contain classified information—including, without limitation, notes taken or memoranda prepared by counsel and pleadings or other documents intended for filing with the Commission—shall be transcribed, recorded, typed, duplicated, copied, or otherwise prepared only by persons possessing an appropriate approval for access to such classified information. Such activities shall take place in secure areas, on approved word processing equipment, and in accordance with procedures approved by the CSO. All such documents and any associated materials containing classified information—such as notes, memoranda, drafts, copies, typewriter ribbons, magnetic recordings, and exhibits—shall be maintained in secure areas unless and until the CSO advises that those documents or associated materials are unclassified in their entirety. None of these materials shall

be disclosed to the Government unless authorized by the Commission, by counsel for the Accused, or as otherwise provided in this Protective Order.

26. The Defense may discuss classified information only within secure areas and shall not discuss, disclose, or disseminate classified information over any non-secure communication system, such as standard commercial telephones, office intercommunication systems, or non-secure electronic mail.

27. The Defense shall not disclose any classified documents or information to any person, including counsel in related cases of Guantanamo Bay detainees in military commissions or other courts (including, but not limited to, habeas proceedings), except those persons authorized by this Protective Order, the Commission, and counsel for the Government with the appropriate clearances and the need-to-know that information.

28. To the extent that the Defense is not certain of the classification of information it wishes to disclose, the Defense shall consult with the CSO for a determination as to its classification. In any instance in which there is any doubt as to whether information is classified, the Defense must consider the information classified unless and until it receives notice from the CSO that such information is not classified.

29. Until further order of this Commission, the Defense shall not disclose to the Accused any classified information not previously provided by the Accused to the Defense, except where such information has been approved for release to the Accused and marked accordingly.

30. Except as otherwise stated in this paragraph, and to ensure the national security of the United States, at no time, including any period subsequent to the conclusion of these proceedings, shall the Defense make any public or private statements disclosing any classified information accessed pursuant to this Protective Order, or otherwise obtained in connection with

this case, including the fact that any such information or documents are classified. In the event classified information enters the public domain without first being properly declassified by the United States Government, counsel are reminded that they may not make public or private statements about the information if the information is classified. (See paragraph 7 of this Protective Order for specific examples of information which remains classified even if it is in the public domain.) In an abundance of caution and to help ensure clarity on this matter, the Commission emphasizes that counsel shall not be the source of any classified information entering the public domain, nor should counsel comment on information which has entered the public domain but which remains classified.

VI. PROCEDURES FOR FILING DOCUMENTS

31. Any pleading or other document filed with the Commission in this case, which counsel know, reasonably should know, or are uncertain of whether the filing contains classified information, shall be filed under seal in accordance with the provisions of the M.C.A., R.M.C., M.C.R.E., R.T.M.C., and the Military Commissions Trial Judiciary Rules of Court applicable to filing classified documents or information. Documents containing classified information that is not at the TS/CODEWORD level shall be filed pursuant to the procedures specified for classified information contained in the Trial Judiciary Rules of Court 3(10)(d) to the extent that the material can be transmitted via the Secret Internet Protocol Router Network (SIPR). Information that is classified at the TS/CODEWORD level, including presumptively classified statements of the Accused that have not yet been determined to be unclassified by the appropriate Government agency, cannot be transmitted via SIPR and must be provided in hard copy to the Chief Clerk of the Trial Judiciary.

UNCLASSIFIED//FOR PUBLIC RELEASE

32. Classified filings must be marked with the appropriate classification markings on each page, including classification markings for each paragraph. If a party is uncertain as to the appropriate classification markings for a document, the party shall seek guidance from the CSO, who will consult with the OCA of the information or other appropriate agency, as necessary, regarding the appropriate classification.

33. When filing classified documents or information under seal, the parties shall file the papers containing classified information with the Military Commissions Trial Judiciary Staff ("Judiciary Staff") and provide notice of the classified filing to the other party. Once a filing is properly filed, the CSO for the Judiciary Staff shall promptly review the filing, and in consultation with the appropriate Government agencies, determine whether the filing contains classified information and is marked appropriately. The Judiciary Staff shall then ensure the classified filing is promptly served on the other party (unless filed *ex parte*) and reflected in the filings inventory with an unclassified entry noting that it was filed under seal.

34. The CSO and Judiciary Staff shall ensure any classified information contained in such filings is maintained under seal and stored in an appropriate secure area consistent with the highest level of classified information contained in the filing. All portions of any filed papers that do not contain classified information will be unsealed (unless filed *in camera* or *ex parte*) for inclusion in the public record.

35. Under no circumstances may classified information be filed in an unsealed filing. In the event a party believes that an unsealed filing contains classified information, the party shall immediately notify the CSO and Judiciary Staff, who shall take appropriate action to retrieve the documents or information at issue. The filing will then be treated as containing classified information unless and until the CSO determines otherwise. Nothing herein limits the

Government's authority to take other remedial action as necessary to ensure the protection of the classified information.

36. Nothing herein requires the Government to disclose classified information. Additionally, nothing herein prevents the Government from submitting classified information to the Commission *in camera* or *ex parte* in these proceedings or entitles the Defense access to such submissions or information. Except for good cause shown in the filing, the Government shall provide the Defense with notice on the date of the filing.

VII. PROCEDURES FOR MILITARY COMMISSION PROCEEDINGS

37. Except as provided herein, and in accordance with M.C.R.E. 505, no party shall disclose or cause to be disclosed any information known or believed to be classified in connection with any hearing or proceeding in this case.

A. Notice Requirements

38. The parties must comply with all notice requirements under M.C.R.E. 505 prior to disclosing or introducing any classified information in this case.

39. Because all statements of the Accused are presumed to contain information classified as TOP SECRET / SCI, the Defense must provide notice in accordance with this Protective Order and M.C.R.E. 505(g) if the Accused intends to make statements or offer testimony at any proceeding.

B. Closed Proceedings

40. While proceedings shall generally be publicly held, the Commission may exclude the public from any proceeding, *sua sponte* or upon motion by either party, in order to protect information the disclosure of which could reasonably be expected to damage national security. If the Commission closes the courtroom during any proceeding in order to protect classified

information from disclosure, no person may remain who is not authorized to access classified information in accordance with this Protective Order, which the CSO shall verify prior to the proceeding.

41. No participant in any proceeding, including the Government, Defense, Accused, witnesses, and courtroom personnel, may disclose classified information, or any information that tends to reveal classified information, to any person not authorized to access such classified information in connection with this case.

C. Delayed Broadcast of Open Proceedings

42. Due to the nature and classification level of the classified information in this case, including the classification of the Accused's statements, the Commission finds that to protect against the unauthorized disclosure of classified information during proceedings open to the public, it will be necessary to employ a forty-second delay in the broadcast of the proceedings from the courtroom to the public gallery. Should classified information be disclosed during any open proceeding, this delay will allow the Military Judge, CSO, or Government to take action to suspend the broadcast—including any broadcast of the proceedings to locations other than the public gallery of the courtroom (e.g., any closed-circuit broadcast of the proceedings to a remote location)—so that the classified information will not be disclosed to members of the public.

43. The broadcast may be suspended whenever it is reasonably believed that any person in the courtroom has made or is about to make a statement or offer testimony disclosing classified information.

44. The Commission shall be notified immediately if the broadcast is suspended. In that event, and otherwise if necessary, the Commission may stop the proceedings to evaluate whether the information disclosed, or about to be disclosed, is classified information as defined in this

Protective Order. The Commission may also conduct an *in camera* hearing to address any such disclosure of classified information.

D. Other Protections

45. During the examination of any witness, the Government may object to any question or line of inquiry that may require the witness to disclose classified information not found previously to be admissible by the Commission. Following such an objection, the Commission will determine whether the witness's response is admissible and, if so, may take steps as necessary to protect against the public disclosure of any classified information contained therein.

46. Classified information offered or admitted into evidence will remain classified at the level designated by the OCA and will be handled accordingly. All classified evidence offered or accepted during trial will be kept under seal, even if such evidence was inadvertently disclosed during a proceeding. Exhibits containing classified information may also be sealed after trial as necessary to prevent disclosure of such classified information.

E. Transcripts

47. Transcripts of all proceedings shall be redacted as necessary to prevent public disclosure of classified information. The Clerk of the Military Commission, in conjunction with the CSO, shall ensure the transcripts of all proceedings are reviewed and redacted as necessary to protect any classified information from public disclosure. An unclassified transcript of each proceeding shall be made available for public release.

48. The Clerk of the Military Commission, in conjunction with the CSO, shall ensure that transcripts containing classified information remain under seal and are properly segregated from the unclassified portion of the transcripts, properly marked with the appropriate security markings, stored in a secure area, and handled in accordance with this Protective Order.

VIII. UNAUTHORIZED DISCLOSURE

49. Any unauthorized disclosure of classified information may constitute a violation of United States criminal laws. Additionally, any violation of the terms of this Protective Order shall immediately be brought to the attention of the Commission and may result in disciplinary action or other sanctions, including a charge of contempt of the Commission and possible referral for criminal prosecution. Any breach of this Protective Order may also result in the termination of access to classified information. Persons subject to this Protective Order are advised that unauthorized disclosure, retention, or negligent handling of classified documents or information could cause damage to the national security of the United States or may be used to the advantage of an adversary of the United States or against the interests of the United States. The purpose of this Protective Order is to ensure that those authorized to receive classified information in connection with this case will never divulge that information to anyone not authorized to receive it, without prior written authorization from the OCA and in conformity with this Order.

50. The Defense shall promptly notify the CSO upon becoming aware of any unauthorized access to or loss, theft, or other disclosure of classified information, and shall take all reasonably necessary steps to retrieve such classified information and protect it from further unauthorized disclosure or dissemination. The CSO shall notify the Government of any unauthorized disclosures of classified information so that the Government may take additional remedial measures as necessary to prevent further unauthorized access or dissemination.

IX. DISPOSITION OF CLASSIFIED INFORMATION

51. All classified documents and information to which the Defense has access in this case are the property of the United States. Upon demand of the CSO or the Government, the Defense

shall return any documents containing classified information in its possession which were obtained in discovery from the Government, or for which the Defense is responsible because of its access to classified information in connection with this case.

52. Unless otherwise ordered or agreed, within sixty days after the final termination of this action, including any appeals, the Defense shall, at its option, return or properly destroy all classified information in its possession in connection with this case, including all notes, abstracts, compilations, summaries, or any other form or reproduction of classified information. The Defense is responsible for reminding any expert witnesses, non-testifying consultants, and all other persons working with the Defense of its obligation to return or destroy classified information related to this case. The Defense shall submit written certification to the CSO and the Government by the sixty-day deadline confirming that all classified information has been returned or destroyed as set forth in this Protective Order.

X. SURVIVAL OF ORDER

53. The terms of this Protective Order and any signed MOU shall survive and remain in effect after the termination of this case.

54. This Protective Order is entered without prejudice to the right of the parties to seek such additional protections, or exceptions to those stated herein, as they deem necessary.

SO ORDERED:

DATED: _____

JAMES L. POHL
COL, JA, USA
Military Judge

**MILITARY COMMISSIONS TRIAL JUDICIARY
GUANTANAMO BAY, CUBA**

UNITED STATES OF AMERICA)	
)	
v.)	Memorandum of Understanding
)	Regarding the Receipt of Classified
)	Information
KHALID SHAIKH MOHAMMAD;)	
WALID MUHAMMAD SALIH)	
MUBARAK BIN ATTASH;)	
RAMZI BINALSHIBH;)	
ALI ABDUL AZIZ ALI;)	
MUSTAFA AHMED ADAM AL)	
HAWSAWI)	

I, _____, [print or type full name], have been provided a copy of and have read Protective Order #1 relating to the protection of classified information in the above-captioned case, and agree to be bound by the terms of that order. I understand that in connection with this case I will receive classified documents and information that are protected pursuant to both the terms of the Protective Order and the applicable laws and regulations governing the use, storage, and handling of classified information. I also understand that the classified documents and information are the property of the United States and refer or relate to the national security of the United States.

I agree that I will not use or disclose any classified documents or information, except in strict compliance with the provisions of the Protective Order and the applicable laws and regulations governing the use, storage, and handling of classified information. I have further familiarized myself with the statutes, regulations, and orders relating to the unauthorized disclosure of classified information, espionage, and other related criminal offenses, including but

not limited to 50 U.S.C. § 421; 18 U.S.C. § 641; 18 U.S.C. § 793; 50 U.S.C. § 783; and Executive Order 13526.

I agree to take all reasonable precautions to prevent any unauthorized use or disclosure of any classified documents or information in my possession or control. I understand that failure to comply with this Memorandum of Understanding Regarding the Receipt of Classified Information (MOU) or any protective order entered in this case could result in sanctions or other consequences, including criminal consequences. I understand that the terms of this MOU shall survive and remain in effect after the termination of this case, and that any termination of my involvement in this case prior to its conclusion will not relieve me from the terms of this MOU or any protective order entered in the case.

I make the above statements under penalty of perjury.

Signature

Date

Witness

Date

Witness

Date

MILITARY COMMISSIONS TRIAL JUDICIARY
GUANTANAMO BAY, CUBA

UNITED STATES OF AMERICA)	
)	
v.)	ORDER
)	
KHALID SHAIKH MOHAMMAD;)	
WALID MUHAMMAD SALIH)	
MUBARAK BIN ATTASH;)	
RAMZI BINALSHIBH;)	
ALI ABDUL AZIZ ALI;)	
MUSTAFA AHMED ADAM AL)	_____ April 2012
HAWSAWI)	

Upon consideration of the Government's request to maintain UNDER SEAL the classified declarations of: David H. Petraeus, Director, Central Intelligence Agency, dated 7 April 2012; Information Review Officer, Central Intelligence Agency, dated 12 April 2012; General Douglas M. Fraser, United States Air Force, Commander, United States Southern Command, dated 24 October 2011; Mark F. Guiliano, Assistant Director, Counterterrorism Division, Federal Bureau of Investigation, dated 7 September 2011, (the "Declarations"), and pursuant to the Commission's authority under the Military Commissions Act of 2009, 10 U.S.C. § 948a, *et. seq.*, Rule for Military Commissions 806, Military Commission Rules of Evidence 104, 505-507, and the general supervisory authority of the Commission;

IT IS HEREBY ORDERED that the Declarations contain classified and sensitive but unclassified information that, if publicly released, could reasonably be expected to damage

UNCLASSIFIED//FOR PUBLIC RELEASE

national security and threaten the safety of individuals, and shall therefore be kept UNDER

SEAL.

SO ORDERED:

DATED: _____

James L. Pohl
COL, JA, USA
Military Judge

UNCLASSIFIED//FOR PUBLIC RELEASE

CERTIFICATE OF SERVICE

I certify that on the 26 day of April 2012, I filed AE 013, the **Government's Motion To Protect Against Disclosure of National Security Information** with the Office of Military Commissions Trial Judiciary and I served a copy on counsel of record.

//s//

Joanna Baltes
Deputy Trial Counsel
Office of the Chief Prosecutor
Office of Military Commissions

Tab 2

**Military Commissions Trial Judiciary
Guantanamo Bay, Cuba**

UNITED STATES OF AMERICA

v.

KHALID SHAIKH MOHAMMAD,
WALID MUHAMMAD SALIH MUBARAK
BIN 'ATTASH,
RAMZI BINALSHIBH,
ALI ABDUL AZIZ ALI ,
MUSTAFA AHMED ADAM AL-HAWSAWI

**Motion of the
American Civil Liberties Union**
for Public Access to Proceedings and
Records

May 2, 2012

- 1. Timeliness.** There is no established timeframe for the filing of this motion in the Rules of Court (“RC”) or the 2011 Regulation for Trial by Military Commission (“Regulation”).
- 2. Relief Sought.** The American Civil Liberties Union and the American Civil Liberties Union Foundation (together, the “ACLU”), respectfully request that this Military Commission grant the public meaningful access to the proceedings against Khalid Shaikh Mohammad, Walid Muhammad Salih Mubarak Bin ‘Attash, Ramzi Binalshibh, Ali Abdul Aziz Ali, and Mustafa Ahmed Adam Al-Hawsawi, as required by the Constitution and the Military Commissions Act. Specifically, the ACLU, on behalf of itself and its members, challenges the portions of the U.S. government’s proposed protective order that would permit the government to suppress defendants’ statements about their detention and treatment, including torture and other abuse, in U.S. custody. The ACLU requests that this Commission deny the government’s request: (1) to prevent the public, press, and trial observers from hearing the defendants’ statements concerning their personal knowledge of their detention and treatment in U.S. custody; and (2) for a 40-second delay

in the audio feed of the commission proceedings to the public, press and trial observers. If the Commission grants the government's request for a 40-second audio delay, the ACLU alternatively requests that the Commission order the public release of unredacted transcripts containing the defendants' statements on an expedited basis to minimize the infringement on the public's right of contemporaneous access to the proceedings.

3. Overview. Both the Constitution and the Military Commissions Act of 2009 ("MCA") recognize the public's presumptive right of access to all proceedings and records of this historic military commission. That right of access may only be overcome if there is a countervailing interest of "transcendent" importance, a standard that the government's extraordinary and draconian proposed restrictions cannot meet. The government asks this Commission to suppress as presumptively classified the defendants' every utterance concerning their personal knowledge of their detention and abuse in CIA custody. It also asks the Commission to suppress as classified the defendants' personal knowledge of their detention and treatment by the Department of Defense. Based on these improper classification claims, the government seeks a 40-second time delay for the audio feed of these proceedings. That delay renders the proceedings presumptively closed by withholding from the public, media, and observers, at the press of a button, any access to detainees' personal accounts of their detention and mistreatment.

In order to adjudicate whether the government's proposed restrictions on the public's right to hear defendants' statements satisfies the First Amendment's strict scrutiny standard, this court must determine whether the government may properly classify defendants' statements. The government cannot. It has no legal authority to classify defendants' statements containing their personal knowledge of the detention and

treatment, including torture, to which they were subjected in U.S. custody—information that defendants acquired by virtue of the government forcing it upon them. In addition, the President of the United States has banned the illegal CIA interrogation techniques to which the defendants were subjected and closed the secret facilities at which they were held. The government’s suppression of defendants’ statements about techniques and detention that are banned and prohibited by law—and that, accordingly, cannot be legitimately employed in the future—is not justified by the government’s interest in protecting legitimate methods, and thus fails strict scrutiny as well. Finally, it is the very antithesis of the narrow tailoring required by the First Amendment for the government to categorically gag defendants when copious details about the CIA’s use of torture and coercive techniques, including on the defendants, have been disclosed publicly in official government documents and other reports and press accounts.

The eyes of the world are on this Military Commission, and the public has a substantial interest in and concern about the fairness and transparency of these proceedings. This Commission should reject—and not become complicit with—the government’s improper proposals to suppress the defendants’ personal accounts of government misconduct.

4. Burden of Proof. As the party advocating restrictions on the public’s right of access to these proceedings, the government bears the burden of meeting the First Amendment’s strict scrutiny test by showing that public access poses a direct threat to an overriding governmental interest. *See Press-Enterprise Co. v. Superior Court*, 464 U.S. 501, 510 (1984) (“*Press-Enterprise I*”); *Press-Enterprise Co. v. Superior Court*, 478 U.S. 1, 15 (1986) (“*Press-Enterprise II*”); *Lugosch v. Pyramid Co. of Onodaga*, 435 F.3d 110,

123–24 (2d Cir. 2006); *ABC, Inc. v. Stewart*, 360 F.3d 90, 106 (2d Cir. 2004); *Wash. Post v. Robinson*, 935 F.2d 282, 288 (D.C. Cir. 1991).

5. Statement of Facts. On May 5, 2012, five men accused of involvement in the September 11th attacks will be arraigned before this Military Commission on capital charges of murder, conspiracy, and other terrorism offenses. This Commission has recognized that “due to the serious nature of the crimes alleged and the historic nature of military commissions, there is significant public interest in the Commission proceedings.” Order, Government Mot. for Public Access to Open Proceedings of this Military Commission, Apr. 26, 2012 (AE 007B) at 1.

On April 26, 2011, the government filed with this Commission a Motion to Protect Against Disclosure of National Security Information (AE 013). That motion has not yet been made public, but the ACLU expects that it or another government motion to be filed and/or made public on or before May 5 will apply to the May 5 arraignment and all other proceedings, and is or will be similar in sum and substance to the government’s motion for a protective order in *United States v. Al-Nashiri*, filed on October 28, 2011 as AE 013 in that case (“Gov’t Al-Nashiri Mot.”).

Based on the government’s filing in the *Al-Nashiri* Commission and the positions it has taken in its previous prosecution of these defendants,¹ the government has asked or

¹ On June 4, 2008, the day before defendants’ first arraignment, the government requested (AE 032B) and the Commission judge granted (AE 032A) a protective order “treating” defendants’ statements as presumptively classified based on the judge’s finding that the defendants had “been exposed to information that the U.S. government continues to protect as properly classified.” AE 032A ¶¶ 24, 26. The protective order permitted a 20-second audio feed delay. ¶¶ 27–37. At the arraignment, the audio feed was cut off and the arraignment transcript redacted when defendant Binalshibh began to discuss his detention at CIA black sites and conditions at Guantanamo, and when defendant Mohammad mentioned waterboarding and “actions” taken against him in 2005 (when he was in CIA custody). A full list of redactions of the defendants’ statements at the 2008 arraignment is available at <http://www.mc.mil/CASES/MilitaryCommissions.aspx>.

will ask this Commission to issue a protective order accepting the government's claim that any statements made by the defendants concerning their "exposure" to the Central Intelligence Agency's ("CIA") detention and interrogation program are presumptively classified and must be kept from the public. The government has also asked or will ask the Commission to accept its assertion that defendants' statements concerning their personal knowledge and experience of their imprisonment and treatment in Department of Defense ("DOD") custody are classified and must be suppressed. Based on these claims, the government has requested or will request that the Commission order a 40-second delay in the audio feed the government makes available to the public, media, and representatives of non-governmental organizations who observe the tribunal either via closed-circuit video or in a soundproof viewing room separated from the courtroom by a panel of sound-proof glass. The 40-second delay will permit a courtroom security official to cut off the audio feed whenever the defendants describe their detention and interrogation in U.S. custody.

The ACLU files this motion constrained by the lack of a public government filing that it can timely challenge before the May 5 arraignment and, therefore, the ACLU's legal arguments are based on the government's motion for a protective order in the *Al-Nashiri* case and filings in the previous Commission prosecution of these defendants. The ACLU reserves the right to supplement its motion once the government's motion for a protective order in this prosecution is made public.

6. Legal Basis for Relief Requested. The public's right of access to the proceedings of this tribunal is mandated by the Constitution of the United States and expressly granted by the MCA. The government has no legitimate basis under the First Amendment or the

MCA to limit that access by presumptively and categorically designating the defendants' speech, based on their personal knowledge of the government's detention and interrogation regime, as classified. The ACLU has standing to seek access to these court proceedings under the Constitution and regulations promulgated by the Department of Defense pursuant to the MCA.²

A. The First Amendment Protects the Public's Right of Meaningful Access to Proceedings and Records of Adjudicative Military Tribunals.

1. The First Amendment Right of Access Extends to Military Commissions.

The First Amendment "protects the public and the press from abridgement of their rights of access to information about the operation of their government." *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 584 (1980) (Stevens, J., concurring) (recognizing First Amendment right of public access to criminal trials); *Globe Newspaper*, 457 U.S. at 604–06 (same); *Press-Enterprise I*, 464 U.S. at 508–10, 513 (recognizing First Amendment right of public access to *voir dire* proceedings); *Press-Enterprise II*, 478 U.S. at 10 (same as to preliminary hearings in a criminal prosecution). The scope of this constitutional right was first defined by the U.S. Supreme Court in *Richmond Newspapers*, a case involving access to a criminal trial that the State of Virginia had conducted entirely in secret. Although a Virginia statute specifically granted the trial judge discretion to conduct a secret trial, the Supreme Court held that the First

² *Globe Newspaper Co. v. Superior Court*, 457 U.S. 596, 609 n.25 (1982) ("[R]epresentatives of the press and general public 'must be given an opportunity to be heard on the question of their exclusion.'"); *Phoenix Newspapers, Inc. v. U.S. Dist. Court*, 156 F.3d 940, 949 (9th Cir. 1998) (requiring court to "provide sufficient notice to the public and press to afford them the opportunity to object or offer alternatives. If objections are made, a hearing on the objections must be held as soon as possible."); see also *Nixon v. Warner Communications, Inc.*, 435 U.S. 589, 597–98 (1978). Moreover, the ACLU has been recognized as a "national organization" by the Office of the Secretary of Defense under the Rules for Military Commissions 806(a), and has standing to assert its rights under statutory and constitutional law for access to the proceedings. The 2011 Regulation for Trial by Military Commission specifically permits a third party, like the ACLU, to challenge whether information presented in these proceedings "may be released to the public." Regulation 19-3(c) and (d).

UNCLASSIFIED
FOR PUBLIC RELEASE

Amendment created an affirmative, enforceable constitutional right of access to certain government proceedings, such as a criminal trial.³

The public's right of access exists where government proceedings and information historically have been available to the public, and public access plays a "significant positive role" in the functioning of government. *E.g.*, *Globe Newspaper*, 457 U.S. at 605–07; *Press-Enterprise II*, 478 U.S. at 8–9; *Wash. Post*, 935 F.2d at 287–92. Under the "experience" and "logic" analysis applied by the Supreme Court, the right of access "has special force" when it carries the "favorable judgment of experience," but what is "crucial" in deciding where an access right exists "is whether access to a particular government process is important in terms of that very process." *Richmond Newspapers*, 448 U.S. at 589 (Brennan, J., concurring); *see also Globe Newspaper*, 457 U.S. at 605–06; *Press-Enterprise II*, 478 U.S. at 89; *United States v. Simone*, 14 F.3d 833, 837 (3d Cir. 1994); *Capital Cities Media, Inc. v. Chester*, 797 F.2d 1164, 1173 (3d Cir. 1986).⁴

Based upon the same experience and logic tests, a First Amendment right of public access also attaches to proceedings of adjudicative military tribunals, including military commissions. *See, e.g.*, *United States v. Anderson*, 46 M.J. 728, 729 (A. Ct. Crim. App. 1997) (per curiam) (absent adequate justification clearly set forth on the record, "trials in the United States military justice system are to be open to the public");

³ *See Richmond Newspapers*, 448 U.S. at 577 (Burger, J.) (the right of access is "assured by the amalgam of the First Amendment guarantees of speech and press" and their "affinity to the right of assembly"); *id.* at 585 (Brennan, J., concurring) (First Amendment secures "a public right of access.").

⁴ While this right has most frequently been asserted to compel access to judicial proceedings and documents, the right also applies to proceedings and information in the executive and legislative branches. *E.g.*, *Detroit Free Press v. Ashcroft*, 303 F.3d 681, 695–96, 700 (6th Cir. 2002) (right of access to executive branch deportation proceedings); *Soc'y of Prof'l Journalists v. Sec'y of Labor*, 616 F. Supp. 569, 574–75 (D. Utah 1985) (administrative hearing), *vacated as moot*, 832 F.2d 1180 (10th Cir. 1987).

see also ABC, Inc. v. Powell, 47 M.J. 363, 366 (C.A.A.F. 1997) (First Amendment right of public access applies to investigations under Art. 32); *United States v. Travers*, 25 M.J. 61, 62 (C.M.A. 1987) (First Amendment right of public access extends to courts-martial); *United States v. Hershey*, 20 M.J. 433, 436 & 438 n.6 (C.M.A. 1985) (same); *United States v. Scott*, 48 M.J. 663, 665 (A. Ct. Crim. App. 1998) (same); *United States v. Story*, 35 M.J. 677, 677 (A. Ct. Crim. App. 1992) (per curiam) (same).

Historical Experience. Our nation has a well-established tradition of public access to adjudicative military tribunals. William Winthrop, the “Blackstone of Military Law” (*Reid v. Covert*, 354 U.S. 1, 19 n.38 (1957) (plurality opinion)), described in his classic military law opus a history of open proceedings that dates back centuries. William Winthrop, *Military Law and Precedents* 161–62 (rev. 2d ed. 1920) (“Winthrop”) (“Originally, (under the Carolingian Kings,) courts-martial . . . were *held in the open air*, and in the Code of Gustavus Adolphus . . . criminal cases before such courts were required to be tried ‘*under the blue skies*.’ The modern practice has inherited a similar publicity.”). Based on this long tradition of access, military courts recognized the right to public access to trials even before the Supreme Court recognized the First Amendment right of public access to criminal proceedings in *Richmond Newspapers*. *United States v. Brown*, 22 C.M.R. 41, 48 (C.M.A. 1956), *overruled, in part, on other grounds by United States v. Grunden*, 2 M.J. 116, 116 (C.M.A. 1977); *see also Hamdan v. Rumsfeld*, 548 U.S. 557, 617, 623 (2006) (“[T]he procedures governing trials by military commission historically have been the same as those governing courts-martial.”).

History’s lesson is clear: almost without exception, the thousands of military commissions held during wartime in our nation’s history have been conducted publicly.

Ex. A (Decl. of David Glazier ¶ 4, Apr. 30, 2011) (“Evidence of the openness of military commissions can be found in the publicly available descriptions of virtually every historically significant military commission trial, including those of Lambden Milligan [sic], John Y. Beall, and the Lincoln assassination conspirators in the Civil War; the Dakota Sioux and Modoc Indian trials, and scores of war crimes trials in the aftermath of World War II.”). It is also clear that secrecy in military commissions is the exception, one that history judges harshly:

The one well-known historical anomaly, a closed military commission trial, took place in the *Quirin* case. That case concerned eight Nazi saboteurs who crossed the Atlantic in German U-boats [and landed in the United States]. . . . Some commentators have noted it may have been closed to avoid embarrassment to the U.S. government over its perceived incompetence in preventing the landings and the subsequent interagency bungling What is clear, however, is that the secrecy of the proceeding contributed to what is widely acknowledged as the tarnished legacy of that case.

Id. ¶ 5.⁵

Policies Advanced by Public Access. The logic prong of the Supreme Court’s test for public access is unquestionably met here because of the “historic nature” of the proceedings against the defendants and the public’s interest in the fairness and transparency of these proceedings. There is also substantial public and press interest in the circumstances of the defendants’ capture and the legality of their detention and interrogation in U.S. custody. *See Richmond Newspapers*, 448 U.S. at 569–71 (the interests advanced by open adjudicatory criminal proceedings include (1) ensuring that

⁵ It is now widely believed that the “real reason President Roosevelt authorized these military tribunals [in *Quirin*] was to keep evidence of the FBI’s bungling of the case secret.” *Department of Justice Oversight: Preserving Our Freedoms While Defending Against Terrorism: Hearings Before the Senate Comm. on the Judiciary*, 107th Cong. 377 (2001) (statement of Neal Katyal, Visiting Professor, Yale Law School, and Professor of Law, Georgetown University), available at <http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1095&context=cong>.

proper procedures are being followed; (2) discouraging biased decisions; (3) providing an outlet for community hostility and emotion; (4) ensuring public confidence in a trial's results through the appearance of fairness; and (5) inspiring confidence in government through public education regarding the methods followed and remedies granted by government). Our nation's courts recognize that the truth, no matter how ugly, is better aired than concealed, and that the legitimacy of adjudicatory tribunals is undermined by secrecy.

Thus, just as with civilian judicial proceedings, military courts recognize that an open military proceeding "reduces the chance of arbitrary or capricious decisions and enhances public confidence," which would "quickly erode" if proceedings are arbitrarily closed. *Scott*, 48 M.J. at 665 (citations and internal quotation marks omitted); *see also Anderson*, 46 M.J. at 731 (same). Indeed, even before the Supreme Court recognized the right of access to criminal proceedings in *Richmond Newspapers*, the Court of Military Appeals had identified the functional benefits of public proceedings: (1) improving the quality of testimony; (2) curbing abuses of authority; and (3) fostering greater public confidence in the proceedings. *See Brown*, 22 C.M.R. at 45–48; *Hershey*, 20 M.J. at 436; *see also United States v. Hood*, 46 M.J. 728, 731 n.2 (A. Ct. Crim. App. 1996). Whether this adjudicative military commission is seen as legitimate and inspires public confidence depends in part on the openness of the proceedings it holds.

2. The Presumption of Public Access Can Only Be Overcome by An Overriding Interest That is Narrowly Tailored.

The public's constitutional right of open access to these military commission proceedings can be overcome only if there is a countervailing interest of "transcendent" importance. *Richmond Newspapers*, 448 U.S. at 581; *Press-Enterprise Co. II*, 464 U.S.

at 510. The adjudicatory tribunals of the military branches apply this same standard. As explained in *Hershey*, “the party seeking closure must advance an overriding interest that is likely to be prejudiced [by openness]; the closure must be narrowly tailored to protect that interest; the trial court must consider reasonable alternatives to closure; and it must make adequate findings supporting the closure to aid in review.” 20 M.J. at 436; *see also Anderson*, 46 M.J. at 729 (“[T]he military judge placed no justification on the record for her actions. Consequently, she abused her discretion in closing the court-martial.”); *Scott*, 48 M.J. at 665. If access is to be denied, judicial findings on the need for closure or sealing must be entered as written findings of fact, made with sufficient specificity to allow appellate review. *Press-Enterprise II*, 478 U.S. at 9–10, 14.

B. The Military Commissions Act and its Implementing Regulations Require Meaningful Public Access to All Commission Proceedings.

In adopting the Military Commissions Act in 2006 and again in 2009, Congress recognized that it is critically important for these criminal proceedings to be conducted in the open so their validity is accepted by the public. Pub. L. No. 109-366, 120 Stat. 2600 (2006) (codified as amended 10 U.S.C. §§ 949–950 (2009)) (“MCA”). The MCA thus expressly mandates access by “the public” to all “proceedings” of any military commission, unless specifically delineated exceptions are found to apply. 10 U.S.C. § 949d(c)(1).

The statutory right of access is recognized and implemented in both the 2011 Regulation for Trial by Military Commissions and the 2010 Manual for Military Commissions (“Manual”) containing the 2010 Rules for Military Commissions (“2010 RMC”). *See* Regulation 19-6 (“The proceedings of military commissions *shall* be public to the maximum extent practicable.” (emphasis added)); 2010 RMC 806(a) (“[M]ilitary

commissions *shall* be publicly held.” (emphasis added)). The MCA and its implementing regulations make clear that the public’s right of access extends beyond the “trial” to all aspects of the “proceeding” against an accused. 10 U.S.C. § 949d(c). Under the Regulation, the right of access applies “from the swearing of charges until the completion of trial and appellate proceedings or any final disposition of the case.” Reg. MC 19-2. Motions, rulings, and summaries of Rule 802 conferences are all required to be part of the Record of Trial, and thus expressly subject to the right of access. The 2010 Manual also identifies pre-trial motions as being among the “proceedings” that a judge controls.

C. This Commission Must Adjudicate the Propriety of the Government’s Proposed Categorical Classification of Defendants’ Statements.

This Commission must review the government’s proposed categorical classification of defendants’ statements about their detention and mistreatment under the First Amendment’s strict scrutiny standard, and make specific factual findings on the record before permitting any national-security-related closure. *Grunden*, 2 M.J. at 121 (“The blanket exclusion of the spectators from all or most of a trial . . . has not been approved . . . nor could it be absent a compelling showing that such was necessary to prevent the disclosure of classified information.”); *see also Richmond Newspapers*, 448 U.S. at 581; *Globe Newspaper*, 457 U.S. at 606–07; *Press-Enterprise II*, 478 U.S. at 13–14. The MCA supports this demanding standard, permitting this Court to deny public access to the proceedings “*only* upon making a *specific finding* that such closure *is necessary* to — (A) protect information the disclosure of which could reasonably be expected to cause damage to the national security, including intelligence or law enforcement sources, methods, or activities; or (B) ensure the physical safety of individuals.” 10 U.S.C. § 949d(c)(2) (emphases added).

UNCLASSIFIED
FOR PUBLIC RELEASE

Only the Military Commission judge, and not the government, may make the decision to limit public access to these commission proceedings. 10 U.S.C. § 949d(c) (“The *military judge* may close to the public all or part of the proceedings of a military commission under this chapter.” (emphasis added)). Part of the military judge’s obligation in ruling on a government request to close proceedings is assessing whether purportedly classified information is in fact properly classified. *Grunden*, 2 M.J. at 122–23 & n.14 (“Before a trial judge can order the exclusion of the public on this basis, he must be satisfied from all the evidence and circumstances that there is a reasonable danger that presentation of these materials before the public will expose military matters which in the interest of national security should not be divulged.”);⁶ *see also* 10 U.S.C. § 949d(c)(2).

The government may argue that MCA Sections 949p-1(a) and (c) bar this Commission from independently determining the propriety of the government’s decision to classify the defendants’ personal knowledge of their detention and treatment. The Commission should reject any such argument, and has three grounds on which to do so.

First, the Commission should find that Section 949p-1(a) permits it to determine that only *properly* classified information may be withheld from the public, and thus that the military judge has the authority to review the government’s classification decisions.⁷ This is what the term “classified information” in the statute clearly requires; it is

⁶ Although *Grunden* was decided under the Sixth Amendment right to a public trial, the considerations and procedures set forth in the opinion apply equally to First Amendment right-of-access challenges. *See Powell*, 47 M.J. at 365 (“[W]hen an accused is entitled to a public hearing, the press enjoys the same right and has standing to complain if access is denied.”).

⁷ MCA Section 949p-1(a) reads:

Classified information shall be protected and is privileged from disclosure if disclosure would be detrimental to the national security. Under no circumstances may a military judge order the release of classified information to any person not authorized to receive such information.

elementary that in order to designate information as classified, the government must properly adhere to the requirements of the relevant executive order. *See* Exec. Order No. 13,526, 75 Fed. Reg. 707 § 1.1(a) (Dec. 29, 2009). This reading would avoid conflict with the military judge’s constitutional obligation to adjudicate whether the government’s classification decisions constitute a “transcendent” interest that overrides the public’s First Amendment right of access. *See Gomez v. United States*, 490 U.S. 858, 864 (1989) (“It is our settled policy to avoid an interpretation of a federal statute that engenders constitutional issues if a reasonable alternative interpretation poses no constitutional question.”).

Second, the Commission should find that a plain text reading of Section 949p-1(c) limits its application to evidence presented by the government.⁸ The plain language of Section 949p-1(c) constrains only the military judge’s power to review a decision not to declassify evidence *submitted by the prosecution* at trial, not information presented by the defense, including statements of the accused.⁹ Indeed, the provision makes no mention of the defense or the accused. Thus, the military judge’s authority to scrutinize strictly the government’s purported classification of information that is within the personal knowledge of the defendants is unaffected by Section 949p-1(c). This plain text reading also avoids any conflict with the military judge’s obligation to determine whether the

⁸ MCA Section 949p-1(c) reads:

Trial counsel shall work with the original classification authorities for evidence that may be used at trial to ensure that such evidence is declassified to the maximum extent possible, consistent with the requirements of national security. A decision not to declassify evidence under this section shall not be subject to review by a military commission or upon appeal.

⁹ The ACLU does not concede that this reading of Section 949p-1(c) is a constitutionally permissible restriction on the judge’s authority with respect to classified information the government seeks to offer at trial, but this Commission need not reach this issue in order to decide the instant motion.

government's classification decisions may override the public's First Amendment's right of access.

Third, and in the alternative, if this Commission were to find that Sections 949p-1(a) and (c) bar it from reviewing the propriety of the government's proposed classification of defendants' statements, it must find those provisions unconstitutional as applied. That is because, read as a complete bar, the provisions would unconstitutionally prevent the military judge from fulfilling his mandate to preserve the public's First Amendment right of access to proceedings and to close proceedings *only* when necessary to protect *properly* classified national security information. The military judge has the authority to strike down the provisions under well-established civilian and military precedent.

It is a fundamental tenet of our constitutional system that federal statutes that are inconsistent with the Constitution and the Bill of Rights are invalid, and that courts have the power to hold statutes unconstitutional on their face or as applied. *See Marbury v. Madison*, 5 U.S. (1 Cranch) 137 (1803). There is no question that a federal court faced with provisions analogous to Sections 949p-1(a) and (c) would be empowered to find them unconstitutional as applied. Federal courts routinely consider the impact of the First Amendment on federal statutory and regulatory schemes dealing with control and release of classified information. *See, e.g., Wilson v. CIA*, 586 F.3d 171, 183–84 (2009) (evaluating constitutionality of government pre-publication review of book by former CIA employee); *Doe v. Gonzales*, 500 F. Supp. 2d 379, 411 (S.D.N.Y. 2007), affirmed in part and reversed in part sub nom *John Doe, Inc. v. Mukasey*, 549 F.3d 861 (2d Cir. 2008) (“Congress cannot legislate a constitutional standard of review that contradicts or

supercedes what the courts have determined to be the standard applicable under the First Amendment for that purpose.”).

Military courts, no less than civilian courts, have the power to invalidate federal statutes or their specific provisions on constitutional grounds. In *United States v. Matthews*, 16 M.J. 354 (C.M.A. 1983), the Court of Military Appeals (“CMA”) squarely rejected the prosecution’s argument that, because it was a military court constituted under Article I of the Constitution, it lacked authority to rule on the constitutionality of provisions of the Uniform Code of Military Justice. The CMA noted that there is no absolute bar on Article I courts adjudicating the constitutionality of statutes, and that military courts’ exercise of their judicial power includes the power to declare statutes unconstitutional. *Id.* at 364–66. It further explained that Congress is empowered by Article I of the Constitution to establish military courts, “with judges who are sworn to uphold the Constitution,” and it would be “anomalous” if Congress could not “authorize those judges to refuse to enforce statutes which they determine are unconstitutional.” *Id.* at 366. Indeed, the CMA held that precluding military judges from deciding constitutional issues “would itself raise the constitutional question whether a judge—even one appointed under Article I, rather than under Article III—could be required by oath to support the Constitution of the United States, *see* U.S. Const. art. VI, but at the same time be forced to make decisions and render judgments based on statutes which he concluded were contrary to that Constitution.” *Id.*; *see also* *U.S. Navy-Marine Corps. Court of Military Review v. Carlucci*, 26 M.J. 328, 332 (C.M.A. 1988); *United States v. Graf*, 35 M.J. 450, 461–66 (C.M.A. 1992).¹⁰ Military courts also routinely consider whether

¹⁰ Inferior military courts also have the power to review the constitutionality of statutes, and frequently do so. *See, e.g., United States v. Turner*, 30 M.J. 1276, 1277–83 (N-M.C.M.R. 1990); *United States v. Herd*,

federal statutes are unconstitutional as applied. *See, e.g., United States v. Wilson*, 66 M.J. 39, 50–51 (C.A.A.F. 2008) (“[T]his Court may decide to hold the statute unconstitutional as applied in certain circumstances”); *United States v. Gorski*, 47 M.J. 370, 371 (C.A.A.F. 1997); *United States v. Lumagui*, 31 M.J. 789, 790 (A.F.C.M.R. 1990); *United States v. Stratton*, 2012 WL 244062, at *1 (N-M. Ct. Crim. App. Jan. 26, 2012).

This Commission is empowered to declare Sections 949p-1(a) and (c) unconstitutional as applied for the same reasons that judges presiding over other courts in the military justice system could do so. *Cf. Matthews*, 16 M.J. at 366 (military judges are judicial officers who are “required by oath to support the Constitution of the United States”). Accordingly, if this Commission interprets Sections 949p-1(a) and (c) to preclude it from reviewing the propriety of the government’s classification claims in deciding whether to limit the public’s right to open commission proceedings, the provisions are an unconstitutional infringement on the First Amendment and must be ruled as such.

D. There is No Legitimate Basis for the Government’s Categorical Suppression of Defendants’ Statements Concerning Abuse and Mistreatment

The government has invoked or will invoke Executive Order No. 13,526, or its predecessor Orders, for its classification authority. Gov’t Al-Nashiri Mot. 7. Executive Order No. 13,526 provides a comprehensive system for classifying national security information, and contains four prerequisites: (1) the information must be classified by an “original classification authority”; (2) the information must be “owned by” or “under the control of” the government; (3) the information must fall within one of the authorized withholding categories under this order; and (4) the original classification authority must

29 M.J. 702, 705–08 (A.C.M.R. 1989); *United States v. Allen*, 1999 WL 305093, at *2 (A.F. Ct. Crim. App. Apr. 22, 1999).

UNCLASSIFIED
FOR PUBLIC RELEASE

“determine[] that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security” and must be “able to identify or describe the damage.” Exec. Order No. 13,526, § 1.1(a). To be properly classified, agency information must fall within an authorized withholding category set forth in the Executive Order; the government has or will rely on two: “intelligence activities (including covert action), intelligence sources or methods,” and “foreign activities of the United States.” *Id.* § 1.4(c), (d); Gov’t Al-Nashiri Mot. 2, 5.

The government’s claims that defendants’ statements about their detention and treatment in U.S. custody may be classified fail because: (1) the government has no authority to classify information within the defendants’ personal knowledge and experience, and which they acquired by virtue of having it involuntarily imposed on them by the government; (2) the President of the United States has banned the “enhanced interrogation techniques” to which defendants were subjected, and ordered permanently closed the CIA sites at which they were held; and (3) the information the government seeks to suppress has been declassified already and is publicly available. Moreover, because “enhanced interrogation techniques” are banned, the CIA sites closed, and information about the U.S. government’s detention and mistreatment of the defendants public, defendants’ statements on these issues would not harm the national security. The government’s classification claims are therefore not legitimate and do not override the public’s right to hear defendants’ statements. *Richmond Newspapers*, 448 U.S. at 581; *Press-Enterprise Co. II*, 464 U.S. at 510.

1. The government may not classify information within the defendants' personal knowledge.

The government seeks to censor defendants' statements based on a chillingly Orwellian claim: because a defendant was "detained and interrogated in the CIA program" of secret detention, torture, and abuse, he was "exposed to classified sources, methods, and activities" and must be gagged lest he reveal his knowledge of what the government did to him. Gov't Al-Nashiri Mot. 3. It makes a similar claim with respect to defendants' knowledge of DOD sources, methods, and activities at Guantanamo. *Id.* at 5. But the government has no legal authority to classify statements based on the defendants' personal knowledge and experience of government conduct. The Executive Order's threshold requirement for classification, that national security information be "owned by . . . or [be] under the control of the United States Government," simply may not be categorically extended to *human beings* under the government's control, let alone to individuals who were "exposed" to classified information by virtue of having it forcibly imposed on them by the government. Exec. Order 13,526, § 1.1(a)(2).

Although the government may enjoin the disclosure of information by a government employee in ways that, if imposed on private individuals, would be unlawful, "this principle implies a substantially *voluntary assumption* of special burdens in exchange for special opportunities." *Wright v. F.B.I.*, 2006 WL 2587630, at *6 (D.D.C. July 31, 2006) (emphasis added); *see also McGehee v. Casey*, 718 F.2d 1137, 1143 n.11 (D.C. Cir. 1983) ("One who enters the foreign intelligence service thereby occupies a position of 'special trust' reached by few in government"); *Stillman v. CIA*, 517 F. Supp. 2d 32, 37 (D.D.C. 2007) (former CIA employee foreclosed from publicly discussing information obtained after his termination under broad terms of non-disclosure

agreements signed in consideration for offer of CIA employment). Unlike government employees or others in privity with the government, who might be contractually obligated to keep their knowledge and experiences secret, the defendants' "exposure" to the CIA torture and secret detention program and their detention and treatment in DOD custody have obviously not been voluntary, nor based on a special relationship of trust. The government has no legal authority to restrict information that comes from the defendants' own personal knowledge and observations.

Similarly, the defendants' statements about interrogation techniques and places or conditions of confinement are not protectable "activities, sources and methods" or "foreign activities" under the Executive Order because the government lacks the authority to classify information that detainees know based on their personal observations and experiences. There is no authority for the extraordinary proposition that the government's detention and interrogation of a prisoner somehow creates a new, unwritten power to classify any and all utterances made by that prisoner concerning his own knowledge of his whereabouts, incarceration, and treatment. Indeed, if the government were correct that the defendants' "exposure" to its "foreign activities" or "activities, sources and methods" justified the enforcement of a gag on defendants' statements about their experience, then surely it would follow that whoever in government was responsible for disclosing the classified information to terrorism suspects must have violated criminal statutes prohibiting transmission of intelligence secrets to anyone unauthorized to receive them. *See, e.g.*, 18 U.S.C. § 793(d) and (f).¹¹ That is an absurd proposition, to be sure,

¹¹ "Whoever, lawfully having possession of . . . information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated,

but no more so than the notion that when the government detains a person and applies coercive interrogation techniques against him, that person's statements or allegations of government misconduct must be suppressed.

The reality is that the government's practical authority – and ability – to suppress the defendants' descriptions of their own experiences of detention and mistreatment derives solely from its decision to detain defendants and either keep them in detention indefinitely or seek to impose the death penalty without permitting the knowledge they have to be revealed. This Commission should not accept – and become complicit in – the government's improper classification of detainees' statements based on their own knowledge and experience of their detention and abuse in U.S. custody.

2. The President of the United States has Categorically Banned the CIA's Coercive Interrogation and Secret Detention program.

The government's rationale for its proposed presumptive classification of defendants' statements about their "exposure" to the CIA's detention and interrogation program is that revelation would disclose the means by which the United States "defends against international terrorism and terrorist organizations" and result in damage to the national security. Gov't Al-Nashiri Mot. 7. But the government can have no legitimate interest, let alone a compelling one, in preserving its ability to use a "program" that the President of the United States has banned and that is prohibited by law. A protective order that permits the suppression of statements about clearly prohibited and illegal activities is overbroad on its face.

delivered, or transmitted . . . to any person not entitled to receive it . . . Shall be fined under this title or imprisoned not more than ten years, or both." 18 U.S.C. § 793(d).

UNCLASSIFIED
FOR PUBLIC RELEASE

The seminal Supreme Court case interpreting the government's authority to classify "intelligence sources and methods" makes clear that the CIA may withhold information about only those sources or methods that "fall within the Agency's mandate." *CIA v. Sims*, 471 U.S. 159, 169 (1985). The CIA's so-called "enhanced interrogation techniques" have been categorically prohibited by the President, and its overseas detention and interrogation facilities have been permanently closed. *See* Exec. Order No. 13,491, 74 Fed. Reg. 4893 (Jan. 22, 2009). Thus, neither the illegal "enhanced interrogation techniques," nor secret overseas detention is within the Agency's mandate. Even assuming that they did at one point legitimately and lawfully fall within the CIA's mandate, no amount of disclosure about their use in the past could reveal details about current "activities, sources and methods" that may be legitimately protected.

President Obama shares this view. In 2009, he ordered the release of the legal memos upon which the CIA relied for its interrogation program. Upon release of the memos, the President stated:

First, the interrogation techniques described in these memos have already been widely reported. Second, the previous Administration publicly acknowledged portions of the program – and some of the practices – associated with these memos. Third, I have already ended the techniques described in the memos through an Executive Order. Therefore, withholding these memos would only serve to deny facts that have been in the public domain for some time.¹²

When the President himself has squarely rejected the argument that further dissemination of details of interrogation techniques would cause harm to national security, the CIA (as the "original classification authority") has no basis to assert that claim. The President's determination is, in effect, a finding by the Chief Executive that

¹² President Barack Obama, Statement on Release of OLC Memos (April 16, 2009), *available at* http://www.whitehouse.gov/the_press_office/Statement-of-President-Barack-Obama-on-Release-of-OLC-Memos.

the predicate element of the Executive Order upon which the CIA relies no longer applies. The government is now indisputably foreclosed from claiming that classification of such information is authorized on the ground that it “could reasonably be expected to result in damage to the national security.”

The use of illegal interrogation methods on prisoners is also expressly prohibited by U.S. law, *see* 18 U.S.C. § 2340A (providing for prosecution of a U.S. national or anyone present in the U.S. who, while outside the U.S., commits or attempts to commit torture); 18 U.S.C. § 2441 (making it a criminal offense for U.S. military personnel and U.S. nationals to commit grave breaches of Common Article 3 of the Geneva Convention), and by international law, *see* Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, Dec. 10, 1984, 108 Stat. 382, 1465 U.N.T.S. 85. Neither the CIA nor DOD is exempt from these laws. Detainee Treatment Act of 2005, Pub. L. No. 109-148, 119 Stat. 2680, § 1003 (2005) (“No individual in the custody or under the physical control of the United States Government, regardless of nationality or physical location, shall be subject to cruel, inhuman, or degrading treatment or punishment.”); *see also* 109 Cong. Rec. S14257 (statement of Sen. Carl Levin) (stating that with enactment into law of this provision, “the United States will put itself on record as rejecting any effort to claim that these words have one meaning as they apply to the Department of Defense and another meaning as they apply to the CIA”).

Similarly unlawful are the practices of extraordinary rendition and secret detention. Extraordinary rendition contravenes the Foreign Affairs Reform and Restructuring Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681–822 § 2242, which states that the United States “[shall] not . . . expel, extradite, or otherwise effect the involuntary

return of any person to a country in which there are substantial grounds for believing the person would be in danger of being subjected to torture, regardless of whether the person is physically present in the United States,” and Article 3 of the Convention Against Torture, which includes a similar proscription. Secret detention is prohibited by both the Geneva Conventions, *see* Third Geneva Convention Relative to the Treatment of Prisoners of War, art. 122–25, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Fourth Geneva Convention relative to the Protection of Civilian Persons in Time of War, art. 136–4, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287; and by the UN Standard Minimum Rules for the Treatment of Prisoners and the UN Body of Principles for the Protection of All Persons Under Any Form of Detention or Imprisonment. The government does not have any legitimate interest in preserving the effectiveness of interrogation and detention methods that it is not authorized to use in the first place.

Finally, the Executive Order explicitly forbids classification to “conceal violations of law” or to “prevent embarrassment.” Exec. Order No. 13,526, § 1.7(a)(1)–(2). To the extent that the government argues in any classified submission to this tribunal that disclosure of the details of the CIA program would harm the national security on either of these grounds, those arguments must be rejected.

3. The Defendants’ Allegations of Abuse are Already Substantially Declassified and Public

The government cannot argue that the *details* of the CIA’s detention and interrogation program remain categorically classified because numerous publicly available documents – including official, declassified government records – set forth in painstaking detail the types of interrogation techniques that were part of the CIA’s

UNCLASSIFIED
FOR PUBLIC RELEASE

program, the CIA's use of those techniques on prisoners, including defendants, and the locations of the sites at which the CIA held the defendants.

On April 16, 2009, President Obama declassified four Department of Justice memoranda (the "OLC Memos") that purported to authorize, and described in concrete and minute detail, the interrogation techniques that the CIA applied to so-called "High-Value Detainees," including defendants. For example, a memo issued on May 10, 2005, contains nine pages of the CIA's operational details of thirteen "enhanced interrogation techniques," and an additional fifteen pages of descriptions mixed with legal analysis. *See* Memorandum from Steven G. Bradbury, Principal Deputy Assistant Attorney Gen. to John A. Rizzo, Senior Deputy Gen. Counsel, CIA, Re: Application of 18 U.S.C. §§ 2340–2340A to Certain Techniques That May Be Used in the Interrogation of a High Value al Qaeda Detainee (May 10, 2005), *available at* <http://bit.ly/JDphtn> ("Techniques Memo").

The memo makes explicit how the CIA used and intended to use each of the interrogation techniques, including: waterboarding, *id.* at 13, 42–44 (involving "a gurney that is inclined at an angle of 10 to 15 degrees to the horizontal," the pouring of water "from a height of approximately 6 to 18 inches," and applications of water for no more than 40 seconds per "application" and describing the number of times the CIA may waterboard a detainee per session, per day, and per month, and the protocol required for the presence of medical personnel); "sleep deprivation," *id.* at 11–13 (describing operational details); "water dousing," *id.* at 9–10 (describing time limits based on water temperature); and, three specific "stress positions," *id.* at 9 (describing details of the position and angles at which prisoners' heads and limbs would be held).

Significantly, the Techniques Memo also reviewed the CIA's *actual application* of the techniques and their impact. *See, e.g., id.* at 8 (“walling” “is not intended to—and based on experience you have informed us that it does not—inflict any injury or cause severe pain”); *id.* at 11 (“We understand from you that no detainee subjected to [sleep deprivation] by the CIA has suffered any harm or injury, either by falling down and forcing the handcuffs to bear his weight or in any other way.”); *id.* at 11–12 n.15 (“Specifically, you have informed us that on three occasions early in the program, the interrogation team and the attendant medical officers identified the potential for unacceptable edema in the lower limbs of detainees undergoing standing sleep deprivation, and in order to permit the limbs to recover without impairing interrogation requirements, the subjects underwent horizontal sleep deprivation.”); *id.* at 12 (“You have informed us that to date, more than a dozen detainees have been subjected to sleep deprivation of more than 48 hours, and three detainees have been subjected to sleep deprivation of more than 96 hours; the longest period of time for which any detainee has been deprived of sleep by the CIA is 180 hours.”).

Another May 10, 2005 memo assesses the CIA's combined use of the “enhanced interrogation techniques” and describes the operational details of a full-scale “enhanced” interrogation from beginning to end, based on information provided by the CIA. *See* Memorandum from Steven G. Bradbury to John A. Rizzo, Re: Application of 18 U.S.C. §§ 2340–2340A to the Combined Use of Certain Techniques in the Interrogation of High Value al Qaeda Detainees (May 10, 2005), *available at* <http://bit.ly/Iltguh>. The memo describes the phases of interrogation (from “Initial Conditions”, *id.* at 4, to the “Transition to Interrogation” and interrogation itself, including establishing a “baseline,

dependent state” and the use of “corrective” and “coercive” interrogation techniques, *id.* at 4–6)). The memo includes the CIA’s description of a “prototypical interrogation,” which contains detailed information about precisely how the CIA conducted interrogations and employed “enhanced interrogation techniques.” *Id.* at 5–9.

A memo dated May 30, 2005 provides even greater detail about the CIA’s application of specific torture and abusive techniques. *See* Memorandum from Steven G. Bradbury to John A. Rizzo, Re: Application of United States Obligations Under Article 16 of the Convention Against Torture to Certain Techniques That May Be Used in the Interrogation of High Value al Qaeda Detainees (May 30, 2005), *available at* <http://bit.ly/Iltguh>. For example, it notes that the CIA “has employed enhanced techniques to varying degrees in the interrogations of 28 of these detainees,” *id.* at 5, and that “the CIA has used [waterboarding] in the interrogations of only three detainees to date (KSM, Zubaydah, and ‘Abd Al-Rahim Al-Nashiri),” *id.* at 6. The memo reveals granular details about the treatment of particular detainees, including that the CIA waterboarded defendant Mohammad “183 times during March 2003.” *Id.* at 37.

On August 24, 2009, the CIA itself declassified large portions of a CIA Inspector General’s report concerning the Agency’s detention and interrogation operations. CIA Office of the Inspector General, *Counterterrorism Detention and Interrogation Activities (September 2001 – October 2003)* (May 7, 2004), *available at* <http://wapo.st/3JNHM> (“IG Report”). The IG Report describes actual applications of coercive techniques that *exceeded* the authority purportedly conferred by the OLC Memos, recounting in detail numerous instances in which CIA and contract interrogators engaged in unauthorized coercive practices. The report includes multiple descriptions of the treatment of

defendant Mohammed, *id.* ¶¶ 99–100, and other unauthorized interrogation activities that bear no relation to the techniques described in the OLC memos, including, for example, that an “experienced Agency interrogator reported that . . . interrogators said to Khalid Shaykh Muhammad that if anything else happens in the United States, ‘We’re going to kill your children.’” *Id.* ¶ 95. The report also reveals that defendant al Hawsawi was subject to interrogation. *Id.* ¶ 214.

A second CIA document declassified with the IG Report is a self-styled “Background Paper” prepared by the CIA to describe the Agency’s “combined use of interrogation techniques.” CIA, *Background Paper on CIA’s Combined Use of Interrogation Techniques* (Dec. 30, 2009), available at <http://bit.ly/3YJp0>. The document is intended to provide “additional background on how interrogation techniques are used, in combination and separately, to achieve interrogation objectives.” *Id.* at 1 (emphasis added). The entire document makes clear that actual descriptions of detention conditions and techniques have been declassified. *Id.* at 4 (summarizing “detention conditions that are used in all CIA HVD facilities,” and describing in detail each of the techniques actually applied, *id.* at 4–17).

Any statements defendants make during the Military Commission proceedings about their experience while subject to CIA interrogation are likely to reveal little or nothing that the government, at the direction of the President, has not already officially disclosed.

Further, even if defendants were to describe information about their treatment beyond what the government has itself disclosed, that information would cause no harm to national security because a publicly available report by the International Committee of

the Red Cross, based entirely on the firsthand accounts of former CIA prisoners held at Guantanamo, describes their treatment in CIA custody. Int'l Comm. of the Red Cross, *Report on the Treatment of Fourteen "High Value" Detainees in CIA Custody* (Feb. 2007), available at <http://assets.nybooks.com/media/doc/2010/04/22/icrc-report.pdf> ("ICRC Report"). The ICRC Report is based on interviews with 14 detainees, including all five defendants here. *Id.* at 5. Although the Report does not constitute an official government disclosure, it contains much of the same information that defendants could potentially provide in testimony before the commission. *See, e.g., id.* at 10 (Mr. Mohammed: "A cloth would be placed over my face. Water was then poured onto the cloth by one of the guards so that I could not breathe."); *id.* at 11 ("Mr Ramzi Binalshib alleged that he was shackled in this position for two to three days in Afghanistan his second place of detention and for seven days in his fourth . . ."); *id.* ("Mr Bin Attash commented that during the two weeks he was shackled in the prolonged stress standing position with his hands chained above his head, his artificial leg was sometimes removed by the interrogators to increase the stress and fatigue of the position."); *id.* at 31–33 (full account of statement of Mr. Bin Attash); *id.* at 33–37 (full account of statement of Mr. Mohammed).

Official investigations by United Nations and European human rights officials and accounts in the press have made public the locations of the overseas CIA-operated detention facilities at which defendants were held, including Afghanistan, Poland, Romania, Lithuania, Morocco, and Thailand. A mere sampling of these reports reveals the very information about detention by the CIA that the government seeks to classify here. *See, e.g.,* U.N. Human Rights Council, *Joint Study on Global Practices in Relation*

UNCLASSIFIED
FOR PUBLIC RELEASE

to Secret Detention in the Context of Countering Terrorism, ¶ 114, U.N. Doc. A/HRC/13/42 (May 20, 2010), available at <http://bit.ly/cziSQc> (Defendants Mohamed, bin al-Shibh, and bin Attash held in the Polish village of Stare Kiejkut between 2003 and 2005); *id.* ¶ 108 (“The *Washington Post* also reported that the officials had stated that Ramzi Binalshibh had been flown to Thailand after his capture.”); Memorandum from Dick Marty, Switzerland Rapporteur to the Council of Europe, Secret Detentions and Illegal Transfers of Detainees Involving Council of Europe Member States: Second Report, ¶ 127 & n.85 (June 8, 2007), available at <http://bbc.in/JMRLRM> (same); see also Alex Spillius, *CIA ‘Used Romania Building as Prison for Khalid Sheikh Mohammed,’* Telegraph, Dec. 8, 2011, <http://tgr.ph/u18pgx> (“Among the prisoners on board a flight from Poland to Bucharest in September 2003, according to former CIA officials, were [Khalid Sheikh] Mohammed and Walid bin Attash . . . Later, other senior al-Qaeda suspect[] Ramzi Binalshibh . . . w[as] also moved to Romania.”); *id.* (“The prison [in Romania] was part of a network of so-called ‘black sites’ that included prisons in Poland, Lithuania, Thailand and Morocco operated by the CIA.”); Dana Priest, *CIA Holds Terror Suspects in Secret Prisons*, Wash. Post, Nov. 2, 2005, <http://wapo.st/Ud8UD> (“Sept. 11 planner Ramzi Binalshibh was also captured in Pakistan and flown to Thailand.”); Matthew Cole & Brian Ross, *Exclusive: CIA Secret ‘Torture’ Prison Found at Fancy Horseback Riding Academy*, ABC News, Nov. 8, 2009, <http://abcn.ws/liByQk> (“The CIA built one of its secret European prisons inside an exclusive riding academy outside Vilnius, Lithuania, a current Lithuanian government official and a former U.S. intelligence official told ABC News this week.”).

Given the vast amount of information that is already public concerning the CIA's coercive interrogation techniques and the sites at which those techniques were administered, the government cannot meet its burden of demonstrating that the public must be excluded from hearing statements from the defendants about their knowledge and experiences in CIA custody. To the contrary, the government's proposed categorical suppression of defendants' statements—irrespective of the truth of those statements and whether their contents have been widely publicized—is the very antithesis of the narrow tailoring required by the First Amendment.

E. There is no justification for the 40-second audio feed delay.

Because the government's proposed classification of defendants' statements based on their personal knowledge of their detention and treatment in U.S. custody is improper, there is no justification for the government's proposed 40-second audio delay. The audio delay is also improper because it turns the presumption of open public access to these proceedings, subject only to narrowly-tailored exceptions, on its head by presumptively closing them. Gov't Al-Nashiri Mot. 15 (requesting audio delay "so that *if* classified information is disclosed, inadvertently or otherwise," the government may prevent it from being heard) (emphasis added). If this Commission nevertheless grants the government's request for a 40-second delay, it should order the public release of unredacted transcripts containing the defendants' statements on an expedited basis to minimize the infringement on the public's right of contemporaneous access to the proceedings. *Lugosch*, 435 F.3d at 126–27 ("Our public access cases and those in other circuits emphasize the importance of immediate access when a right of access is found." (emphasis added)); *Wash. Post*, 935 F.2d at 287 (recognizing "the critical importance of

contemporaneous access . . . to the public's role as overseer of the criminal justice process").

7. Oral Argument. The ACLU requests oral argument.

8. Attachment.

A. Declaration of David Glazier

Respectfully submitted,



Hina Shamsi
Nathan Freed Wessler
Zachary Katznelson
American Civil Liberties Union
Foundation
125 Broad St., 18th Fl.
New York, NY 10004
Tel.: (212) 549-2500
Fax: (212) 549-2654
hshamsi@aclu.org

DECLARATION OF DAVID GLAZIER

Pursuant to 28 U.S.C. § 1746, I, David Glazier, do declare as follows:

1. I am a Professor of Law at Loyola Law School in Los Angeles, California. After graduating with a B.A. in history from Amherst College in 1980, I attended Navy Officer Candidate School in Newport, Rhode Island. I was commissioned as an Ensign in September, 1980 and spent the next twenty-one years on active duty as a Surface Warfare Officer, culminating in command of USS George Philip (FFG 12). I retired from the Navy effective September 1, 2001 in order to take advantage of the opportunity to attend law school at the University of Virginia. Following graduation from law school I remained in Charlottesville for two additional years as a research fellow at the Center for National Security Law. I have been employed by Loyola since July 2006 and was promoted to full professor and granted tenure in July 2009.
2. I have been a scholar of military commissions and their historical use by the United States since my second semester of law school in the spring of 2002. My first publication on the subject was my student note for the Virginia Law Review, *Kangaroo Court or Competent Tribunal?: Judging the 21st Century Military Commission* (81 Va. L. Rev. 2005(2003)). The original argument I made in that note that Article 36 of the UCMJ should be read to require uniformity between court-martial and military commission procedure was adopted by the District Court as one of its two grounds for overturning Salim Hamdan's trial. *Hamdan v. Rumsfeld*, 344 F. Sup.2d 152, 166-72 (D.D.C. 2004). I have continued to engage in extensive scholarship on the subject of military commissions along with the closely interrelated issues of the history of U.S. military

UNCLASSIFIED
FOR PUBLIC RELEASE

justice and the law of war since that time, and have published three additional full-length law review articles on military commission history and law. I will be submitting a fourth article for publication in the very near future.

3. In the course of this research I have personally examined the results of every U.S. military commission conducted during the Mexican War (more than 400 trials) and Philippine Insurrection (more than 800 trials) via the holdings of the National Archives and Library of Congress, and have reviewed a mixture of primary and secondary source materials from the Civil War, 19th century Indian Wars, World War I, and World War II eras. I have also done extensive original research on claimed military commission precedents from the Revolution, War of 1812, and Seminole Wars which pre-date their formal creation by General Winfield Scott during the Mexican War.
4. As a practical matter the remote location of many military trials, both commissions and courts-martial, had the practical effect of limiting public attendance. But by rule they were open proceedings. This seems to have been so taken for granted that military justice commentators have found little reason to comment on it. Evidence of the openness of military commissions can be found in the publicly available descriptions of virtually every historically significant military commission trial, including those of Lambden Milligan, John Y. Beall, and the Lincoln assassination conspirators in the Civil War; the Dakota Sioux and Modoc Indian trials, and scores of war crimes trials in the aftermath of World War II. William Winthrop specifically noted the requirement for public court martial sessions in his seminal treatise on U.S. military justice. William Winthrop, *Military Law and Precedents* * 234-36. He further opined that it is preferable for court-martial trial panels to retire for deliberations rather than clearing the courtroom to avoid

UNCLASSIFIED
FOR PUBLIC RELEASE

the significant “inconvenience and embarrassment caused to the accused, counsel, clerks and reporters, witnesses *and the public.*” Winthrop, * 433 (emphasis added). Although specifically addressing courts-martial, he cites with approval the practice of the Milligan military commission as an example of a military trial following this practice. And it is important to note that until the 1942 military commission trial of eight Nazi saboteurs conducted at the Department of Justice in Washington D.C., there was no difference between military commission and court-martial procedure at all. Indeed, in Senate testimony explaining the rationale for a new Article 15 proposed for inclusion in the Army’s Articles of War (subsequently carried over as UCMJ Article 21) Judge Advocate General Enoch Crowder testified explicitly that the court-martial and military commission “have the same procedure.” Senate Report 64-582 at 40 (1916). So the history of open conduct of courts-martial is clearly equally applicable to military commissions.

5. The one well-known historical anomaly, a closed military commission trial, took place in the *Quirin* case. That case concerned eight Nazi saboteurs who crossed the Atlantic in German U-boats before successfully penetrating porous U.S. coastal defenses on eastern Long Island and in Florida just south of Jacksonville. Despite the fact that Long Island group was observed on the beach by an unarmed Coast Guard patrol, the saboteurs were only rounded up by the FBI after one turned himself in and provided the identification and probable locations for the others. All eight were questioned by the FBI under the constitutional criminal procedure standards of the day and freely admitted their mission. They also revealed the existence of a German sabotage school which they attended that was training additional individuals to conduct follow-on raids on the United States. The

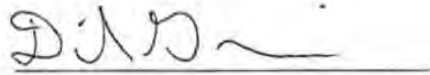
UNCLASSIFIED
FOR PUBLIC RELEASE

Quirin case is controversial for a number of reasons, including that the trial was conducted in secret. Some commentators have noted it may have been closed to avoid embarrassment to the U.S. government over its perceived incompetence in preventing the landings and the subsequent interagency bungling, and I think this may well have been a factor. What is clear, however, is that the secrecy of the proceeding contributed to what is widely acknowledged as the tarnished legacy of that case.

6. Based on my extensive study of the historical record, it is my conclusion that our nation has a strong tradition of opening military commissions to the public.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 30th day of April, 2012.



David Glazier

Tab 3

**MILITARY COMMISSIONS TRIAL JUDICIARY
GUANTANAMO BAY, CUBA**

UNITED STATES OF AMERICA v. KHALID SHAIKH MOHAMMAD, WALID MUHAMMAD SALIH MUBARAK BIN ATTASH, RAMZI BINALSHIBH, ALI ABDUL AZIZ ALI, MUSTAFA AHMED ADAM AL HAWSAWI	AE 013D Government's Response To the American Civil Liberties Union Motion for Public Access to Proceedings and Records 16 May 2012
---	--

1. Timeliness.

This response is filed timely pursuant to Military Commissions Trial Judiciary Rule of Court 3.7.c(1).

2. Relief Sought.

The government respectfully requests that the Commission deny the American Civil Liberties Union's (ACLU) motion challenging certain provisions contained within the government's proposed order protecting against disclosure of national security information. Specifically, the ACLU asserts that the Commission reject the following provisions: 1) that statements of the accused are treated as classified until an Original Classification Authority ("OCA") conducts a classification review; and 2) implementing a 40-second delay of the audio feed of commission proceedings to protect against the unauthorized disclosure of classified information during proceedings open to the public.

3. Overview.

The public has a statutory right to access military commission proceedings against the five accused who have been charged with multiple offenses related to the 11 September 2001

terrorist attacks which resulted in the deaths of 2,976 people, serious injury to others, and significant property damage. This right, like analogous constitutional and common law rights of public access to proceedings in federal courts and courts-martial, is a qualified right. The government has a strong interest in ensuring public access to these historic proceedings and has moved the Commission to authorize closed-circuit television (CCTV) transmission of all commission proceedings to remote viewing sites located in the continental United States. During the arraignment of the five accused on 5 May 2012, the proceedings were viewed by individuals and media at seven different sites in the United States. *See* AE7B. Such a transmission has enabled and will continue to enable the public and victim family members (VFM) to access the trial of the accused.¹

¹ The arraignment proceedings had widespread coverage by major media outlets and local news stations as reflected in the following news stories: <http://www.cnbc.com/id/47317654> (“U.S. prosecutors say ready for long haul in 9/11 case”); <http://www.cnn.com/2012/05/06/justice/guantanamo-ksm-arraignment/> (“9/11 victim’s brother to alleged mastermind: I came a long way to see you, eye to eye”); <http://www.time.com/time/nation/article/0,8599,2114018,00.html> (“9/11 defendants disruptive at Guantanamo”); http://www.cbsnews.com/8301-201_162-57428546/9-11-mastermind-others-back-before-guantanamo-judge/ (“9/11 “mastermind,” others back before Guantanamo judge”); <http://abcnews.go.com/blogs/politics/2012/05/911-plotters-accused-refuses-to-answer-in-guantanamo-bay-arraignment/> (“9/11 Plotters Defer Pleas at Guantanamo Bay Arraignment”); http://worldnews.msnbc.msn.com/_news/2012/05/05/11548929-alleged-sept-11-planners-disrupt-arraignment-at-guantanamo-hearing?lite (“Alleged Sept. 11 planners disrupt arraignment at Guantanamo hearing”); <http://www.foxnews.com/us/2012/05/06/anger-sighs-as-11-families-watch-terror-hearing-1682598921/> (“Anger, sighs as 9/11 families watch terror hearing”); <http://www.usatoday.com/news/world/story/2012-05-05/911-mastermind-gitmo-defiant-court/54771104/1> (“9/11 defendants formally charged, ignore judge at hearing”); <http://www.npr.org/2012/05/06/152129287/pleas-delayed-in-sept-11-case> (“Pleas deferred in Sept. 11 case”); <http://online.wsj.com/article/SB10001424052702304752804577386102452510454.html?KEYWORDS=guantanamo> (“Guantanamo judge grapples with disruptive terror suspects”); <http://www.nydailynews.com/news/national/khalid-sheikh-mohammed-co-defendants-court-arraignment-article-1.1073016> (“Arraignment ends with accused terrorist, Ramzi Binalshibh, mocking 9/11 family member with a thumbs up”); <http://www.baltimoresun.com/news/breaking/bs-md-911-arraignments-20120505,0,7842454.story> (“9/11 defendants refuse to participate in arraignment”); <http://www.latimes.com/news/nation/nationnow/la-na-nn-gitmo-mohammad-arraignment-begins20120505.0.6952315.story> (“9/11 trial begins at Guantanamo with protest by defendants”); http://www.washingtonpost.com/world/national-security/911-detainees-seek-to-disrupt-opening-of-arraignment-at-guantanamo-bay/2012/05/05/gIQAnGzh3T_story.html?tid=pm_world_pop (“9/11 detainees work to disrupt opening of arraignment at Guantanamo Bay”); http://www.nytimes.com/2012/05/06/nyregion/families-watch-9-11-case-at-guantanamo-via-video.html?_r=1 (“Via Video Feed, Families Watch 9/11 Case and Seethe”); <http://www.chicagotribune.com/news/nationworld/la-na-nn-terror-trial-20120505,0,2288105.story> (“Sept. 11 terrorism trial at Guantanamo gets off to a silent start”); <http://bostonglobe.com/news/world/2012/05/05/five-defendants-attacks-disrupt-tribunal-guantanamo/gcHr48BuoSPadgetGFecWJ/story.html> (“Five defendants in 9/11 attacks disrupt tribunal”); <http://www.miamiherald.com/2012/05/05/2784620/911-mastermind-back-before->

As in any prosecution involving national security, the government is responsible for protecting information that has been properly classified by the Executive Branch. Accordingly, the government has proposed narrowly tailored procedures to reduce the risk of unauthorized disclosures of classified information—to which there is no First Amendment right—where disclosure could cause exceptionally grave damage to national security. The ACLU attempts to substitute its judgment for the intelligence professionals within the Executive Branch in determining whether and to what extent the sources and methods employed by the United States can be protected to safeguard national security. The Supreme Court has cautioned against even judicial interference with the legitimate interest and responsibilities of the Executive Branch in assessing whether the disclosure of classified information may lead to an unacceptable risk of compromising national security. The ACLU's requested relief would force the government into the unenviable position of having to predict the accused's possible future behavior knowing that their interests are clearly inconsistent with the interests of the national security. As such, the ACLU's motion should be denied.

4. Burden of Proof.

As the moving party, the ACLU must demonstrate by a preponderance of the evidence that the requested relief is warranted. R.M.C. 905(c)(1)-(2).

5. Facts.

On 31 May 2011 and 26 January 2012, pursuant to the Military Commissions Act of 2009, charges related to the 11 September 2001 terrorist attacks were sworn against Khalid

[guantanamo.html](#) ("9/11 defendants ignore judge at Guantanamo hearing");
http://www.nj.com/news/index.ssf/2012/04/nj_military_base_one_of_six_si.html ("N.J. military base one of six sites to broadcast alleged Sept. 11 mastermind's arraignment");
http://www.nypost.com/p/news/local/families_outraged_at_tribunal_farce_EnauN08nEjKhYLvkeKuWQO?utm_medium=rss&utm_content=Local ("Families outraged at tribunal's farce")

Sheikh Mohammad, Walid Muhammad Salih Bin Attash, Ramzi Binalshibh, Ali Abdul Aziz Ali, and Mustafa Ahmed Adam al Hawsawi (collectively referred to as the “accused”). These charges were referred jointly to this capital Military Commission on 4 April 2012. The accused are charged with Conspiracy, Attacking Civilians, Attacking Civilian Objects, Intentionally Causing Serious Bodily Injury, Murder in Violation of the Law of War, Destruction of Property in Violation of the Law of War, Hijacking an Aircraft, and Terrorism.

The arraignment for this Commission was held on 5 May 2012. Pursuant to an order signed by the Military Judge on 26 April 2012, the proceedings were transmitted to multiple sites in the continental United States. *See* AE7B.

On 11 September 2001, a group of al Qaeda operatives hijacked four civilian airliners in the United States. After the hijackers killed or incapacitated the airline pilots, a pilot-hijacker deliberately slammed American Airlines Flight 11 into the North Tower of the World Trade Center in New York, New York. A second pilot-hijacker intentionally flew United Airlines Flight 175 into the South Tower of the World Trade Center. Both towers collapsed soon thereafter. Hijackers also deliberately slammed a third airliner, American Airlines Flight 77, into the Pentagon in Northern Virginia. A fourth hijacked airliner, United Airlines Flight 93, crashed into a field in Shanksville, Pennsylvania, after passengers and crew resisted the hijackers and fought to reclaim control of the aircraft. A total of 2,976 people were murdered as a result of al Qaeda’s 11 September 2001 attacks on the United States. Numerous other civilians and military personnel also were injured. The al Qaeda leadership praised the attacks, vowing that the United States would not “enjoy security” until al Qaeda’s demands were met. The United States Congress responded on 18 September 2001 with an Authorization for Use of Military Force.

In response to the terrorist attacks on 11 September 2001, the United States instituted a program run by the CIA to detain and interrogate a number of known or suspected high-value terrorists, or “high-value detainees” (“HVDs”). This CIA program involves information that is classified TOP SECRET / SENSITIVE COMPARTMENTED INFORMATION (TS/SCI), the disclosure of which would cause exceptionally grave damage to national security. The accused are HVDs and, as such, they were participants in the CIA program.

Because the accused were participants in the CIA program, they were exposed to classified sources, methods, and activities. Due to their exposure to classified information, the accused are in a position to disclose classified information publicly through their statements. Consequently, any and all statements by the accused are presumptively classified until a classification review can be completed.

On 6 September 2006, President George W. Bush officially acknowledged the existence of the CIA program and he announced that a group of HVDs had been transferred by the CIA to Department of Defense (“DoD”) custody at Joint Task Force – Guantanamo (JTF-GTMO). *See* President George W. Bush, *President Discusses Creation of Military Commissions to Try Suspected Terrorists*, Remarks from the East Room of the White House, Sep. 6, 2006, available at <http://georgewbush-whitehouse.archives.gov/news/releases/2006/09/20060906-3.html>. The five accused were among the group of HVDs transferred to DoD custody, and they have remained in detention at JTF-GTMO since that time.

Since 6 September 2006, a limited amount of information relating to the CIA program has been declassified and officially acknowledged, often directly by the President. This information includes a general description of the program; descriptions of the various “enhanced interrogation techniques” that were approved for use in the program; the fact that the so-called

“waterboard” technique was used on three detainees; and the fact that information learned from HVDs in this program helped identify and locate al Qaeda members and disrupt planned terrorist attacks. *See id.*; *see also* CIA Inspector General, *Special Review: Counterterrorism Detention and Interrogation Activities (September 2001 – October 2003)*, May 7, 2004, available at http://media.washingtonpost.com/wp-srv/nation/documents/cia_report.pdf.

Other information related to the CIA program has not been declassified or officially acknowledged, and, therefore, such information remains classified. This classified information includes allegations involving (i) the location of detention facilities, (ii) the identity of cooperating foreign governments, (iii) the identity of personnel involved in the capture, detention, transfer, or interrogation of detainees, (iv) interrogation techniques as applied to specific detainees, and (v) conditions of confinement. The disclosure of this classified information would cause exceptionally grave damage to national security.

On 26 April 2012, the government filed its Motion to Protect Against Disclosure of National Security Information. *See* AE 013. The motion and accompanying declarations set forth the classified information at issue in the case, the harm to national security that unauthorized disclosure of such information would cause, and the narrowly tailored remedies that seek to protect national security information. The proposed order includes, in its definition of classified information, statements made by the accused, which, due to these individuals’ exposure to classified sources, methods, or activities of the United States, are presumed to contain information classified as TOP SECRET / SCI. AE 013, Attachment E, Proposed Order at ¶ 7(d)(vi). To protect against the unauthorized disclosure of classified information during proceedings open to the public, the proposed order institutes a 40-second delay in the transmission of the proceedings from the courtroom to the public gallery. AE 013, Attachment

E, Proposed Order at ¶ 42. The proposed order also provides that an unofficial, unauthenticated, unclassified transcript of each proceeding shall be made available for public release. AE 013, Attachment E, Proposed Order at ¶ 47.

On 3 May 2012, the government filed its response to the defense Motion to End Presumptive Classification (AE 009A), which set forth the legal authority for the Executive Branch determination that the statements of the accused are properly presumptively classified until reviewed by an OCA. The ACLU's motion contains allegations that the government has previously addressed in AE 009 and AE 013, and the government respectfully requests that those responses be incorporated into this filing.

6. Law and Argument.

I. The Statutory Right Of Public Access To The Trial Of The Accused Is Not Abrogated By The Implementation Of A 40-Second Delay To The Proceedings.

The United States Supreme Court has said, “[p]eople in an open society do not demand infallibility from their institutions, but it is difficult for them to accept what they are prohibited from observing.” *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 572 (1980). The best traditions of American jurisprudence call for providing an opportunity for the public to witness the trial of the accused, to observe first-hand that the accused in a reformed military commission receives stronger protections than an accused tried under the London Charter at Nuremberg following World War II, and to see that the accused receives stronger protections than an accused in many respected criminal-justice systems around the world. The government has a strong interest in ensuring public access to these historic proceedings and has moved the Commission to authorize closed-circuit television (CCTV) transmission of all commission proceedings to remote viewing sites located in the continental United States.

The M.C.A. and the Manual for Military Commissions (M.M.C.) provide that trials by military commission shall generally be open to the public. 10 U.S.C. §§ 949d(c)(2), 949p-3; R.M.C. 806(b)(2)(B). This right, like analogous constitutional and common law rights of public access to proceedings in federal court and courts-martial, is a qualified right. Due to the classified information involved with this case, and the harm to national security that its disclosure reasonably could be expected to cause, the M.C.A. allows for certain protective measures to be adopted in this military commission that apply at all stages of the proceedings. M.C.R.E. 505(a)(1); *see generally* 10 U.S.C. §§ 949p-1 through 949p-7.

The government has requested a 40-second delay in the transmission to the public viewing gallery (including transmission to the CCTV sites) so that if classified information is disclosed, inadvertently or otherwise, in open court, the government will have the opportunity to prevent it from being publicly disclosed. The ACLU appears to allege that a 40-second delay amounts to a closure of the courtroom, but neither case cited by the ACLU stands for the proposition that a 40-second delay could reasonably be considered a denial of public access because the transmission is not immediate or contemporaneous.

Instead, this narrowly tailored measure is necessary to protect classified information during proceedings. If any of the accused testify, for example, the delayed-transmission mechanism is vital to the protection of classified information since the accused's statements are presumed classified until a classification review is completed. Because the government cannot predict what an accused will say during proceedings or whether he will comply with orders from the Military Judge, the time delay is the only effective means of preventing any intentional or inadvertent disclosure of classified information to the public. Additionally, the time delay will

prevent the public disclosure of classified information by other witnesses, who may reveal such information inadvertently during their testimony in proceedings.

If classified information is disclosed during the proceeding, and the transmission is suspended to prevent its public disclosure, then that portion of the proceeding will not be transmitted, but will remain part of the classified record of the proceeding. If it is determined that classified information was not disclosed then the proceedings and the transmission, with the time delay, will resume. Additionally, the transcripts released at the end of each session will recapture any unclassified information that was not originally transmitted to the public.

During the arraignment of the five accused on 5 May 2012, the proceedings were viewed on a delayed 40-second transmission by individuals and media at seven different sites in the United States, clearly satisfying the public's right of access. *See e.g., Nixon v. Warner Communications, Inc.*, 435 U.S. 589, 610, 98 S.Ct. 1306, 55 L.Ed.2d 570 (1978) (public's right of access is constitutionally satisfied when some members of both the public and the media are able to "attend the trial and report what they have observed."). The transmission included statements made by one of the accused. Although the transmission was briefly suspended for approximately 60 seconds during the more than 13 hours of the proceeding, the unofficial unauthenticated, transcript that was publicly released recaptured the information once it was determined to be unclassified. The public access to these proceedings exceeds that which was deemed constitutionally sufficient in the terrorist prosecutions of Zaccarias Moussaoui and Timothy McVeigh. *See, e.g., U.S. v. Moussaoui*, 205 F.R.D. 183, 185 (E.D.Va. 2002); *United States v. McVeigh*, No. 96-CR-68-M (W.D.Okla.). And, the public access to these proceedings fully satisfies the statutory requirements for openness and accessibility. The closed-circuit

transmission has enabled and will continue to enable the public and victim family members (VFM) to access the trial of the accused.

II. The Executive Branch Is Legally Authorized To Classify Information That May Be Communicated Orally, And Such Practice Does Not Limit The Public Access To These Proceedings.

In its motion², the ACLU alleges that the government has no legal authority to make a presumptive determination that statements of the accused are classified pending a review by an OCA. However, a determination whether to classify information, and the proper classification thereof, is a matter committed solely to the Executive Branch. *See, e.g., Dep't of Navy v. Egan*, 484 U.S. 518, 527 (1988) (“The authority to protect such information falls on the President as head of the Executive Branch and as Commander in Chief.”). The Supreme Court has recognized this broad deference to the Executive Branch in matters of national security, holding that, “it is the responsibility of the Director of Central Intelligence, not that of the judiciary, to weigh the variety of subtle and complex factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the Agency's intelligence-gathering process.” *CIA v. Sims*, 471 U.S. 159, 180 (1985).

Because the accused have been exposed to highly classified sources and methods, the public disclosure of which reasonably could be expected to cause exceptionally grave damage to national security, an OCA properly decided that statements of the accused must be handled in a classified manner—thus the term presumptively classified—until an OCA conducts a classification review to determine what information contained within the statements are in fact classified. An OCA determined that the accused are in possession of classified material that falls within one of the eight substantive categories of material pursuant to Section 1.4 of Executive

² The government responded to many of the challenges raised by the ACLU in its response to AE009, incorporated here by reference.

Order 13526, and meets the conditions set forth in Section 1.1(a).³ This determination provides a means to restrict the unauthorized disclosure of classified information that could cause exceptionally grave damage to the national security from an individual accused who does not hold a security clearance and who owes no duty of loyalty to the United States. Without a process to protect classified information that may be contained within the statements of the accused, the government would be in the unenviable position of having to predict the accused's possible future behavior knowing that their interests are clearly inconsistent with the interests of the national security.

The ACLU's assertions that presumptive classification of the statements of the accused prevents public access ignores the principal that, "[t]here is no First Amendment right to reveal properly classified information." AE 009, p. 22. *See, e.g., Stillman v. C.I.A.*, 319 F.3d 546, 548

³ Executive Order 13526 is the current presidential order governing the classification of national security information. Section 1.1(a) provides that information may be originally classified under the terms of the Order only if the following conditions are met:

- (1) an original classification authority is classifying the information;
- (2) the information is owned by, produced by or for, or is under the control of the United States Government;
- (3) the information falls within one or more of the categories of information listed in section 1.4 of this order; and
- (4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.

Section 1.4 of Executive Order 13526 requires that for information to be considered for classification, it must concern one of the eight substantive categories, which include: foreign government information; intelligence activities (including covert action), intelligence sources and methods, or cryptology; and foreign relations or foreign activities of the United States, including confidential sources. Pursuant to Section 1.2 of Executive Order 13526, information may be classified as TOP SECRET, SECRET, OR CONFIDENTIAL based on the severity to the damage to the national security reasonably expected to result from the unauthorized disclosure of information. Thus, if an unauthorized disclosure of information reasonably could be expected to cause *damage* to the national security, that information may be classified as CONFIDENTIAL. If an unauthorized disclosure of information reasonably could be expected to cause *serious damage* to the national security, that information may be classified as SECRET. Finally, if an unauthorized disclosure of information reasonably could be expected to cause *exceptionally grave damage* to the national security, that information may be classified as TOP SECRET.

(D.C. Cir. 2003) (“If the Government classified the information properly, then [appellant] simply has no first amendment right to publish it.”); *see also*, *Snepp v. United States*, 444 U.S. 507, 510 n.3 (1980) (“The Government has a compelling interest in protecting both the secrecy of information important to our national security and the appearance of confidentiality so essential to the effective operation of our foreign intelligence service.”); *see also*, *ACLU v. DOD*, 584 F.Supp. 2d 19, 25 (D.D.C. 2008)(“There is obviously no First Amendment right to receive classified information.”) The protections that the government seeks in this case are narrowly tailored to protect the unauthorized disclosure of classified information, and do not amount to a suppression of any and all statements of the accused, as evidenced by the public broadcast on 5 May 2012, which included statements made by at least two of the accused in this case.

Although some details of the CIA’s program have been declassified, many details that relate to the capture, detention, and interrogation of the accused, for reasons of national security, remain classified. The ACLU appears to argue that the fact that many details have been declassified undermines any justification for continuing to classify any information about the capture, detention, and interrogation of the accused. However, the ACLU could not possibly be in a position to assess the risk to national security inherent in declassifying the remaining categories of information. Indeed, the Supreme Court has repeatedly stressed that even courts should be “especially reluctant to intrude upon the authority of the Executive in . . . national security affairs.” *Egan*, 484 U.S. at 530; *see also*, *CIA v. Sims*, 471 U.S. 159, 168-169 (1985) (the Director of Central Intelligence has broad authority to protect all sources of intelligence information from disclosure); *Haig v. Agee*, 453 U.S. 280, 307 (1981) (protecting the secrecy of the U.S. Government’s foreign intelligence operations is a compelling interest).

The ACLU's position is further undermined by the principle that even when classified information has been leaked to the public domain, it remains classified and cannot be further disclosed unless it has been declassified or "officially acknowledged," which entails that it "must already have been made public through an official and documented disclosure." *Wolf v. CIA*, 473 F.3d 370, 378 (D.C. Cir. 2007) (internal quotations and citations omitted) (recognizing that "the fact that information exists in some form in the public domain does not necessarily mean that official disclosure will not cause [cognizable] harm" to government interests); *see also Fitzgibbon v. CIA*, 911 F.2d 755, 765 (D.C. Cir. 1990) ("[I]n the arena of intelligence and foreign relations, there can be a critical difference between official and unofficial disclosures."); *United States v. Moussaoui*, 65 Fed. Appx. 881, 887 n.5 (4th Cir. 2003) ("[I]t is one thing for a reporter or author to speculate or guess that a thing may be so or even, quoting undisclosed sources, to say that it is so; it is quite another thing for one in a position to know of it officially to say that it is so.") (quoting *Alfred A Knopf, Inc. v. Colby*, 509 F.2d 1362, 1370 (4th Cir. 1975)); *see also Afshar v. Dep't of State*, 702 F.2d 1125, 1130 (D.C. Cir. 1983) ("[E]ven if a fact . . . is the subject of widespread media attention and public speculation, its official acknowledgement by an authoritative source might well be new information that could cause damage to the national security.").

7. Conclusion.

The ACLU's attempt to substitute its judgment for that of the intelligence professionals within the Executive Branch in determining whether and to what extent the sources and methods employed by the United States can be protected to safeguard national security should be rejected. Instead, such decisions should be left to the Executive Branch, which has the legitimate interest

Tab 4

**Military Commissions Trial Judiciary
Guantanamo Bay, Cuba**

**UNITED STATES OF AMERICA
v.
KHALID SHAIKH MOHAMMAD,
WALID MUHAMMAD SALIH
MUBARAK
BIN 'ATTASH, RAMZI BINALSHIBH,
ALI ABDUL AZIZ ALI,
MUSTAFA AHMED ADAM AL-
HAWSAWI**

**Response/Opposition by 14 News
Organizations to Government's Motion
to Protect Against Disclosure of
National Security Information (AE013)
and Cross-Motion to Enforce Public
Access Rights**

May 16, 2012

1. **Timeliness.** This Opposition is timely filed in response to the Government's for a protective order motion (AE013) under the Rules of Court ("RC").

2. **Relief Sought.** Pursuant to Rules of Court 3(5)(c) and Regulations 17-1 and 19-3(c) & (d) of the 2011 Regulation for Trial by Military Commissions, The Miami Herald, ABC, Inc., Associated Press, Bloomberg News, CBS Broadcasting, Inc., Fox News Network, The McClatchy Company, National Public Radio, The New York Times, The New Yorker, Reuters, Tribune Company, Wall Street Journal, and Washington Post (collectively the "Press Objectors") respectfully oppose as overly broad the Government's motion for a protective order (AE013) ("Gov't Mot."). The Commission should deny the Government's request to deny public access to all records and proceedings that involve any classified information.

No proceeding or record in this case may be closed to the public unless the Government first makes an evidentiary showing sufficient to overcome the public's First Amendment right of access. Specifically, the Government must demonstrate that (1) the disclosure of specific information would create a substantial likelihood of harm to a compelling governmental interest, (2) no alternative other than closure can avoid that harm, (3) closure will be effective in

preventing the threatened harm, and (4) the closure requested is narrowly tailored in scope and time. The Government's blanket request for permission to close all testimony by defendants and all statements made in open court concerning their treatment on the ground that this information is classified does not satisfy this constitutional test.

3. **Overview.** In seeking a protective order to seal records and close proceedings, the Government reasons that because the defendants in this case were detained and interrogated in a classified CIA information-gathering program, any statements made *by the defendants* are all "presumptively classified until a classification review can be completed." Gov't Mot. at 6, ¶ 5g. The Government then argues that because the Military Commissions Act, 10 U.S.C. § 948a, *et seq.* (M.C.A.), permits some proceedings involving classified information to be closed to the press and public, the Commission should take a number of steps that would automatically close the trial during any statement by a defendant and during any comments by others about defendants' treatment and conditions of confinement until they can be subjected to government review and permission. The Government's request is fundamentally flawed in multiple respects.

a. Even if statements made by defendants or about their treatment can properly be deemed "classified" under the Executive Order (a questionable premise),¹ both the M.C.A. and the First Amendment require the Commission to demonstrate a specific threat to national security before a Commission proceeding may be closed. The M.C.A. allows commission proceedings to be closed only where a specific finding is made that closure is necessary to prevent reasonably expected damage to the national security or to ensure the physical safety of

¹ As noted in the pending ACLU Motion for Public Proceedings (AE013A) ("ACLU Mot."), the authority to classify information by Executive Order 13,526 §1.1(a)(2) is restricted to information "by . . . or is under the control of the United States Government," and this authority cannot be used to restrict disclosure of information simply because it is embarrassing or to conceal illegal conduct. (ACLU Mot. at 19-21.)

individuals. M.C.A. § 949d(c)(2). The First Amendment allows commission proceedings to be closed only upon a specific finding of a “substantial probability” of harm to national security or some equally compelling governmental interest. *Press-Enterprise Co. v. Superior Court*, 478 U.S. 1, 10 (1986) (“*Press-Enterprise II*”). Because the First Amendment independently mandates open commission proceedings, the Government must satisfy its higher standard before closure is allowed.² The Government’s motion fails to do so. Testimony provided in open court may not be withheld—even for a few weeks—simply because the Government has classified it. *In re Washington Post*, 807 F.2d 383, 391-92 (4th Cir. 1986).

b. The blanket order requested by the Government that would automatically close proceedings during any testimony by a defendant and during all discussions about his treatment is procedurally improper. The United States Supreme Court has made clear that proceedings subject to the First Amendment access right may only be closed on a case by case basis. An independent judge must determine on a specific set of facts whether a need for secrecy actually has been demonstrated that is sufficient to overcome the public’s constitutional access right. *Globe Newspaper Co. v. Superior Court*, 457 U.S. 596 (1982).

c. The extensive public record concerning the interrogation and treatment of the defendants in this case, including information from the Government itself, undermines the Government’s blanket claim that the national security would be threatened by their own testimony. Barring contemporaneous public access to testimony about information already known to the public is not proper, under either the M.C.A. or the First Amendment. Transparency is essential for public acceptance of the verdict and public accountability of the

² To the extent the M.C.A. allows closure under any standard less rigorous than “substantial probability” of prejudice to national security, its authorization is inconsistent with the First Amendment, and the heightened constitutional standard must prevail. *Press Enterprise II*, 478 U.S. at 14 (rejecting “reasonable likelihood” standard as insufficiently protective of public access right).

government, and it may not lightly be restricted. *Press Enterprise II*, 478 U.S. at 14 (any closure permitted must “prevent” the threatened harm).

4. **Burden of Proof.** Because these proceedings are subject to both a statutory and constitutional right of public access, the Government bears the burden of establishing a proper factual basis for sealing any records and closing any proceedings, in whole or in part. See *Press-Enterprise Co. v. Superior Court*, 464 U.S. 501, 510 (1984) (“*Press-Enterprise I*”); *Press-Enterprise Co. II*, 478 U.S. at 15; *Lugosch v. Pyramid Co. of Onondaga*, 435 F.3d 110, 123-24 (2d Cir. 2006); *ABC, Inc. v. Stewart*, 360 F.3d 90, 106 (2d Cir. 2004); *Washington Post v. Robinson*, 935 F.2d 282, 288 (D.C. Cir. 1991).

5. **Statement of Facts.** Defendants in this capital case stand accused of planning, orchestrating and committing the most deadly acts of international terrorism in this Nation’s history: the September 11, 2001 attacks, using hijacked commercial airliners, on the World Trade Center, the Pentagon, and aborted United Airlines Flight 93 that crashed in Shanksville, Pennsylvania.

The defendants have been in U.S. custody since 2002 and 2003. During this time, by the Government’s own admission, they have been subjected to “enhanced interrogation techniques” in a CIA program designed for “high-value detainees” (“HVDs”). The treatment of the defendants while in U.S. custody continues to be the focus of significant public controversy and concern. As evidenced at their arraignment on May 5, 2012, the defendants apparently intend to make their treatment a centerpiece of their defense.

The Government asserts that any statements by the defendants about their own treatment is classified and must be kept from the public: “Because the Accused were detained and interrogated in the CIA program, they *were exposed to classified sources, methods and*

activities” so that “*any and all statements by the Accused are presumptively classified* until a classification review can be completed.” Gov’t Mot. at 6 ¶ 5g (emphasis added). The Government concedes that information about the defendants’ treatment is already publicly available, including officially acknowledged descriptions of the various “enhanced interrogation techniques” that were approved for use by the CIA. *Id.* ¶ 5i. These techniques are not secret. Nevertheless, the Government asserts that

Other information related to the program has not been declassified or officially acknowledged, and therefore remains classified. This classified information includes allegations involving (i) the location of its detention facilities, (ii) the identity of any cooperating foreign governments, (iii) the identity of personnel involved in the capture, detention, transfer, or interrogation of detainees, (iv) interrogation techniques as applied to specific detainees, and (v) conditions of confinement [REDACTED] The disclosure of this classified information would be detrimental to national security. [REDACTED]

Id. ¶ 5j. The Government also asserts that disclosure of classified information relating to DOD sources, methods and activities at JTF-GTMO would be detrimental to national security.

Id. ¶ 5k.

6. **Discussion.** The Commission should deny the Government’s over-reaching request for automatic closure of proceedings by means of a white noise generator to prohibit public access to the courtroom proceedings anytime a defendant testifies or counsel discuss anything relating to the treatment of a defendant in U.S. custody. The heart of the Government’s motion is its claim that any and all testimony by defendants in this capital case, *describing their own first-hand experience* while in U.S. custody, is presumptively “classified” and should therefore be withheld from the public for declassification review in all cases. Gov’t Mot. (AE013) at 18 (“the Accused’s statements are presumed classified until a classification review is

completed.”).³ But even if the Government’s effort to declare all such information “presumptively classified” is permissible, the classification *ab initio* of testimony given in open court constitutes an insufficient basis for automatically overriding the public’s constitutional rights, as the Government requests. Rather, the Government is required to identify to the Commission the specific secret facts whose disclosure would truly threaten national security, and if the Commission finds that disclosure would indeed create a substantial probability of harm, then *only* those facts may be subject to initial exclusion of the public, through the use of the 40-second delay or otherwise.

I.

SIMPLY DESIGNATING TESTIMONY BY DEFENDANTS AS “CLASSIFIED” DOES NOT, BY ITSELF, PROVIDE A SUFFICIENT BASIS FOR CLOSING COMMISSION PROCEEDINGS

A. The Press and Public Have An Affirmative Right of Access to Commission Proceedings

Both the Military Commissions Act (“MCA”) and the Constitution of the United States recognize a qualified right of public access to the proceedings and records of the military commissions at Guantanamo.

1. Statutory Based Right of Public Access

In first adopting the Military Commissions Act in 2006, Congress recognized the critical importance that these proceedings be conducted in the open so the watching world would accept their validity. *See, e.g.*, 152 CONG. REC. H7522, H7534 (Sept. 27, 2006) (statement of Rep.

³ While the Press Objectors do not necessarily accept as proper all of the Government’s classification decisions, and are not privy to the Government’s sealed filings in support of its motion, they are *not* asking the Commission to conduct a review (*de novo* or otherwise) of the classification decisions made by DOD or CIA officials. *See* R.M.C. 806, Discussion. Rather, the Press Objectors call upon the Commission to fulfill its constitutional duty to independently determine whether disclosure of information these agencies have deemed “classified” in open court during this criminal prosecution would create a substantial probability of harm to national security.

Hunter); 152 CONG. REC. H7508, H7509 (Sept. 27, 2006) (statement of Rep. Cole); 152 CONG. REC. H7522, H7552 (Sept. 27, 2006) (statement of Rep. Hunter); 152 CONG. REC. H7925, H7937 (Sept. 29, 2006) (statement of Rep. Sensenbrenner); 152 CONG. REC. H7925, H7945 (Sept. 29, 2006) (statement of Rep. Sensenbrenner). Congress thus expressly mandated, in 2006 *and again in 2009*, that the commission proceedings must be open to the press and public, except in certain narrowly limited circumstances. *See* 10 U.S.C. § 949d(c)(2).

Consistent with this statutory mandate, the Department of Defense Regulation for Trial by Military Commission (“Regulation” or “Reg.”), the Manual for Military Commissions (“Manual” or “R.M.C.”), and the Military Commissions Trial Judiciary Rules of Court (“R.C.”) all make plain that the proceedings are to be open to “representatives of the press, representatives of national and international organizations, . . . and certain members of both the military and civilian communities.” R.M.C. 806(a.) The “proceedings” open for public inspection include motion papers, rulings, and conference summaries that form the record. Under the Regulation, the right of access applies “from the swearing of charges until the completion of trial and appellate proceedings or any final disposition of the case.” Reg. 19-2.

Under the M.C.A., proceedings of the Commission may only be closed to the public where a military judge makes a “specific finding” that closure is “necessary” to protect information “which could reasonably be expected to cause damage to national security” or to “ensure physical safety of individuals.” *See* M.C.A. §949(c)(2). DOD cannot impose by regulation restrictions on access that are inconsistent with this statutory mandate. *See* 10 U.S.C. 949a(a) (“Pretrial, trial, and post-trial procedures” before military commissions, to be prescribed by Secretary of Defense, “may not be contrary to or inconsistent with this chapter.”) Recognizing this fact, Reg. 19-6 states that “[t]he military judge may close proceedings of military

commissions to the public *only* upon making the findings required by M.C.A. § 949d(c) and R.M.C. 806.” (Emphasis added.) *See also* Reg. 18-3 (requiring express finding, which “shall be appended to the record of trial.”).

2. Constitutional Right of Access

The First Amendment independently “protects the public and the press from abridgement of their rights of access to information about the operation of their government.” *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 584 (1980) (Stevens, J., concurring) (recognizing First Amendment right of public access to criminal trials); *Press-Enterprise Co. I*, 464 U.S. at 508 (Blackmun, J. and Stevens, J., concurring) (recognizing First Amendment right of public access to *voir dire* proceedings). The scope of this qualified constitutional right was first defined by the U.S. Supreme Court in *Richmond Newspapers*, a case involving access to a criminal trial that the State of Virginia had conducted entirely in secret. A Virginia statute granted the trial judge discretion to conduct a secret trial, but the Supreme Court held that the First Amendment created an affirmative, enforceable constitutional right of access to certain government proceedings that trumped the state statute.

The Court found this right to be implicit in the First Amendment’s guarantees of free speech and press, just as the right of association, right of privacy, right to travel the right to be presumed innocent and other rights are implicit in various provisions of the Bill of Rights.⁴ As the Court later put it in *Globe Newspaper Co. v. Superior Court*, 457 U.S. at 604, the First Amendment right of access is based upon,

⁴ *See Id.* at 577 (Burger, J.) (the right of access is “assured by the amalgam of the First Amendment guarantees of speech and press” and their “affinity to the right of assembly”); *Id.* at 585 (Brennan, J., concurring) (“the First Amendment – of itself and as applied to the States through the Fourteenth Amendment – secures such a public right of access).

the common understanding that a “major purpose of that Amendment was to protect the free discussion of government affairs.” By offering such protection, the First Amendment serves to ensure that the individual citizen can effectively participate in and contribute to our republican system of self-government. (Citation omitted.)

Richmond Newspapers “unequivocally holds that an arbitrary interference with access to important information is an abridgement of the freedoms of speech and of the press protected by the First Amendment.” 448 U.S. 583 (Stevens, J. concurring).⁵

Under the “history and policy” analysis adopted by the Supreme Court, the constitutional right of access exists where government proceedings traditionally have been open to the public, and public access plays a “significant positive role” in the functioning of the proceeding. *E.g.*, *Globe Newspaper*, 457 U.S. at 605-07; *Press-Enterprise II*, 478 U.S. at 8-9. While this right has most frequently been asserted to compel access to judicial proceedings,⁶ the right equally applies to proceedings conducted in the executive branch. *E.g.*, *New York Civil Liberties Union v. New York City Transit Auth.*, 652 F.3d 247 (2d Cir. 2011) (administrative adjudication); *Detroit Free Press v. Ashcroft*, 303 F.3d 681, 695-96 (6th Cir. 2002) (deportation hearings); *Whiteland Woods, L.P. v. West Whiteland*, 193 F.3d 177, 181 (3d Cir. 1999) (planning meeting).

⁵ Like any member of the public, the press has standing to be heard in opposition to the denial of public access. *See, e.g.*, *Globe Newspaper Co.*, 457 U.S. at 609 n.25 (“representatives of the press and general public ‘must be given an opportunity to be heard on the question of their exclusion’”) (citation omitted); *ABC, Inc. v. Powell*, 47 M.J. 363, 365 (C.A.A.F. 1997) (press has standing to complain if access is denied); *Denver Post Corp. v. United States*, Army Misc. 20041215, at *2 (A. Ct. Crim. App. Feb. 23, 2005) (noting “obvious” error in closing proceedings before allowing newspaper’s counsel to address the issue).

⁶ The constitutional right also attaches to government records in certain contexts. *See, e.g.*, *Washington Post v. Robinson*, 935 F.2d at 287-88 (First Amendment access right attaches to plea agreement); *Globe Newspaper Co. v. Pokaski*, 868 F.2d 497, 502-04 (1st Cir. 1989) (same for sealed criminal court files); *In re Search Warrant for Secretarial Area Outside Office of Gunn*, 855 F.2d 569, 573 (8th Cir. 1988) (same for search warrant affidavits); *In re New York Times Co.*, 828 F.2d 110, 114 (2d Cir. 1987) (same for pre-trial suppression motion); *Associated Press v. U.S. Dist. Court*, 705 F.2d 1143, 1145 (9th Cir. 1983) (same for all pretrial court filings).

Applying the same history and policy analysis, the First Amendment right of access plainly applies to these proceedings:

Historical Experience. William Winthrop, known as the “Blackstone of Military Law” (*Reid v. Covert*, 354 U.S. 1, 19, n. 38 (1957) (plurality opinion)), described in his classic opus on military law a history of open military tribunals that dates back centuries:

Originally, (under the Carlovingian Kings,) courts-martial . . . were held *in the open air*, and in the Code of Gustavus Adolphus. . . criminal cases before such courts were required to be tried “*under the blue skies*.” The modern practice has inherited a similar publicity.

WILLIAM WINTHROP, *MILITARY LAW AND PRECEDENTS* 161-62 (rev. 2d ed. 1920). The same tradition of public access to courts-martial also runs through the history of military commissions. After all, commissions historically have “differed from the court-martial only in terms of jurisdiction.” David W. Glazier, Notes, *Kangaroo Court or Competent Tribunal?: Judging the 21st Century Military Commission*, 89 VA. L. REV. 2005, 2092 (2003). As the Supreme Court has explained:

[T]he procedures governing trials by military commission historically have been the same as those governing courts-martial. . . . The military commission was not born of a desire to dispense a more summary form of justice than is afforded by courts-martial; it developed, rather, as a tribunal of necessity to be employed when courts-martial lacked jurisdiction over either the accused or the subject matter. *See* Winthrop 831. Exigency lent the commission its legitimacy, but did not further justify the wholesale jettisoning of procedural protections. That history explains why the military commission’s procedures typically have been the ones used by courts-martial.

Hamdan v. Rumsfeld, 126 S. Ct. 2749, 2788, 2792 (2006).⁷

⁷ The United States Court of Military Commission Review has also recognized that Congress intended the practices of military commissions to “mirror” those of courts-martial. *United States v. Khadr*, CMCR 07-001 at 23 & n.35 (Sept. 24, 2007) (citing and quoting M.C.A. §§ 949a(a) & 948b(c)).

With rare exception,⁸ military commissions have been conducted publicly throughout our nation's history:

- During the Civil War, for example, members of the 1864 military commission of Lambdin P. Milligan and others retired from the room to deliberate in order “to avoid the inconvenience of dismissing *the audience assembled to listen to the proceedings.*” WILLIAM WINTHROP, *MILITARY LAW AND PRECEDENTS* 289 (rev. 2d ed. 1920) (emphasis added and internal quotation marks omitted).
- The military commission established to try John Wilkes Booth's co-conspirators in Lincoln's assassination was opened to the public after reporters complained and Gen. Ulysses S. Grant “led them to the White House to talk to the president.” See James H. Johnston, *Swift and Terrible: A Military Tribunal Rushed to Convict After Lincoln's Murder*, WASH. POST, F1 (Dec. 9, 2001).⁹
- The military commission that tried General Tomoyuki Yamashita in 1945 was also open to the press and public. See Ass'n of Bar of City of NY, *The Press and the Public's First Amendment Right of Access to Terrorism on Trial: A Position Paper*, 22 CARDOZO ARTS & ENT. L.J. 767, 790 (2005).

The weight of experience across centuries supports the recognition of a public right of access to prosecutions in military courts.

Policies Advanced by Public Access. Justice Brennan wrote separately in *Richmond Newspapers* to underscore the crucial structural role of public access in criminal cases, describing open trials as “bulwarks of our free and democratic government.” *Richmond Newspapers*, 448 U.S. at 592 (Brennan, J., concurring). The Supreme Court in that case

⁸ A 1942 trial of Nazi saboteurs was conducted in secret, but that precedent underscores how secrecy is counterproductive in the long run. It is now widely believed that the “real reason President Roosevelt authorized these military tribunals was to keep evidence of the FBI's bungling of the case secret.” *Department of Justice Oversight: Preserving Our Freedoms While Defending Against Terrorism*, HEARINGS BEFORE THE SENATE COMM. ON THE JUDICIARY, 107th Cong. 377 (Nov. 28, 2001) (statement of N. Katyal, Visiting Professor, Yale Law School, and Professor, Georgetown University), available at http://www.judiciary.senate.gov/hearings/testimony.cfm?id=4f1e0899533f7680e78d03281fdabd2c&wit_id=4f1e0899533f7680e78d03281fdabd2c-0-0 (last visited May 13, 2012).

⁹ The openness of these Civil War era commissions is particularly significant in light of the rampant suppression of the freedom of the press and “gross violations of the First Amendment” that otherwise occurred during the Civil War era. See WILLIAM H. REHNQUIST, *ALL THE LAWS BUT ONE: CIVIL LIBERTIES IN WARTIME* (1998).

identified at least five distinct interests that are advanced by open proceedings, each of which applies to prosecutions by military commissions as well: (1) ensuring that proper procedures are being followed; (2) discouraging perjury, misconduct of participants, and biased decisions; (3) providing an outlet for community hostility and emotion; (4) ensuring public confidence in a trial's results through the appearance of fairness; and (5) inspiring confidence in government through public education regarding the methods followed and remedies granted. *See Id.*, 448 U.S. at 569-71.

Judges within the military justice system have long recognized that openness significantly assists the functioning of military tribunals in this very same fashion. Even before the Supreme Court first articulated the constitutional access right in *Richmond Newspapers*, the Court of Military Appeals had identified the functional benefits of public proceedings to include: (1) improving the quality of testimony; (2) curbing abuses of authority; and (3) fostering greater public confidence in the proceedings. *See United States v. Brown*, 22 C.M.R. 41, 45-48 (C.M.A. 1956). Just as in civilian courts, public access to military tribunals improves the performance of all involved, protects judges and prosecutors from claims of dishonesty, and provides a forum for educating the public. *See Ass'n of Bar of City of NY, "If it Walks, Talks and Squawks . . ." The First Amendment Right of Access to Administrative Adjudications: A Position Paper*, 23 CARDOZO ARTS & ENTERT. L.J. 21, 25 (2005).

For all the reasons cited in *Brown*, a long chain of precedent since *Richmond Newspapers* recognizes that the public's constitutional right of access extends to military tribunals. *See, e.g., United States v. Anderson*, 46 M.J. 728, 729 (A. Ct. Crim. App. 1997) (per curiam) (absent justification clearly set forth on the record, "trials in the United States military justice system are to be open to the public"); *United States v. Travers*, 25 M.J. 61, 62 (C.M.A. 1987) (First

Amendment right of public access extends to courts-martial); *United States v. Hershey*, 20 M.J. 433, 436, 438 n.6 (C.M.A. 1985) (finding First Amendment right of public access to a court-martial proceeding); *United States v. Scott*, 48 M.J. at 665 (same); *United States v. Story*, 35 M.J. 677, 677 (A. Ct. Crim. App. 1992) (per curiam) (same); *ABC, Inc. v Powell*, 47 M.J. 363 (C.A.A.F. 1997) (First Amendment right of access applies to investigations under Article 32).

As explained by Wigmore in his seminal treatise quoted in *Brown* “[n]ot only is respect for the law increased and intelligent acquaintance acquired with the methods of government, but a strong confidence in judicial remedies is secured which could never be inspired by a system of secrecy.” Wigmore, *Evidence* (3d ed.) § 1834, *quoted in Brown*, 22 C.M.R. at 45; *see also United States v. Hood*, 46 M.J. 728, 731 n.2 (A. Ct. Crim. App. 1996). Openness is particularly important here, given the world-wide attention being paid to these proceedings:

Secrecy of judicial action can only breed ignorance and distrust of courts and suspicion concerning the competence and impartiality of judges; free and robust reporting, criticism, and debate can contribute to public understanding of the rule of law and to comprehension of the functioning of the entire criminal justice system, as well as improve the quality of that system by subjecting it to the cleansing effects of exposure and public accountability.

Nebraska Press Ass’n v. Stuart, 427 U.S. 539, 587 (1976) (Brennan, J., concurring). *See also United States v. Clark*, 475 F.2d 240, 247 (2d Cir. 1973) (“Secret hearings – though they be scrupulously fair in reality – are suspect by nature.”); *United States v. Scott*, 48 M.J. 663, 665 (A. Ct. Crim. App. 1998) (public confidence can “quickly erode” when proceedings are closed); *United States v. Anderson*, 46 M.J. 728, 731 (Army Ct. Crim. App. 1997) (same). As one commentator has cautioned: “Conducting military commission trials today that fall short of both their historic purposes and contemporary standards of justice is likely to stain the reputation of both the American military and the American justice system as a whole.” David W. Glazier,

B. To Overcome The Public's Access Rights, The Government Must Demonstrate A Substantial Probability Of Risk To National Security

While the constitutional access right is a qualified right, not an absolute right, a proceeding subject to the First Amendment right may be closed *only* if the party seeking to seal can satisfy a rigorous four-part test. Different verbal formulations have been used by various courts to define the showing that must be made, but the governing standard applied by the Supreme Court encompasses four distinct factors:

- 1. There must be a substantial probability of prejudice to a compelling interest.** Anyone seeking to restrict the access right must demonstrate a substantial probability that openness will cause harm to a compelling governmental interest. *See, e.g., Richmond Newspapers, Inc. v. Virginia*, 448 U.S. at 582; *Press-Enterprise I*, 464 U.S. at 510; *Press-Enterprise Co. II*, 478 U.S. at 13-14. In *Press-Enterprise I*, the Supreme Court stressed that a denial of access is permissible only when “essential to preserve higher values.” 464 U.S. at 510. In *Press-Enterprise II* it specifically held that a “reasonable likelihood” standard is not sufficiently protective of the access right, and directed that a “substantial probability” standard must be applied. 478 U.S. at 14-15.
- 2. There must be no alternative to adequately protect the threatened interest.** Anyone seeking to defeat access must further demonstrate that there is nothing short of a limitation on the constitutional access right that can adequately protect the threatened interest. *Press-Enterprise II*, 478 U.S. at 13-14. A “trial judge must consider alternatives and reach a reasoned conclusion that closure is a preferable course to follow to safeguard the interests at issue.” *In re The Herald Co.*, 734 F.2d 93, 100 (2d Cir. 1984).
- 3. Any restriction on access that is imposed must be effective.** Any order limiting access must be effective in protecting the threatened interest for which the limitation is imposed. As articulated in *Press-Enterprise II*, 478 U.S. at 14, the party seeking secrecy must demonstrate “that closure would prevent” the harm sought to be avoided. *See In re The Herald Co.*, 734 F.2d at 101 (closure order cannot stand if “the information sought to be kept confidential has already been given sufficient public exposure”); *Associated Press v. U.S. District Court*, 705 F.2d 1143, 1146 (9th Cir. 1983) (must be “a substantial probability that closure will be effective in protecting against the perceived harm” (citation omitted)).

4. **Any restriction on access must be narrowly tailored.** The Supreme Court has long recognized that even “legitimate and substantial” governmental interests “cannot be pursued by means that broadly stifle fundamental personal liberties when the end can be more narrowly achieved.” *Shelton v. Tucker*, 364 U.S. 479, 488 (1960). Any limitation imposed on public access thus must be no broader than necessary to protect the threatened interest. *See, e.g., Press-Enterprise II*, 478 U.S. at 13-14; *Lugosch*, 435 F.3d at 124; *In re New York Times Co. (Biaggi)*, 828 F.2d at 116.

The adjudicatory tribunals of the military branches have applied these same standards to their proceedings. As explained in *Hershey*, “the party seeking closure must advance an overriding interest that is likely to be prejudiced [by openness]; the closure must be narrowly tailored to protect that interest; the trial court must consider reasonable alternatives to closure; and it must make adequate findings supporting the closure to aid in review.” 20 M.J. at 436; *see also Anderson*, 46 M.J. at 729 (“[T]he military judge placed no justification on the record for her actions. Consequently, she abused her discretion in closing the court-martial.”). The Army Court of Military Appeals has also applied this standard as the substantive prerequisite for a court to enter a “protective order” limiting public access to documents admitted into evidence in a court martial proceeding. *See Scott*, 48 M.J. at 665.

C. The Fact That Classified Information May Be Discussed is Not, By Itself, An Adequate Grounds for Closing A Commission Proceeding

The Government urges the Commission to close proceedings in this prosecution by interposing the white noise signal to the viewing gallery any time a defendant testifies or the treatment of a defendant is discussed by counsel. The Government considers all such information “classified,” even the first-hand accounts defendants may give during the course of their defense. Gov’t Mot. at 8-11.

The Government cannot by mere invocation of “national security” concerns purportedly arising automatically from any “classified” information justify the closing of a criminal trial. As Justice Black warned in the Pentagon Papers case:

The word ‘security’ is a broad, vague generality whose contours should not be invoked to abrogate the fundamental law embodied in the First Amendment. The guarding of military and diplomatic secrets at the expense of informed representative government provides no real security for our Republic.

United States v. New York Times Co., 403 U.S. 713, 719 (1971) (Black, J., concurring). As the Fourth Circuit has aptly noted, “the mere assertion of national security concerns by the Government is not sufficient reason to close a hearing or deny access to documents. . . . Rather, [courts] must independently determine whether, and to what extent, the proceedings and documents must be kept under seal.” *United States v. Moussaoui*, 65 F. App’x 881, 887 (4th Cir. 2003) (unpublished) (internal citation omitted).

Consistent with their obligation to uphold public access rights, courts previously have rejected the argument that the heightened First Amendment closure requirements are satisfied automatically whenever classified information is involved:

[T]roubled as we are by the risk that disclosure of classified information could endanger the lives of both Americans and their foreign informants, we are equally troubled by the notion that the judiciary should abdicate its decision-making responsibility to the executive branch whenever national security concerns are present. History teaches us how easily the spectre of a threat to “national security” may be used to justify a wide variety of repressive government actions. A blind acceptance by the courts of the government’s insistence on the need for secrecy, without notice to others, without argument, and without a statement of reasons, would impermissibly compromise the independence of the judiciary and open the door to possible abuse.

In re Washington Post, 807 F.2d 383, 391-92 (4th Cir. 1986).¹⁰

¹⁰ The Government argues in response to the ACLU Motion that there is no First Amendment right either “to reveal” or “to receive” classified information. Gov’t Response at 12 (AE013D). It’s argument misperceives the nature of the First Amendment access right—it is a right of the public to observe *this proceeding*, a right that can only be overcome where this tribunal finds a substantial probability of harm to the national security. The fact that information is deemed classified by the Government is not sufficient, by itself to close a trial.

As the Government acknowledges, the M.C.A.'s provisions governing the handling of classified information in these proceedings are derived from, and premised upon, the Classified Information Procedures Act ("CIPA"). *See* Gov't Mot. at 8. The CIPA statute does not trump presumption of access to a public trial. "Even disputes about claims of national security are litigated in the open." *Union Oil Co. v. Leavell*, 220 F.3d 562, 567 (7th Cir. 2000) (citing *New York Times Co. v. United States*, 403 U.S. 713 (1971)); *see also United States v. Progressive, Inc.*, 467 F. Supp. 990 (W.D. Wis. 1979).

Notably, all courts to address the issue have uniformly held that CIPA neither purports to – nor could it – override the requirements of the First Amendment with respect to public access to the trial itself. *See, e.g., In re Washington Post Co.*, 807 F.2d at 393 (even if CIPA "purported to resolve the issues raised here, the district court would not be excused from making the appropriate constitutional inquiry"); *Moussaoui*, 65 F. App'x at 887 (although press did not seek access to classified information, court noted "CIPA alone cannot justify the sealing of oral argument and pleadings"); *United States v. Poindexter*, 732 F. Supp. 165, 167 n.9 (D.D.C. 1990) ("CIPA obviously cannot override a constitutional right of access"); *United States v. Pelton*, 696 F. Supp. 156, 159 (D. Md. 1986) (holding that CIPA statute does not provide for the closure of a criminal trial and First Amendment standards must be satisfied prior to closure of criminal trial).¹¹ CIPA does not relieve the Government of its heavy constitutional burden to overcome the public's access right.

¹¹ *See also United States v. Rosen*, 487 F. Supp. 2d 703, 710 (E.D. Va. 2007) ("Closing a trial, even partially, is a highly unusual result disfavored by the law. A statute, even one regulating the use of classified information, should not be construed as authorizing a trial closure. . . . Rather, because a trial closure implicates important constitutional rights, CIPA should not be read to authorize closure absent a clear and explicit statement by Congress in the statutory language.")

Notwithstanding CIPA, this Commission is required to make an independent assessment of whether the Government has met its burden, and may not blindly accept the blanket insistence of secrecy for all purportedly classified information. Merely because information is classified does not automatically mean that either a “likelihood” or a “substantial probability” exists that its disclosure in a criminal prosecution will harm our national security.¹²

Moreover, it is not enough for the Government to argue that use of the 40-second delay switch to temporarily close a proceeding excludes the public only so long as needed for a subsequent classification review. The First Amendment right of access to judicial proceedings is a right of *contemporaneous* and *timely* access to information. *See, e.g., Lugosch*, 435 F.3d at 126-27 (emphasizing “the importance of immediate access where a right to access is found”); *Hirschkop v. Snead*, 594 F.2d 356, 373 (4th Cir. 1979) (“the first amendment protects not only the content of speech but also its timeliness”). As the Supreme Court observed in *Nebraska Press Association v. Stuart*, “[d]elays imposed by governmental authority” are inconsistent with the press’ “traditional function of bringing news to the public promptly.” 427 U.S. at 560-61. Put simply, “each passing day may constitute a separate and cognizable infringement of the First Amendment.” *CBS Inc. v. Davis*, 510 U.S. 1315, 1317 (1994) (Blackmun, J., in chambers) (quoting *Nebraska Press Ass’n v. Stuart*, 423 U.S. 1319, 1329 (1975) (Blackmun, J., in chambers)); *Lugosch*, 435 F.3d at 126-27 (“loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury”) (citation omitted).

¹² *See Too Many Secrets: Overclassification as a Barrier to Critical Information Sharing*: Hearing Before the Subcomm. on National Security, Emerging Threats, and International Relations of the Comm. on Government Reform, 108th Cong. 263 at 82-83 (2004) (statement of J. William Leonard, Director, Information Security Oversight Office, National Archives and Records Administration) (estimating that more than 50 percent of all classified government information has been improperly designated as such); *see also* Pub. L. 111-258, § 2, 124 Stat. 2648 (Oct. 7, 2010) codified at 6 U.S.C. § 124m & 50 U.S.C. § 135d (the Reducing Over-Classification Act) (congressional finding that “the over-classification of information . . . needlessly limits stakeholder and public access to information.”).

To satisfy its constitutional burdens, before excluding the public the Government must make a factual showing that each step of the four-part test is satisfied for specific items of information that threaten the national security. Only those items may be withheld, even temporarily.

II.

A PER SE RULE CLOSING ALL STATEMENTS ABOUT THE TREATMENT OF DEFENDANTS WOULD VIOLATE THE PUBLIC'S CONSTITUTIONAL ACCESS RIGHT

The Government improperly asks the Commission for a blanket order that would effectively close the proceedings any time there is testimony or discussion concerning the conditions of confinement and/or interrogations of a defendant while in U.S. custody. See Gov. Proposed Protective Order ¶ 43 (“the broadcast may be suspended whenever it is reasonably believed that any person in the courtroom has made or is about to make a statement or offer testimony disclosing classified information.”); Gov’t Mot. at 18 (“the Accused’s statements are presumed classified”). Under settled precedent, such a *per se* presumption of harm flowing inevitably from any testimony by a defendant in all circumstances is not a proper basis for denying access rights.

In *Globe Newspaper Co. v. Superior Court*, 457 U.S. 596 (1982), the Supreme Court struck down a Massachusetts statute that imposed such a *per se* exclusion of the public from criminal trials of certain sexual offenses during the testimony of any minor victim. *Id.* at 610-11. Even though the interest of protecting minor sex crime victims from additional trauma is undoubtedly a compelling one, the Supreme Court held that the statute did not allow for the constitutionally required case-by-case review and findings necessary to justify closure. *Id.* at 607-08. As *Globe Newspaper* makes clear, *per se* rules that restrict First Amendment rights, by definition, are not sufficiently “narrowly tailored” to pass constitutional muster. *See also*

Florida Star v. B.J.F., 491 U.S. 524, 539-40 (1989) (“We have previously noted the impermissibility of categorical prohibitions upon media access where important First Amendment interests are at stake.”) (citing *Globe Newspaper Co. v. Superior Court*, 457 U.S. 596, 608 (1982)). The Commission should therefore reject the Government’s request for a per se presumption of harm arising from any and all testimony concerning the defendants’ confinement, treatment and interrogation while in U.S. custody. The First Amendment requires a case-by-case determination and particularized findings that closure is necessary, *in a particular set of circumstances*, to protect a governmental interest of the highest order.

III.

THE GOVERNMENT HAS NOT ESTABLISHED ANY PROPER BASIS FOR CLOSING THESE PROCEEDINGS

The requested closure order is overbroad for the further reason that a great deal is already known about the nature of the interrogation of these defendants and the conditions of their confinement. The Government cannot credibly establish a risk to national security from testimony about information that is already widely known and available on the Internet.

The circumstances of these defendants’ treatment while in custody has been the subject of significant attention worldwide and raises issues of profound public interest. While the Government’s motion suggests that only “a limited amount of information relating to the CIA program” of detaining and interrogating “high-value detainees” is publicly known, Gov’t Mot. at 6, in fact, rather detailed information concerning the treatment and interrogations of defendants has already been the subject of reports and memoranda publicly released by the United States Government. Among the disclosures:

- A publicly-released U.S government memorandum describes the interrogation techniques the CIA was authorized to use and provides great detail about the

treatment of particular detainees, including that defendant Mohammad was waterboarded 183 times in March 2003.¹³

- A CIA Inspector General's report describes several instances of coercive techniques used by the CIA that exceeded authority provided to the CIA, providing details of actual techniques used, with such examples as the threat to defendant Mohammad that "if anything else happens in the United States, 'We're going to kill your children.'"¹⁴ Id. ¶ 95.
- An FBI report discloses several incidents of prolonged shackling or stress positions, including that from other agents or from detainees. For example, one FBI agent told the OIG that defendant Abdel Aziz complained that he had been subjected to yelling, short-shackling, lowered room temperature, strobe lights, and music, and that he was left in the interrogation room for over 12 hours with no food, bathroom breaks, or breaks to pray.¹⁵

See ACLU Mot. at 24-28 (summarizing facts disclosed in several declassified memoranda and other official U.S. Government records public disclosed); see also *Background Paper on CIA's Combined Use of Interrogation Techniques*, available at <http://bit.ly/3YJp0>.

Many reports of international organizations and press accounts have provided additional information about the interrogation of detainees and their treatment while in custody.¹⁶ The

¹³ Memorandum from Steven G. Bradbury to John A. Rizzo, Re: Application of United States Obligations Under Article 16 of the Convention Against Torture to Certain Techniques That May Be Used in the Interrogation of a High Value al Qaeda Detainee (May 10, 2005), at 8, available at <http://bit.ly/Iltguh>.

¹⁴ CIA Office of the Inspector General, Counterterrorism Detention and Interrogation Activities (September 2001 – October 2003) (May 7, 2004), ¶ 95, available at <http://wapo.st/3JNHM> ("IG Report"). [declassified August 24, 2009]

¹⁵ Justice Department Office of the Inspector General Review of the FBI's Involvement in and Observations of Detainee Interrogations in Guantanamo Bay, Afghanistan and Iraq, (May 20, 2008) (Part 5, p. 182, available at http://www.aclu.org/files/pdfs/safefree/OIG_052008_158_207.pdf)

¹⁶ See, e.g., International Committee for the Red Cross, *ICRC Report on the Treatment of Fourteen "High Value Detainees" in CIA Custody* (Feb. 2007) (ICRC Report), available at <http://assets.nybooks.com/media/doc/2010/04/22/icrc-report.pdf>. (based on interviews with 14 detainees, including the five defendants, detailing interrogations techniques used on defendants and conditions of confinement); Joby Warrick, Peter Finn & Julie Tate, *Red Cross Described 'Torture' at CIA Jails*, WASHINGTON POST (Mar. 16, 2009), available at <http://www.washingtonpost.com/wp-dyn/content/article/2009/03/15/AR2009031502724.html> (summarizing ICRC Report, reporting that "the captives were routinely beaten, doused with cold water and slammed head-first into walls. . . they were stripped of clothing, bombarded with loud music, exposed to cold temperatures, and deprived of sleep and solid food for days on end. Some detainees described being forced to stand for days, with their arms

Government suggests that such public reports are not significant to the continued status of the information as “classified” if facts have not been confirmed U.S. officials, but the fact that these reports are known and available on the Internet has an obvious significance to the issue of whether testimony by defendants concerning this same information has any substantial probability of damaging our national security.

The Government identifies five categories of information about these defendants, the release of which it contends could damage national security, but fails to make a convincing showing on the publicly known facts:

- (i) Location of detention facilities. As documented in the ACLU motion for public proceedings (AE013A), the public results of investigations by the United Nations and European officials identify six nations as places where these defendants were held while in U.S. custody. (ACLU Mot. at 29-30.) The identified locations include the Polish village of Stare Kiejkut, Bucharest, Romania, Afghanistan, Thailand, Lithuania and Morocco.¹⁷

shackled above them, wearing only diapers”); Peter Taylor, ‘*Vomiting and screaming*’ in *destroyed waterboarding tapes*, BBC (May 9, 2012), *available at* <http://www.bbc.co.uk/news/world-us-canada-17990955> (describing treatment of defendant Mohammed by CIA interrogators, which “included being deprived of sleep for over a week, standing naked, wearing only a nappy, and being waterboarded 183 times”).

¹⁷ See, e.g., U.N. Human Rights Council, *Joint Study on Global Practices in Relation to Secret Detention in the Context of Countering Terrorism*, ¶ 114, U.N. Doc.A/HRC/13/42 (May 20, 2010), *available at* <http://bit.ly/cziSQ> (Mr. Mohamed, Mr. bin al-Shibh, and Mr. bin Attash held in the Polish village of Stare Kiejkut between 2003 and 2005.); Alex Spillius, *CIA ‘Used Romania Building as Prison for Khalid Sheikh Mohammed,* TELEGRAPH (Dec. 8, 2011), (Mr. Mohammed and Mr. bin Attash transferred “Poland to Bucharest in September 2003,” and “Ramzi Binalshibh . . . w[as] also moved to Romania,” noting that “[t]he prison [in Romania] was part of a network of so-called ‘black sites’ that included prisons in Poland, Lithuania, Thailand and Morocco operated by the CIA.”); Dana Priest, *CIA Holds Terror Suspects in Secret Prisons*, WASHINGTON POST (Nov. 2, 2005), <http://wapo.st/Ud8UD>, (“Sept. 11 planner Ramzi Binalshibh was also captured in Pakistan and flown to Thailand.”); Molly Moore, *Report Gives Details on CIA Prisons*, WASHINGTON POST (June 9, 2007), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/06/08/AR2007060800985_2.html (Mr. Mohammad was detained and interrogated at “[a] facility at Poland’s Stare Kiejkuty intelligence training

- (ii) Identity of Cooperating Foreign Governments. The 9-11 Commission Final Report (at 385) identifies Pakistan as playing a leading role in the capture of defendant Mohammad, and the International Committee for the Red Cross has reported that all defendants in this case were arrested by Pakistani national police/security forces.¹⁸ Swiss officials have stated that there is enough evidence to establish that “secret detention facilities run by the CIA did exist in Europe from 2003-2005, in particular in Poland and Romania.”¹⁹ It was widely reported that videotapes of interrogations were recorded in Morocco by the Moroccan intelligence service and provided to the CIA by Moroccan officials.²⁰
- (iii) Identity of Personnel Involved. Some interrogators have publicly been identified,²¹ and names of specific individuals can be withheld in any event

base”); Siobhan Gorman, *CIA Interrogation Tapes of 9/11 Planner Are Found*, WALL STREET JOURNAL (Aug. 17, 2010), available at <http://online.wsj.com/article/SB10001424052748704554104575435272683060714.html?KEYWORDS=Binalshibh+interrogation> (Mr. Binalshibh was captured “in Karachi, Pakistan, on Sept. 11, 2002,” and later “transferred to Afghanistan and then Morocco.”).

¹⁸ International Committee for the Red Cross, *ICRC Report on the Treatment of Fourteen “High Value Detainees” in CIA Custody*, (Feb. 2007) (ICRC Report), at 5, available at <http://assets.nybooks.com/media/doc/2010/04/22/icrc-report.pdf>.

¹⁹ Jon Boyle, *Secret CIA jails hosted by Poland, Romania: watchdog* REUTERS (Jun. 8, 2007), available at <http://www.reuters.com/article/2007/06/08/us-security-renditions-idUSL0870585420070608>

²⁰ Siobhan Gorman, *CIA Interrogation Tapes of 9/11 Planner Are Found*, WALL STREET JOURNAL (Aug. 17, 2010), available at <http://online.wsj.com/article/SB10001424052748704554104575435272683060714.html?KEYWORDS=Binalshibh+interrogation>; Associated Press, *9/11 plotter interrogation tapes found under CIA desk*, NEW YORK POST (Aug. 17, 2010), available at http://www.nypost.com/p/news/national/plotter_interrogation_tapes_found_ozV9gaEh0bhprlCSurWWRI#ixzz1ul4DYEnk

²¹ E.g., Scott Shane, *Inside a 9/11 Mastermind’s Interrogation*, THE NEW YORK TIMES (June 22, 2008), available at http://www.nytimes.com/2008/06/22/washington/22ksm.html?_r=1&ref=khalidshaikhmohammed (interrogator Mr. Deuce Martinez “did not engage in EIT”).

without the drastic closure of all statements about defendants' treatment requested by the Government.

(iv) Interrogation Techniques, as Applied to Specific Defendants. The same official reports and press coverage of the information gathering techniques used by the CIA generally disclose much about the application of those techniques to the defendants in this case specifically. For example, the ICRC discloses:

- Defendant Mohammed gave a detailed description of the techniques used during his interrogation: “I would be strapped to a special bed, which can be rotated into a vertical position. A cloth would be placed over my face. Water was then poured onto the cloth by one of the guards so that I could not breathe. This obviously could only be done for one or two minutes at a time. The cloth was then removed and the bed was put into a vertical position. The whole process was then repeated during about 1 hour.’ As during other forms of ill-treatment he was always kept naked during the suffocation. Female interrogators were also present during this form of ill-treatment, again increasing the humiliation aspect. . . . [He also] alleged that, apart from the time when he was taken for interrogation, he was shackled in the prolonged stress standing position for one month in his third place of detention (he estimates he was interrogated for approximately eight hours each day at the start of the month gradually declining to four hours each day at the end of the month). . . . And “alleged that, in his third place of detention: ‘a thick plastic collar would be placed around my neck so that it could then be held at the two ends by a guard who would use it to slam me repeatedly against the wall.’” And also alleged “that on a daily basis during the first month of interrogation in his third place of detention: ‘if I was perceived not to be cooperating I would be placed against a wall and subjected to punches and slaps in the body, head and face.’”²²
- Defendant Binalshib “alleged that he was shackled in [the prolonged stress standing] position for two to three days in Afghanistan his second place of detention and for seven days in his fourth . . .” And defendant Bin Attash alleged he was held in the same position “for two weeks with two or three short breaks where he could lie down in Afghanistan and for several days in his fourth place of detention . . . *Id.* at 11.
- Defendant Bin Attash “alleged that during interrogation in Afghanistan: ‘on a daily basis during the first two weeks a collar was looped around my

²² ICRC Report at 9-13.

neck and then used to slam me against the walls of the interrogation room. It was also placed around my neck when being taken out of my cell for interrogation and was used to lead me along the corridor. It was also used to slam me against the walls of the corridor during such movements. . . . And further alleged “that: ‘every day for the first two weeks [in Afghanistan] I was subjected to slaps to the face and punches to the body during interrogation. This was done by one interrogator wearing gloves. He was then replaced by a second interrogator who was more friendly and pretended that he could save me from the first interrogator.’” He further described the following from his detention in Afghanistan: ‘on a daily basis during the first two weeks I was made to lie on a plastic sheet placed on the floor which would then be lifted at the edges. Cold water was then poured onto my body with buckets. They did not have a hosepipe to fill the sheet more easily. This jail was not so well equipped for torture.’ He was kept enveloped within the sheet with the cold water for several minutes. In his next place of detention, he was allegedly doused every day during the month of July 2003 with cold water from a hosepipe. He commented that: ‘in this place of detention they were rather more sophisticated than in Afghanistan because they had a hosepipe with which to pour water over me.’” Defendant Bin Attash also has alleged that he was made to wear a garment that resembled a diaper. *Id.* at 11-16.

- “Defendant Binalshib alleged that he was: ‘*splashed with cold water from a hose*’ during interrogation in his fourth place of detention and that in his eighth place of detention he was: ‘*restrained on a bed, unable to move, for one month, February 2005 and subjected to cold air-conditioning during that period.*’” And he further states that “he was kept permanently handcuffed and shackled throughout his first six months of detention. During the four months he was held in his third place of detention, when not kept in the prolonged stress standing position, his ankle shackles were allegedly kept attached by a one meter long chain to a pin fixed in the corner of the room where he was held.”²³

²³ *Id.* at 16-17. See also, e.g., Jess Bravin, *Guantanamo Judge Grapples With Disruptive Terror Suspects*, WALL STREET JOURNAL (May 6, 2012), available at <http://online.wsj.com/article/SB10001424052702304752804577386102452510454.html?KEYWORDS=khalid+> (disclosing that all five defendants were held in CIA “black sites,” or secret overseas prisons, where U.S. authorities inflicted brutal treatment including, in some instances, waterboarding.”); Scott Shane, *Inside a 9/11 Mastermind’s Interrogation*, THE NEW YORK TIMES (June 22, 2008), available at http://www.nytimes.com/2008/06/22/washington/22ksm.html?_r=1&ref=khalidshaikhmohammed (explaining how the CIA program worked: “A paramilitary team put on the pressure, using cold temperatures, sleeplessness, pain and fear to force a prisoner to talk. When the prisoner signaled assent, the tormenters stepped aside. After a break that could be a day or even longer, Mr. Martinez or another interrogator took up the questioning . . . whether it was a result of a fear of waterboarding, the patient trust-building mastered by Mr. Martinez or the demoralizing effects of isolation, Mr. Mohammed and some other prisoners had become quite compliant.”); Jane Mayer, *The Trial: Eric Holder and the battle over Khalid Sheikh Mohammed*, THE NEW YORKER (Feb. 15, 2010), available at

Moreover, because the techniques themselves are publicly known, it is hard to understand how discussion of their application in a particular case could create any real risk to our national security.

- (v) Conditions of Confinement. Published reports are equally detailed in discussing the conditions of defendants' confinement, noting such facts as that various defendants were kept naked for weeks, continuously shackled, had their heads shaved with some spots left in order to make them "look and feel particularly undignified and abused," were deprived of solid food for weeks, denied any possibility of exercise, and denied the Koran for long periods.²⁴

This is just a sampling of the readily available public information. The Commission can, indeed *must*, take notice of the extensive amount of information that is already in the public domain – much of it as a direct result of official U.S. Government statements and publications – concerning the conditions of confinements, interrogations, and treatment of the defendants.

In light of the large amount of publicly available and officially acknowledged information, disclosure of the testimony by defendants concerning these same facts cannot realistically pose a "substantial probability" of damage to the national security. There is simply no basis for closing proceedings that address information already in the public domain. *See, e.g., In re Charlotte Observer*, 882 F.2d 850, 853-55 (4th Cir. 1989) (finding it "dubious" that harm to defendant's fair trial rights will result from re-publication of information already in the public domain; and, "[w]here closure is wholly inefficacious to prevent a perceived harm, that alone suffices to make it constitutionally impermissible."); *In re New York Times*, 828 F.2d 110, 116

http://www.newyorker.com/reporting/2010/02/15/100215fa_fact_mayer#ixzz1uhvwdE6l (discussing the hundred and eighty-three sessions of waterboarding on defendant Mohammad).

²⁴ ICRC Report at 14-20.

(2d Cir. 1987) (holding that sealing of court papers is not proper where much of the information contained in them “has already been publicized”); *CBS v. U.S. Dist. Court*, 765 F.2d 823, 825 (9th Cir. 1985) (finding that a substantial probability of prejudice cannot exist when “most of the information the government seeks to keep confidential concerns matters that might easily be surmised from what is already in the public record”).

To shield from public view the entirety of defendants’ testimony would violate the public’s constitutional rights and undermine the legitimacy and credibility of military commissions. “Not only is respect for the law increased and intelligent acquaintance acquired with the methods of government, but a strong confidence in judicial remedies is secured which could never be inspired by a system of secrecy.” *United States v. Brown*, 22 C.M.R. 41, 45 (C.M.A. 1956) (quoting Wigmore, *Evidence* § 1834 (3d ed.)), *overruled, in part, on other grounds by United States v. Grunden*, 2 M.J. 116 (C.M.A. 1977); *United States v. Travers*, 25 M.J. 61, 62 (C.M.A. 1987) (“public confidence in matters of military justice would quickly erode if courts-martial were arbitrarily closed to the public.”); *United States v. Hood*, 46 M.J. 728, 731 & n.2 (A. Ct. Crim. App. 1996) (“Openness thus enhances both the basic fairness of the criminal trial and the appearance of fairness so essential to public confidence in the system.” (quoting *Press-Enterprise I*, 464 U.S. at 508)).

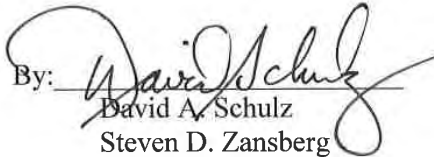
7. **Oral Argument.** The Press Objectors request the Court to entertain oral argument, including allowing the Press Objectors to be heard, through counsel, before closing to the public any portion (including through the use of the “white noise” signal to redact portions of the audio feed from the courtroom) of these proceedings. *See, e.g., Globe Newspaper Co. v. Superior Court*, 457 U.S. 596, 609 n.25 (1982) (“representatives of the press and general public ‘must be given an opportunity to be heard on the question of their exclusion.’”) (emphasis

added); *Phoenix Newspapers, Inc. v. U.S. Dist. Court*, 156 F.3d 940, 949 (9th Cir. 1998) (“[The court] must provide sufficient notice to the public and press to afford them the opportunity to object or offer alternatives [to closure]. If objections are made, a hearing on the objections must be held as soon as possible.”).

WHEREFORE, Press Objectors respectfully ask this honorable Tribunal to deny the Government’s Motion to Protect Against Disclosure of National Security Information.

Dated: May 16, 2012
New York, New York

LEVINE SULLIVAN KOCH & SCHULZ, L.L.P.

By: 
David A. Schulz
Steven D. Zansberg

321 West 44th Street, Suite 510
New York, NY 10036
Email: dschulz@lkslaw.com
Tel: (212) 850-6100
Fax: (212) 850-6299

Attorneys for Press Objectors

Tab 5

**Military Commissions Trial Judiciary
Guantanamo Bay, Cuba**

UNITED STATES OF AMERICA

v.

KHALID SHAIKH MOHAMMAD,
WALID MUHAMMAD SALIH MUBARAK
BIN 'ATTASH,
RAMZI BINALSHIBH,
ALI ABDUL AZIZ ALI ,
MUSTAFA AHMED ADAM AL-HAWSAWI

AE 013H

**Reply of the
American Civil Liberties Union**
to the Government's Response to the
Motion for Public Access to
Proceedings and Records

May 23, 2012

- 1. Timeliness.** This reply is timely filed pursuant to Military Commissions Trial Judiciary Rule of Court 3.7.d(2).
- 2. Overview.** The government's response to the ACLU's motion for public access is remarkable both for what it leaves out and what it claims. The government fails to address the constitutional basis for the ACLU's motion—the public's First Amendment right to access these proceedings—which this commission must adjudicate, and which overrides any statutory provisions to the contrary in the Military Commissions Act of 2009. In order to adjudicate the public's First Amendment right of access, this commission must determine the propriety of the government's classification of detainees' own accounts of their experiences in government custody.

The classification authority the government continues to claim is legally untenable and morally abhorrent. There is simply no basis in law (and the government cites none) for the government to classify and suppress defendants' own accounts of an illegal government torture and detention program the whole purpose of which was to "disclose" the torture and detention to the defendants by subjecting them to it.

Even if this commission were nevertheless to find that the government's classification of some or all of defendants' own statements about government mistreatment is proper, it must still determine whether the government's broad request for presumptive closure of these proceedings meets the First Amendment right-of-access test. The closure the government seeks is not narrowly tailored, and may not be used to shield these crucially important proceedings from public view.

Courts' recognition of the public's First Amendment right of access to judicial proceedings is predicated on the need to ensure legitimacy of those proceedings in the eyes of the public. *See* ACLU Mot. 9–10. This commission is undoubtedly aware that there is a long-running debate, both in the United States and abroad, about the legitimacy and fairness of the entire commission system. That debate may not be ended or cured by the commission's decision on the government's request to classify and suppress the defendants' accounts of government misconduct. But it is a certainty that the commission will not be seen as legitimate if the proceedings have at their heart the government's judicially-approved censorship of the defendants' accounts of their torture.

3. Legal Basis for Relief Requested.

A. The First Amendment Protects the Public's Right of Meaningful Access to These Proceedings.

The government's reply does not address—and nor does it contest—the gravamen of the ACLU's motion: the public's right of access to these military commission proceedings is mandated by the First Amendment, and may only be overcome if the government presents evidence of a substantial likelihood of harm to an overriding government interest, and its requested closure of the proceedings is narrowly tailored. ACLU Mot. 5–11 (discussing First Amendment right of access and standard); Press

Objectors’ Mot. 14–15. Although the government fails to grapple with the public’s First Amendment rights at stake here, this military commission must.¹ Once the First Amendment right is raised and attaches, this commission must adjudicate it. *Globe Newspaper Co. v. Superior Court*, 457 U.S. 596, 609 n.25 (1982) (“[R]epresentatives of the press and general public ‘must be given an opportunity to be heard on the question of their exclusion.’”).

In order to apply the First Amendment right-of-access test, this military commission must determine whether the government’s classification of detainees’ own accounts of their detention, torture and other mistreatment is proper. *See* ACLU Mot. 12–17. For the reasons set forth in Section B below, it is not. Even if the military commission were to find that the government has somehow properly classified some or all of defendants’ statements concerning their personal knowledge of their detention and mistreatment, it must still determine whether the government’s proposed blanket closure of the public’s access to all of defendants’ testimony satisfies the First Amendment strict

¹ The government bases its opposition to the ACLU’s motion on the right of access provisions in the Military Commissions Act of 2009 (“MCA”) and the 2010 Manual for Military Commissions (“Manual”). Gov’t Mot. 11–14; Gov’t Resp. 7–10. When Congress enacted the MCA, it rightly recognized that commission proceedings must be open to the public, subject to narrow exceptions. 10 U.S.C. § 949d(c); *see also* ACLU Mot. 11–12. But the MCA’s standard for closure has a lower threshold than the First Amendment standard. 10 U.S.C. § 949d(c)(2) (requiring military judge to make a “specific finding” that closure is necessary to protect information “which could *reasonably* be expected to cause damage to national security” (emphasis added)). The Supreme Court has squarely held that a statutory “reasonable likelihood” standard does not adequately protect the public’s constitutional rights, and that the First Amendment requires a court to find that any harm asserted by the government meets a higher “substantial likelihood” standard. *Press-Enterprise Co. v. Superior Court*, 478 U.S. 1, 13–14 (1986) (“*Press-Enterprise II*”); *see also* *Doe v. Gonzales*, 500 F. Supp. 2d 379, 411 (S.D.N.Y. 2007), *aff’d in part and rev’d in part sub nom, John Doe, Inc. v. Mukasey*, 549 F.3d 861 (2d Cir. 2008). To the extent the government’s proposed protective order is based on MCA provisions derived from the Classified Information Procedures Act, Gov’t Mot. 12–14, neither the MCA nor CIPA excuse this commission “from making the appropriate constitutional inquiry” under the First Amendment because the commission “may not simply assume that Congress has struck the correct constitutional balance.” *In re Wash. Post Co.*, 807 F.2d 383, 393 (4th Cir. 1986).

scrutiny test. For the reasons set forth in Section C, the government cannot satisfy the First Amendment's searching requirements.

B. The Government Fails to Justify its Classification and Suppression of Defendants' Personal Accounts of Their Abuse and Mistreatment in Government Custody.

The ACLU has argued that the government lacks authority, under Executive Order 13,526, to classify the defendants' own accounts of their detention, torture and abuse, which the government coercively and illegally imposed upon them. Indeed, the government's ability to suppress the defendants' statements derives initially from the fact that the CIA illegally detained them *incommunicado*. Cf. CIA Office of the Inspector General, *Counterterrorism Detention and Interrogation Activities (September 2001 – October 2003)* (May 7, 2004), available at <http://wapo.st/3JNHM> ("IG Report") at 96 (finding, in a section entitled "Endgame," that the CIA "has an interest in the disposition of detainees and a particular interest in those who, if not kept in isolation, would likely divulge information about the circumstances of their detention"). The government's continued suppression of defendants' statements depends on its ability either to keep the defendants in indefinite detention or to impose the death penalty without defendants' accounts becoming public at their trial—if this commission so permits.²

The government mischaracterizes the ACLU's argument. The ACLU does not allege "that the government has no legal authority to make a presumptive determination that statements of the accused are classified pending review by an [Original Classification Authority]." Gov't Resp. 10. That characterization wrongly assumes the ACLU's

² Indeed, former prisoners who were subject to the CIA's illegal detention and torture program and were subsequently released have spoken publicly about their experience in CIA custody. The government could not silence them under any colorable legal theory. See, e.g., Dana Priest, *Wrongful Imprisonment: Anatomy of a CIA Mistake*, Wash. Post, Dec. 4, 2005, <http://wapo.st/eaMIRS> (providing former CIA prisoner Khaled el-Masri's own account of his experience).

concern is only with the presumption of classification and not the classification itself. Rather the ACLU contends—and asks this commission to find—that the government does not have the legal authority to classify information that the government itself disclosed to defendants, who the government acknowledges were not authorized to receive classified information and would be under no obligation to keep silent about it. Gov’t Resp. 11 (each defendant is an “accused who does not hold a security clearance and who owes no duty of loyalty to the United States”).

The core argument the government makes in support of classification to this commission and in response to the ACLU is legally untenable. According to the government, “[b]ecause the Accused were detained and interrogated in the CIA program, they were exposed to classified sources, methods, and activities. Due to their exposure to classified information, the Accused are in a position to reveal this information publicly through their statements.” Gov’t Mot. 6; Gov’t Resp. 10. The government fails utterly to explain how it has a legitimate interest, let alone a compelling one, in suppressing information about a CIA coercive interrogation and detention program that was illegal and has been banned by the President. *See* ACLU Mot. 21–24.

Even if the CIA program could properly be classified, the government cannot justifiably argue that it can also classify and suppress defendants’ own accounts of their experiences because the government itself disclosed the program to defendants. Put another way, if the government is correct that the CIA’s detention and interrogation program was properly classified, then it also follows that the very goal of the program was to disclose—deliberately, purposefully, and with authorization from the highest levels of government—classified information to individuals who the government

concedes were not authorized to receive it. Worse, the government disclosed classified information through coercion: it forced the defendants to acquire their knowledge of the secret methods of torture, abuse and confinement to which the government subjected them, the location of the secret foreign detention sites at which the government forcibly held them, and (to the extent defendants are aware of these) the identities of foreign and U.S. government agents who perpetrated abuses on the them.

The government's claimed authority to gag defendants goes far beyond any that the courts have found permissible under the First Amendment. Courts generally uphold the suppression of properly classified information in the face of a First Amendment challenge if there is a *voluntary* relationship of privity between the government and the individual in possession of classified information. ACLU Mot. 19–20 (citing cases). That is primarily the context in which the government's assertion that "[t]here is no First Amendment right to reveal properly classified information" applies. Gov't Resp. 11 (citing *Stillman v. CIA*, 319 F.3d 546, 548 (D.C. Cir. 2003) (former CIA employee could not publicly discuss information covered by non-disclosure agreements with CIA); *Snepp v. United States*, 444 U.S. 507 (1980) (CIA agent's employment agreement with Agency stipulated a relationship of trust, prohibiting him from publishing information about CIA activities without CIA review); *ACLU v. DOD*, 584 F. Supp. 2d 19, 25 (D.D.C. 2008) *vacated*, 664 F. Supp. 2d 72, 79 (D.D.C. 2009) (summary discussion finding no First Amendment right in Freedom of Information Act case)). It goes without saying that there has been no voluntary relationship, let alone a relationship of trust, between the government and the defendants to whom it disclosed classified information.

Indeed, even when properly classified national security information is leaked, the Supreme Court has held that the government may not prevent its publication on the front pages of this nation's leading newspapers. *United States v. N.Y. Times Co.*, 403 U.S. 713 (1971). Here, the government is seeking to suppress its own purposeful disclosure of classified information to defendants in a judicial proceeding to which the American public has a presumptive First Amendment right of access. It may not do so.

The government's remaining arguments in support of classification are no more persuasive. The government asserts the fact that the Executive Branch alone determines whether to classify information, and that the Supreme Court has held that classification decisions are due judicial deference. Gov't Resp. 10 (citing *Dep't of Navy v. Egan*, 484 U.S. 518 (1988) and *CIA v. Sims*, 471 U.S. 159, 169 (1985)). Neither *Egan* nor *Sims* even remotely contemplates the use of classification authority in the radical manner the government asserts in these proceedings, however. *Egan* concerns the Executive Branch's discretion to deny a security clearance to an individual who sought to access information that was concededly properly classified; here, the propriety of the government's classification must be reviewed by this commission, and the government itself acknowledges that it disclosed the information to prisoners who did not have (and surely have never sought) a security clearance. *Sims* addressed the question of the scope of National Security Act's protection of an intelligence source from compelled disclosure, and made clear that the CIA may withhold only information about sources or methods that "fall within the Agency's mandate." 471 U.S. at 169. Because the CIA's so-called "enhanced interrogation techniques" are illegal and have been categorically prohibited by the President, and its overseas detention and interrogation facilities have

been permanently closed, neither is within the Agency’s mandate. Exec. Order No. 13,491, 74 Fed. Reg. 4893 (Jan. 22, 2009). Although *Sims and Egan* both acknowledge that courts owe some deference to Executive Branch classification decisions, it is also true, in a variety of contexts, that courts—including military courts—nevertheless review the propriety of those decisions, as this commission must do. See *United States v. Grunden*, 2 M.J. 116, 121–23 & n.14 (C.M.A. 1977) (proceedings may be closed only after court determines that information is properly classified and “determine[s] whether a particular classification was done in an arbitrary and capricious manner, thereby compelling its disclosure”); *United States v. Lonetree*, 31 M.J. 849, 854 (N-M.C.M.R. 1990), *aff’d in part*, 35 M.J. 396 (C.M.A. 1992) (military trial judge appropriately “conducted [his] own analysis of the affidavits and the interests at stake” in assessing whether the government had “set[] forth valid reasons for the classification of the information and why it could not be revealed in public session”); see also, e.g., *Wilson v. CIA*, 586 F.3d 171, 185–86 (2d Cir. 2009) (requiring courts “to ensure that the information in question is, in fact, properly classified”).

It is a dark and shameful irony of the government’s own creation that even as it tells this commission and the public that “the government has a strong interest in ensuring public access to these historic proceedings” so it can demonstrate that “the accused receives stronger protections than an accused in many respected criminal-justice systems around the world,” Gov’t Resp. 7, it asks this commission to collude with it in an unprecedented effort to classify improperly and suppress detainees’ accounts of government torture and secret detention. This military commission should reject the

government's legally impermissible and morally abhorrent classification claim, and not further undermine the already-contested legitimacy of this entire historic trial.

C. The Government Fails to Show that its Proposed Blanket Suppression of Defendants' Personal Accounts of Government Misconduct Satisfies the First Amendment's Searching Standards.

The government's mere assertion that classified information may—or even will—be disclosed during these proceedings does not satisfy the First Amendment strict scrutiny standard. Gov't Mot. 8–11; *In re Wash. Post Co.*, 807 F.2d at 391–92 (“[T]roubled as we are by the risk that disclosure of classified information could endanger the lives of both Americans and their foreign informants, we are equally troubled by the notion that the judiciary should abdicate its decision-making responsibility to the executive branch whenever national security concerns are present.”); *see also N.Y. Times Co.*, 403 U.S. at 719 (Black, J., concurring) (“The word ‘security’ is a broad, vague generality whose contours should not be invoked to abrogate the fundamental law embodied in the First Amendment.”).

Even if this commission were to find that the government's classification of all or even some of defendants' statements about their own treatment in government custody is proper, the commission must determine whether the government has met its First Amendment burden of showing, based on factual evidence, that (1) the disclosure of specific information would result in a substantial likelihood of harm to a compelling government interest, (2) no means other than closure can avoid the specific threatened harm, (3) closure would effectively prevent the harm, and (4) closure is narrowly

tailored.³ *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 582–84 (1980); *Press-Enterprise Co. v. Superior Court*, 464 U.S. 501, 510 (1984) (“*Press-Enterprise I*”); *Press-Enterprise II*, 478 U.S. 1 at 13–14; *Lugosch v. Pyramid Co. of Onodaga*, 435 F.3d 110, 123–24 (2d Cir. 2006); *United States v. Hershey*, 20 M.J. 433, 436 (C.M.A. 1985).

On its face, the government’s blanket request for the presumptive closure of the proceedings in order to suppress detainees’ accounts of their detention and interrogation does not meet the first three requirements of the First Amendment right-of-access test.

In addition, the government’s primary defense of its continued classification and presumptive suppression of defendants’ statements—its assertion that “many details that relate to the capture, detention, and interrogation of the accused” remain classified, Gov’t Resp. 12—is squarely refuted by the government’s own declassified disclosures, which reveal in concrete and meticulous detail how the CIA applied so-called “enhanced interrogation techniques” against defendants, and even how the CIA exceeded the authority it was given to apply those techniques. ACLU Mot. 24–31. It is also undercut by the vast number of press accounts and reports of official U.N. and European government investigations that further describe the government’s use of torture and abuse against defendants, as well as the foreign detention sites in which it held defendants. ACLU Mot. 24–31; Press Objectors’ Mot. 21–26. The government argues that to the extent these press and other accounts are based on classified information that is leaked into the public domain, that information is not automatically declassified and cannot be further disclosed unless the government officially acknowledges it. Gov’t Resp. 13.

³ The government’s claim that the ACLU is attempting “to substitute its judgment” for that of the government is disingenuous. Gov’t Resp. 12, 13. As the ACLU’s motion makes abundantly clear, it is this commission which must subject the government’s proposed grounds for closing these proceedings to the First Amendment strict scrutiny test.

Although that is an accurate statement of the “official acknowledgement” doctrine, leaks and other “unofficial disclosures,” either by the press or other sources, do lessen the harm caused by further unofficial disclosure, a factor this Court must take into account in the First Amendment right-of-access balancing test. Moreover, if any of defendants’ accounts of their treatment in government custody constitute new and uncorroborated allegations, their discussion in open court would not require official confirmation of any government program, intelligence method, or interrogation technique. Disclosure in open court would be little or no different from the widespread public disclosure of the leaked report of the International Committee of the Red Cross, detailing interviews with 14 former CIA detainees, including each of the defendants in this case. Int’l Comm. of the Red Cross, *Report on the Treatment of Fourteen “High Value” Detainees in CIA Custody* (Feb. 2007), available at <http://assets.nybooks.com/media/doc/2010/04/22/icrc-report.pdf>. Finally, the government does not contest—nor could it—that the CIA’s detention and interrogation program has now been banned and is prohibited by law, ACLU Mot. 21–24, further undermining its claim that sources and methods the government currently uses to defend against terrorism would be threatened if disclosed.

The fact that the automatic and presumptive 40-second audio delay is not a narrowly tailored restriction on the public’s right of access is clear from the very first hearing in these proceedings, defendants’ May 5, 2012 arraignment. According to the government, the arraignment audio transmission “was briefly suspended for approximately 60 seconds,” but the government later determined that the censored information was not actually classified, and then released a full transcript. Gov’t Resp. 9. Not only does the First Amendment require contemporaneous and timely access,

Lugosch, 435 F.3d at 126–27, but the government’s censorship was a classic prior restraint of speech—the government restricted speech before it was made public—which is “the most serious and the least tolerable infringement on First Amendment rights.” *Neb. Press Ass’n v. Stuart*, 427 U.S. 539, 559 (1976). That the censorship turned out to be unnecessary further demonstrates that presumptive classification, as implemented through the 40-second audio delay, is the complete opposite of the case-by-case determination, based on specific factual findings, that the First Amendment requires before the public’s right of access to judicial proceedings may be suppressed.

Respectfully submitted,



Hina Shamsi
Nathan Freed Wessler
Zachary Katznelson
American Civil Liberties Union
Foundation
125 Broad St., 18th Fl.
New York, NY 10004
Tel.: (212) 549-2500
Fax: (212) 549-2654
hshamsi@aclu.org

Tab 6

**MILITARY COMMISSIONS TRIAL JUDICIARY
GUANTANAMO BAY, CUBA**

UNITED STATES OF AMERICA v. KHALID SHAIKH MOHAMMAD, WALID MUHAMMAD SALIH MUBARAK BIN ATTASH, RAMZI BINALSHIBH, ALI ABDUL AZIZ ALI, MUSTAFA AHMED ADAM AL HAWSAWI	AE013L Government's Supplemental Motion For Modified Order To Protect Against Disclosure of National Security Information 25 September 2012
---	--

1. Timeliness

This Motion is timely filed pursuant to Military Commissions Trial Judiciary Rule of Court 3.7.b.(1).

2. Relief Sought

The Government respectfully requests that the Military Judge issue the proposed modified order to protect national security information from disclosure, attached hereto. *See* 10 U.S.C. § 949p-3; Military Commission Rule of Evidence (M.C.R.E.) 505(e).

3. Overview

Since 26 April 2012, the government has sought an order in this case to establish procedures applicable to all persons who have access to or come into possession of classified documents or information in connection with this case to protect against the unauthorized disclosure of all currently and properly classified information. *See* AE 013. This case involves information that has been properly classified and that the defense has already accessed, in addition to classified discovery that the government expects to provide. The storage, handling and control of classified material, by law or regulation, requires special security precautions, and access to which requires a security clearance and a "need-to-know." Exec. Order No. 13526 §

4.1 (a), 75 Fed. Reg. 707 (Jan. 5, 2010). The government respectfully requests that the attached modified protective order be issued pursuant to statutorily mandated provisions. See 10 U.S.C. § 949p-3; Military Commission Rule of Evidence (M.C.R.E.) 505(e).

4. Burden of proof

As the moving party, the government must demonstrate by a preponderance of the evidence that the requested relief is warranted. R.M.C. 905(c)(1)-(2).

5. Facts

This case alleges a conspiracy between the five accused and al Qaeda, an international terrorist organization which has been and continues to engage in hostilities against the United States. On 31 May 2011 and 25 January 2012, pursuant to the Military Commissions Act of 2009, charges in connection with the 11 September 2001 attacks were sworn against Khalid Shaikh Mohammad (Mohammad), Walid Muhammad Salih Bin Attash (Bin Attash), Ramzi Binalshibh (Binalshibh), Ali Abdul Aziz Ali (Ali), and Mustafa Ahmed Adam al Hawsawi (Hawsawi). These charges were referred jointly to this capital Military Commission on 4 April 2012. The accused are each charged with Conspiracy, Attacking Civilians, Attacking Civilian Objects, Intentionally Causing Serious Bodily Injury, Murder in Violation of the Law of War, Destruction of Property in Violation of the Law of War, Hijacking an Aircraft, and Terrorism.

On 26 April, 2012, the government filed its Motion to Protect Against Disclosure of National Security Information. *See* AE 013. The 26 April 2012 proposed order set forth the storage and handling procedures for classified information, and included in its definition of classified information, material that could be conveyed orally. AE 013, Attachment E, Proposed Order at ¶ 6(d). Specifically, the order sought to reduce the risk of disclosing classified information to those without a “need to know” by requiring the parties to treat the accused statements as classified at the TOP SECRET / SCI level due to their exposure to classified sources and methods, or activities of the United States. AE 013, Attachment E, Proposed Order at ¶ 7(d)(vi). The defense filed a response on 18 May 2012. (AE 013G). The defense objected

to the proposed order, alleging that the order required defense counsel to treat all communications by the accused at the TS/SCI level until and unless they were reviewed by an original classification authority. Currently, there is no protective order in place.

6. Law and Argument

The government has requested the execution of a protective order in this case that would establish procedures for all persons who have access or come into possession of classified documents or information in this case. This protective order is sought pursuant to M.C.R.E. 505(e), which provides that, "Upon motion of the trial counsel, the military judge shall issue an order to protect against the disclosure of any classified information that has been disclosed by the United States to any accused or counsel, regardless of the means by which the accused or counsel obtained the classified information, in any military commission [under the M.C.A.] or that has otherwise been provided to, or obtained by, any such accused in any such military commission." 10 U.S.C. § 949p-3; M.C.R.E. 505(e).

The 26 April 2012 proposed order sets forth the parties obligations with respect to handling classified information, including: 1) defining classified information; 2) explaining the role of the Court Security Officer (CSO); 3) access requirements; 4) the appropriate use, storage, and handling procedures; 5) the procedures for filing documents; 6) notice requirement for use of classified information in proceedings; 7) implementation of security procedures to protect against unauthorized disclosures to individuals without a clearance and a "need to know"; 8) sanctions and criminal penalties available in the event of unauthorized disclosures; 9) the disposition of classified material upon conclusion of the case.

Prior to accessing classified information, an individual must first obtain a security clearance. The obligations of the parties to properly handle classified information set forth in the proposed protective order are based upon the requirements for maintaining such a clearance. Other provisions set forth in the protective order are statutorily mandated for criminal proceedings in which classified information is at issue and in fact are no different than the

provisions found in protective orders issued in Federal court terrorism cases in the early stages of a case to govern the parties obligations with respect to classified information. *See*, Protective Order, *United States v. Warsame*, No. 11 CR 559 (S.D.N.Y. Sept. 9, 2011); Protective Order, *United States v. Ghailani*, No. 98 CR 1023 (S.D.N.Y. Jul. 21, 2009); *United States v. Amawi*, No. 06 CR 719 (N.D.OH. Jul. 17, 2006); *United States v. Moussaoui*, No. 01 CR 455 (E.D.VA. Jan. 22, 2002); *United States v. Bin Laden*, No. 98 CR 1023 (S.D.N.Y. Jul. 29, 1999); Classified Information Procedures Act, 18 U.S.C. App. 3 (CIPA); 10 U.S.C. § 949p-1(d) (making the judicial construction of CIPA authoritative under the M.C.A. where not inconsistent with specific M.C.A. provisions).

The government has a legitimate interest in seeking a protective order at the initiation of a case that will involve classified information to reduce or eliminate the risk that a criminal prosecution will precipitate the unauthorized disclosure of classified information. Indeed, the circumstances precipitating CIPA's enactment make it abundantly clear that it is easier and more effective to prevent the release of classified information in advance than to attempt to undo the damage of unauthorized disclosures after the fact. *See Snapp v. United States*, 444 U.S. 507, 512-13, 62 L. Ed. 2d 704, 100 S. Ct. 763 & nn. 7-8 (1980) (*per curiam*) (noting that unless the Government has adequate mechanisms to prevent unauthorized disclosures, potential sources of classified information may be unwilling to provide such information to the intelligence-gathering [**22] community); *id.* at 514-15 (stating that unauthorized disclosures might cause irreparable harm to the Government and that it may be practically impossible to seek redress against the disclosing party); S. Rep. 96-823 (1980), *reprinted in* 1980 U.S.C.C.A.N. 4294 (referring to a study performed by the Subcommittee on Secrecy and Disclosure of the Senate Intelligence Committee and stating that the study's "key finding . . . was that prosecution of a defendant for disclosing national security information often requires the disclosure in the course of trial of the very information the laws seek to protect"); *see also* Exec. Order No. 12968, 60 *Fed. Reg.* 40,245, at preamble (1995).

The defense in this case all hold the requisite clearance for information that may be provided or that they will have access to during the course of their representation of the accused. In addition, the defense have been provided with classification guidance regarding the classified information that they are likely to encounter during the course of their representation. The defense have noted their objection to requirement in the protective order “that statements made by the Accused, which, due to these individuals’ exposure to classified sources, methods, or activities of the United States, are presumed to contain information classified as TOP SECRET / SCI.” See Attachment E to AE 013, para. 7d. The defense misleadingly construes “presumptive classification” as a separate category of classified information, implying that such information can only be “born” as a result of action by an original classification authority. As explained in the government’s response to AE009, the defense fails to acknowledge that classified information may include material that can be conveyed orally and is not limited to information contained in a document that the government has the ability to physically mark. See, Exec. Order No. 13526 §6.1(t). When granting an individual a security clearance, the government does not provide a waiver for the protection of classified informational that is conveyed in such a fashion. The form of the classified information does not alter its classification, nor is the damage to national security somehow diminished due to an unauthorized disclosure. Accordingly, in a criminal prosecution, the government is entitled to seek an order to protect against the disclosure of classified information, regardless of its form.

In this case, like other cases in which the accused or defendant have had access to classified information, the government has a legitimate national security interest in seeking procedures for the handling and storage of such information that reduces or eliminates the harm to national security that unauthorized disclosures may cause. Accordingly, the government seeks to ensure that the parties handle information that can be conveyed orally according to the appropriate classification levels to which they have been so advised. See, Protective Order, *United States v. Warsame*, No. 11 CR 559 (S.D.N.Y. Sept. 9, 2011); Protective Order, *United States v. Ghailani*, No. 98 CR 1023 (S.D.N.Y. Jul. 21, 2009); *United States v. Amawi*, No. 06 CR

719 (N.D.OH. Jul. 17, 2006); *United States v. Moussaoui*, No. 01 CR 455 (E.D.VA. Jan. 22, 2002); *United States v. Bin Laden*, No. 98 CR 1023 (S.D.N.Y. Jul. 29, 1999).

Contrary to the defense assertions, it is the sole responsibility of an original classification authority, not the defense, to classify or declassify information. As articulated in the government's 26 April 2012 submission, the accused have been exposed to classified information at the TS/SCI level. Although they are not prohibited from discussing that information with their defense counsel, and although there are some statements by the accused that contain nothing even potentially classified (i.e., "Thank you for coming to speak with me today.") the government has the right to seek protective measures to ensure that defense counsel, who are authorized to have access to the classified information known to their clients, will treat such information in the appropriate manner. Because the government has no interest in monitoring the privileged communications between the accused and their defense to properly determine the classification level of any notes taken during the meeting, the proposed mechanism in the 26 April 2012 protective order required the parties to treat all statements of the accused at the highest level of classification to which the accused had previously been exposed. *See, e.g., Al Odah v. United States*, 346 F.Supp. 2d 1, 8-14 (D.D.C. 2004) (court determined that the government's national security concerns were legitimate and, therefore, the defense was required to have a security clearance and to treat all information obtained during the course of their representation as classified until a classification review was conducted).

The 26 April 2012 order did not however, restrict the accused in any way from communicating with their counsel about any topic. It simply requested that the defense counsel handle and store such privileged communications as classified until and unless they requested a classification review. Nor did the protective order restrict the ability of the defense to use the statements in litigation. The order directed the defense to comply with the statutorily mandated procedures for using classified information, contained in M.C.R.E 505 and modeled after CIPA.

Without conceding that the proposed order placed unduly burdensome restrictions upon defense counsel but nevertheless seeking to provide convenient handling and storage options

consistent with the protection of national security information, the government hereby proposes that the protective order it moved the commission to sign on 26 April 2012 be amended. The modified order provides that with respect to information obtained from their clients, defense counsel treat and handle as classified only information that that they know or have a reason to know is classified, including information that relates to specific aspects of the CIA RDI program that remain classified. While the 26 April 2012 proposed order featured legitimate protections for handling classified information, the order, as modified, seeks to alleviate defense concerns that uncertainty may be causing them to unnecessarily treat orally conveyed information as classified when it is clearly unrelated to the classified sources, methods and activities of the United States that the accused have been previously exposed. The modified order will require that defense counsel scrupulously adhere to the classification guidance previously provided as a condition of their read-in to special access programs in determining how to treat information that has been orally conveyed to them by the accused. The government has not modified any other provisions of the 26 April 2012 order.

7. Conclusion

The Government respectfully requests that the Military Judge issue the modified protective order to establish procedures applicable to all persons who have access to or come into possession of classified documents or information in connection with this case to protect against the unauthorized disclosure of all currently and properly classified information.

8. Oral Argument

The government is willing to waive oral argument but requests an opportunity to be heard should the defense request oral argument.

9. Witnesses and Evidence

None

10. Certificate of Conference

The defense objects to the entry of the government's modified order.

CERTIFICATE OF SERVICE

I certify that on the 25th day of September 2012, I filed AE013L, the **Government's Supplemental Motion for Modified Order To Protect Against Disclosure of National Security Information** with the Office of Military Commissions Trial Judiciary and I served a copy on counsel of record.

//s//

Joanna Baltes
Deputy Trial Counsel
Office of the Chief Prosecutor
Office of Military Commissions

**MILITARY COMMISSIONS TRIAL JUDICIARY
GUANTANAMO BAY, CUBA**

<p>UNITED STATES OF AMERICA</p> <p>v.</p> <p>KHALID SHAIKH MOHAMMAD, WALID MUHAMMAD SALIH MUBARAK BIN ATTASH, RAMZI BINALSHIBH, ALI ABDUL AZIZ ALI, MUSTAFA AHMED ADAM AL HAWSAWI</p>	<p>PROTECTIVE ORDER #1</p> <p>To Protect Against Disclosure of National Security Information</p> <p>_____ 2012</p>
--	---

Upon consideration of the submissions regarding the Government's motion for a protective order to protect classified information in this case, the Commission finds that this case involves classified national security information, including TOP SECRET / SENSITIVE COMPARTMENTED INFORMATION (SCI), the disclosure of which would be detrimental to national security, the storage, handling, and control of which requires special security precautions, and access to which requires a security clearance and a need-to-know. Accordingly, pursuant to authority granted under 10 U.S.C. §§ 949p-1 to 949p-7, Rules for Military Commissions (R.M.C.) 701 and 806, Military Commission Rule of Evidence (M.C.R.E.) 505, Regulation for Trial by Military Commissions (R.T.M.C.) ¶ 17-3, and the general supervisory authority of the Commission, in order to protect the national security, and for good cause shown, the following Protective Order is entered.

I. SCOPE

1. This Protective Order establishes procedures applicable to all persons who have access to or come into possession of classified documents or information in connection with this case,

regardless of the means by which the persons obtained the classified information. These procedures apply to all aspects of pretrial, trial, and post-trial stages in this case, including any appeals, subject to modification by further order of the Commission.

2. This Protective Order applies to all information, documents, testimony, and material associated with this case that contain classified information, including but not limited to any classified pleadings, written discovery, expert reports, transcripts, notes, summaries, or any other material that contains, describes, or reflects classified information.

3. Counsel are responsible for advising their clients, translators, witnesses, experts, consultants, support staff, and all others involved with the defense or prosecution of this case, respectively, of the contents of this Protective Order.

II. DEFINITIONS

4. As used in this Protective Order, the term “Defense” includes any counsel for the Accused in this case and any employees, contractors, investigators, paralegals, experts, translators, support staff or other persons working on the behalf of the Accused or his counsel in this case.

5. The term “Government” includes any counsel for the United States in this case and any employees, contractors, investigators, paralegals, experts, translators, support staff or other persons working on the behalf of the United States or its counsel in this case.

6. The words “documents” and “information” include, but are not limited to, all written or printed matter of any kind, formal or informal, including originals, conforming copies and non-conforming copies, whether different from the original by reason of notation made on such copies or otherwise, and further include, but are not limited to:

UNCLASSIFIED//FOR PUBLIC RELEASE

a. papers, correspondence, memoranda, notes, letters, cables, reports, summaries, photographs, maps, charts, graphs, inter-office and intra-office communications, notations of any sort concerning conversations, meetings, or other communications, bulletins, teletypes, telegrams, facsimiles, invoices, worksheets, and drafts, alterations, modifications, changes, and amendments of any kind to the foregoing;

b. graphic or oral records or representations of any kind, including, but not limited to: photographs, charts, graphs, microfiche, microfilm, videotapes, and sound or motion picture recordings of any kind;

c. electronic, mechanical, or electric records of any kind, including, but not limited to: tapes, cassettes, disks, recordings, electronic mail, instant messages, films, typewriter ribbons, word processing or other computer tapes, disks or portable storage devices, and all manner of electronic data processing storage; and

d. information acquired orally.

7. The terms “classified national security information and/or documents,” “classified information,” and “classified documents” include:

a. any classified document or information that was classified by any Executive Branch agency in the interests of national security or pursuant to Executive Order, including Executive Order 13526, as amended, or its predecessor Orders, as “CONFIDENTIAL,” “SECRET,” “TOP SECRET,” or additionally controlled as “SENSITIVE COMPARTMENTED INFORMATION (SCI)” and specifically designated by the United States for limited or restricted dissemination or distribution;

b. any document or information, regardless of its physical form or characteristics, now or formerly in the possession of a private party that was derived from United States

UNCLASSIFIED//FOR PUBLIC RELEASE

Government information that was classified, regardless of whether such document or information has subsequently been classified by the Government pursuant to Executive Order, including Executive Order 13526, as amended, or its predecessor Orders, as “CONFIDENTIAL,” “SECRET,” “TOP SECRET,” or additionally controlled as “SENSITIVE COMPARTMENTED INFORMATION (SCI)”;

c. verbal or non-documentary classified information known to the Accused or the Defense;

d. any document or information as to which the Defense has been notified orally or in writing that such document or information contains classified information, including, but not limited to the following:

(i) Information that would reveal or tend to reveal details surrounding the capture of the Accused other than the location and date;

(ii) Information that would reveal or tend to reveal the foreign countries in which: Khalid Shaikh Mohammad (Mohammad) and Mustafa Ahmed Adam al Hawsawi (Hawsawi) were detained from the time of their capture on or about 1 March 2003 through 6 September 2006; Walid Muhammad Salih Bin Attash (Bin Attash) and Ali Abdul Aziz Ali (Ali) were detained from the time of their capture on or about 29 April 2003 through 6 September 2006; and Ramzi Binalshibh (Binalshibh) was detained from the time of his capture on or around 11 September 2002 through 6 September 2006.

(iii) The names, identities, and physical descriptions of any persons involved with the capture, transfer, detention, or interrogation of the Accused or specific dates regarding the same, from on or around the aforementioned capture dates through 6 September 2006;

(iv) The enhanced interrogation techniques that were applied to the Accused from on or around the aforementioned capture dates through 6 September 2006, including descriptions of the techniques as applied, the duration, frequency, sequencing, and limitations of those techniques; and

(v) Descriptions of the conditions of confinement of the Accused from on or around the aforementioned capture dates through 6 September 2006;

e. In addition, the term “information” shall include without limitation observations and experiences of the Accused with respect to the matters set forth in subparagraphs 7(d)(i)-(v), above.

f. any document or information obtained from or related to a foreign government or dealing with matters of U.S. foreign policy, intelligence, or military operations, which is known to be closely held and potentially damaging to the national security of the United States or its allies.

8. “National Security” means the national defense and foreign relations of the United States.

9. “Access to classified information” means having authorized access to review, read, learn, or otherwise come to know classified information.

10. “Secure area” means a physical facility accredited or approved for the storage, handling, and control of classified information.

11. “Unauthorized disclosure of classified information” means any knowing, willful, or negligent action that could reasonably be expected to result in a communication or physical transfer of classified information to an unauthorized recipient. Confirming or denying information, including its very existence, constitutes disclosing that information.

III. COMMISSION SECURITY OFFICER

12. A Commission Security Officer (CSO) has been appointed by the Commission for the purpose of providing security arrangements necessary to protect against unauthorized disclosure of any classified documents or information in connection with this case. The CSO is authorized to appoint Alternate Commission Security Officers (ACSOs) as necessary. All references to the CSO herein shall be deemed to refer also to any ACSOs appointed to this case.

13. The parties shall seek guidance from the CSO with regard to the appropriate storage, handling, and use of classified information. The CSO shall consult with the original classification authority (OCA) of classified documents or information, as necessary, to address classification decisions or other related issues.

14. The CSO shall not reveal to any person, including the Government, the content of any conversations the CSO hears by or among the Defense, nor reveal the nature of documents being reviewed by the Defense or the work generated by the Defense, except as necessary to report violations of this Protective Order to the Commission after appropriate consultation with the Defense or to carry out duties pursuant to this Protective Order. Additionally, the presence of the CSO shall not operate as a waiver of any applicable privilege under the Military Commissions Act, 10 U.S.C. § 948a, *et seq.* (M.C.A.), R.M.C., or M.C.R.E.

IV. ACCESS TO CLASSIFIED INFORMATION

15. Without authorization from the Government, no member of the Defense, including defense witnesses, shall have access to classified information in connection with this case unless that person has:

UNCLASSIFIED//FOR PUBLIC RELEASE

- a. received the necessary security clearance from the appropriate Department of Defense (DoD) authorities and signed an appropriate non-disclosure agreement, as verified by the CSO;
- b. signed the Memorandum of Understanding Regarding Receipt of Classified Information (MOU), attached to this Protective Order, agreeing to comply with the terms of this Protective Order; and
- c. a need-to-know the classified information at issue, as determined by the OCA of that information.

16. In order to be provided access to classified information in connection with this case, each member of the Defense shall execute the attached MOU, file the executed originals of the MOU with the Commission, and submit copies to the CSO and counsel for the Government. The execution and submission of the MOU is a condition precedent to the Defense having access to classified information for the purposes of these proceedings.

17. The substitution, departure, or removal of any member of the Defense, including defense witnesses, from this case for any reason shall not release that person from the provisions of this Protective Order or the MOU executed in connection with this Protective Order.

18. Once the CSO verifies that counsel for the Accused have executed and submitted the MOU, and are otherwise authorized to receive classified information in connection with this case, the Government may provide classified discovery to the Defense, either directly or via the CSO, who will assist as necessary in ensuring the material is delivered to the Defense.

19. All classified documents or information provided or obtained in connection with this case remain classified at the level designated by the OCA, unless the documents bear a clear indication that they have been declassified. The person receiving the classified documents or

information, together with all other members of the Defense or the Government, respectively, shall be responsible for protecting the classified information from disclosure and shall ensure that access to and storage of the classified information is in accordance with applicable laws and regulations and the terms of this Protective Order.

20. No member of the Defense, including any defense witness, is authorized to disclose any classified information obtained during this case, outside the immediate parameters of these military commission proceedings. If any member of the Defense, the Accused, or any defense witness receives any summons, subpoena, or court order, or the equivalent thereof, from any United States or foreign court or on behalf of any criminal or civil investigative entity within the United States or from any foreign entity, the Defense, including defense witnesses, shall immediately notify the Commission, the CSO, and the Government so that appropriate consideration can be given to the matter by the Commission and the OCA of the materials concerned. Absent authority from the Commission or the Government, the Defense, the Accused, and defense witnesses are not authorized to disseminate or disclose classified materials in response to such requests. The Defense, the Accused, and defense witnesses and experts are not authorized to use or refer to any classified information obtained as a result of their participation in commission proceedings in any other forum, or in a military commission proceeding involving another detainee.

V. USE, STORAGE, AND HANDLING PROCEDURES

21. The Office of the Chief Defense Counsel, Office of Military Commissions, has approved secure areas in which the Defense may use, store, handle, and otherwise work with classified information. The CSO shall ensure that such secure areas are maintained and operated in a

UNCLASSIFIED//FOR PUBLIC RELEASE

manner consistent with this Protective Order and as otherwise reasonably necessary to protect against the disclosure of classified information.

22. All classified information provided to the Defense, and otherwise possessed or maintained by the Defense, shall be stored, maintained, and used only in secure areas. Classified information may only be removed from secure areas in accordance with this Protective Order and applicable laws and regulations governing the handling and use of classified information.

23. Consistent with other provisions of this Protective Order, the Defense shall have access to the classified information made available to them and shall be allowed to take notes and prepare documents with respect to such classified information in secure areas.

24. The Defense shall not copy or reproduce any classified information in any form, except in secure areas and in accordance with this Protective Order and applicable laws and regulations governing the reproduction of classified information.

25. All documents prepared by the Defense that are known or believed to contain classified information—including, without limitation, notes taken or memoranda prepared by counsel and pleadings or other documents intended for filing with the Commission—shall be transcribed, recorded, typed, duplicated, copied, or otherwise prepared only by persons possessing an appropriate approval for access to such classified information. Such activities shall take place in secure areas, on approved word processing equipment, and in accordance with procedures approved by the CSO. All such documents and any associated materials containing classified information—such as notes, memoranda, drafts, copies, typewriter ribbons, magnetic recordings, and exhibits—shall be maintained in secure areas unless and until the CSO advises that those documents or associated materials are unclassified in their entirety. None of these materials shall

be disclosed to the Government unless authorized by the Commission, by counsel for the Accused, or as otherwise provided in this Protective Order.

26. The Defense may discuss classified information only within secure areas and shall not discuss, disclose, or disseminate classified information over any non-secure communication system, such as standard commercial telephones, office intercommunication systems, or non-secure electronic mail.

27. The Defense shall not disclose any classified documents or information to any person, including counsel in related cases of Guantanamo Bay detainees in military commissions or other courts (including, but not limited to, habeas proceedings), except those persons authorized by this Protective Order, the Commission, and counsel for the Government with the appropriate clearances and the need-to-know that information.

28. To the extent that the Defense is not certain of the classification of information it wishes to disclose, the Defense shall consult with the CSO for a determination as to its classification. In any instance in which there is any doubt as to whether information is classified, the Defense must consider the information classified unless and until it receives notice from the CSO that such information is not classified.

29. Until further order of this Commission, the Defense shall not disclose to the Accused any classified information not previously provided by the Accused to the Defense, except where such information has been approved for release to the Accused and marked accordingly.

30. Except as otherwise stated in this paragraph, and to ensure the national security of the United States, at no time, including any period subsequent to the conclusion of these proceedings, shall the Defense make any public or private statements disclosing any classified information accessed pursuant to this Protective Order, or otherwise obtained in connection with

this case, including the fact that any such information or documents are classified. In the event classified information enters the public domain without first being properly declassified by the United States Government, counsel are reminded that they may not make public or private statements about the information if the information is classified. (See paragraph 7 of this Protective Order for specific examples of information which remains classified even if it is in the public domain.) In an abundance of caution and to help ensure clarity on this matter, the Commission emphasizes that counsel shall not be the source of any classified information entering the public domain, nor should counsel comment on information which has entered the public domain but which remains classified.

VI. PROCEDURES FOR FILING DOCUMENTS

31. Any pleading or other document filed with the Commission in this case, which counsel know, reasonably should know, or are uncertain of whether the filing contains classified information, shall be filed under seal in accordance with the provisions of the M.C.A., R.M.C., M.C.R.E., R.T.M.C., and the Military Commissions Trial Judiciary Rules of Court applicable to filing classified documents or information. Documents containing classified information that is not at the TS/CODEWORD level shall be filed pursuant to the procedures specified for classified information contained in the Trial Judiciary Rules of Court 3(10)(d) to the extent that the material can be transmitted via the Secret Internet Protocol Router Network (SIPR). Information that is classified at the TS/CODEWORD level, including presumptively classified statements of the Accused that have not yet been determined to be unclassified by the appropriate Government agency, cannot be transmitted via SIPR and must be provided in hard copy to the Chief Clerk of the Trial Judiciary.

32. Classified filings must be marked with the appropriate classification markings on each page, including classification markings for each paragraph. If a party is uncertain as to the appropriate classification markings for a document, the party shall seek guidance from the CSO, who will consult with the OCA of the information or other appropriate agency, as necessary, regarding the appropriate classification.

33. When filing classified documents or information under seal, the parties shall file the papers containing classified information with the Military Commissions Trial Judiciary Staff (“Judiciary Staff”) and provide notice of the classified filing to the other party. Once a filing is properly filed, the CSO for the Judiciary Staff shall promptly review the filing, and in consultation with the appropriate Government agencies, determine whether the filing contains classified information and is marked appropriately. The Judiciary Staff shall then ensure the classified filing is promptly served on the other party (unless filed *ex parte*) and reflected in the filings inventory with an unclassified entry noting that it was filed under seal.

34. The CSO and Judiciary Staff shall ensure any classified information contained in such filings is maintained under seal and stored in an appropriate secure area consistent with the highest level of classified information contained in the filing. All portions of any filed papers that do not contain classified information will be unsealed (unless filed *in camera* or *ex parte*) for inclusion in the public record.

35. Under no circumstances may classified information be filed in an unsealed filing. In the event a party believes that an unsealed filing contains classified information, the party shall immediately notify the CSO and Judiciary Staff, who shall take appropriate action to retrieve the documents or information at issue. The filing will then be treated as containing classified information unless and until the CSO determines otherwise. Nothing herein limits the

Government's authority to take other remedial action as necessary to ensure the protection of the classified information.

36. Nothing herein requires the Government to disclose classified information. Additionally, nothing herein prevents the Government from submitting classified information to the Commission *in camera* or *ex parte* in these proceedings or entitles the Defense access to such submissions or information. Except for good cause shown in the filing, the Government shall provide the Defense with notice on the date of the filing.

VII. PROCEDURES FOR MILITARY COMMISSION PROCEEDINGS

37. Except as provided herein, and in accordance with M.C.R.E. 505, no party shall disclose or cause to be disclosed any information known or believed to be classified in connection with any hearing or proceeding in this case.

A. Notice Requirements

38. The parties must comply with all notice requirements under M.C.R.E. 505 prior to disclosing or introducing any classified information in this case.

39. Because all statements of the Accused are presumed to contain information classified as TOP SECRET / SCI, the Defense must provide notice in accordance with this Protective Order and M.C.R.E. 505(g) if the Accused intends to make statements or offer testimony at any proceeding.

B. Closed Proceedings

40. While proceedings shall generally be publicly held, the Commission may exclude the public from any proceeding, *sua sponte* or upon motion by either party, in order to protect information the disclosure of which could reasonably be expected to damage national security. If the Commission closes the courtroom during any proceeding in order to protect classified

information from disclosure, no person may remain who is not authorized to access classified information in accordance with this Protective Order, which the CSO shall verify prior to the proceeding.

41. No participant in any proceeding, including the Government, Defense, Accused, witnesses, and courtroom personnel, may disclose classified information, or any information that tends to reveal classified information, to any person not authorized to access such classified information in connection with this case.

C. Delayed Broadcast of Open Proceedings

42. Due to the nature and classification level of the classified information in this case, including the classification of the Accused's statements, the Commission finds that to protect against the unauthorized disclosure of classified information during proceedings open to the public, it will be necessary to employ a forty-second delay in the broadcast of the proceedings from the courtroom to the public gallery. Should classified information be disclosed during any open proceeding, this delay will allow the Military Judge, CSO, or Government to take action to suspend the broadcast—including any broadcast of the proceedings to locations other than the public gallery of the courtroom (e.g., any closed-circuit broadcast of the proceedings to a remote location)—so that the classified information will not be disclosed to members of the public.

43. The broadcast may be suspended whenever it is reasonably believed that any person in the courtroom has made or is about to make a statement or offer testimony disclosing classified information.

44. The Commission shall be notified immediately if the broadcast is suspended. In that event, and otherwise if necessary, the Commission may stop the proceedings to evaluate whether the information disclosed, or about to be disclosed, is classified information as defined in this

Protective Order. The Commission may also conduct an *in camera* hearing to address any such disclosure of classified information.

D. Other Protections

45. During the examination of any witness, the Government may object to any question or line of inquiry that may require the witness to disclose classified information not found previously to be admissible by the Commission. Following such an objection, the Commission will determine whether the witness's response is admissible and, if so, may take steps as necessary to protect against the public disclosure of any classified information contained therein.

46. Classified information offered or admitted into evidence will remain classified at the level designated by the OCA and will be handled accordingly. All classified evidence offered or accepted during trial will be kept under seal, even if such evidence was inadvertently disclosed during a proceeding. Exhibits containing classified information may also be sealed after trial as necessary to prevent disclosure of such classified information.

E. Transcripts

47. Transcripts of all proceedings shall be redacted as necessary to prevent public disclosure of classified information. The Clerk of the Military Commission, in conjunction with the CSO, shall ensure the transcripts of all proceedings are reviewed and redacted as necessary to protect any classified information from public disclosure. An unclassified transcript of each proceeding shall be made available for public release.

48. The Clerk of the Military Commission, in conjunction with the CSO, shall ensure that transcripts containing classified information remain under seal and are properly segregated from the unclassified portion of the transcripts, properly marked with the appropriate security markings, stored in a secure area, and handled in accordance with this Protective Order.

VIII. UNAUTHORIZED DISCLOSURE

49. Any unauthorized disclosure of classified information may constitute a violation of United States criminal laws. Additionally, any violation of the terms of this Protective Order shall immediately be brought to the attention of the Commission and may result in disciplinary action or other sanctions, including a charge of contempt of the Commission and possible referral for criminal prosecution. Any breach of this Protective Order may also result in the termination of access to classified information. Persons subject to this Protective Order are advised that unauthorized disclosure, retention, or negligent handling of classified documents or information could cause damage to the national security of the United States or may be used to the advantage of an adversary of the United States or against the interests of the United States. The purpose of this Protective Order is to ensure that those authorized to receive classified information in connection with this case will never divulge that information to anyone not authorized to receive it, without prior written authorization from the OCA and in conformity with this Order.

50. The Defense shall promptly notify the CSO upon becoming aware of any unauthorized access to or loss, theft, or other disclosure of classified information, and shall take all reasonably necessary steps to retrieve such classified information and protect it from further unauthorized disclosure or dissemination. The CSO shall notify the Government of any unauthorized disclosures of classified information so that the Government may take additional remedial measures as necessary to prevent further unauthorized access or dissemination.

IX. DISPOSITION OF CLASSIFIED INFORMATION

51. All classified documents and information to which the Defense has access in this case are the property of the United States. Upon demand of the CSO or the Government, the Defense

shall return any documents containing classified information in its possession which were obtained in discovery from the Government, or for which the Defense is responsible because of its access to classified information in connection with this case.

52. Unless otherwise ordered or agreed, within sixty days after the final termination of this action, including any appeals, the Defense shall, at its option, return or properly destroy all classified information in its possession in connection with this case, including all notes, abstracts, compilations, summaries, or any other form or reproduction of classified information. The Defense is responsible for reminding any expert witnesses, non-testifying consultants, and all other persons working with the Defense of its obligation to return or destroy classified information related to this case. The Defense shall submit written certification to the CSO and the Government by the sixty-day deadline confirming that all classified information has been returned or destroyed as set forth in this Protective Order.

X. SURVIVAL OF ORDER

53. The terms of this Protective Order and any signed MOU shall survive and remain in effect after the termination of this case.

54. This Protective Order is entered without prejudice to the right of the parties to seek such additional protections, or exceptions to those stated herein, as they deem necessary.

SO ORDERED:

DATED: _____

JAMES L. POHL
COL, JA, USA
Military Judge

Tab 7

MILITARY COMMISSIONS TRIAL JUDICIARY
GUANTANAMO BAY, CUBA

UNITED STATES OF AMERICA

v.

KHALID SHAIKH MOHAMMAD,
WALID MUHAMMAD SALIH MUBARAK
BIN 'ATTASH,
RAMZI BINALSHIBH,
ALI ABDUL AZIZ ALI ,
MUSTAFA AHMED ADAM AL-HAWSAWI

**Response of the
American Civil Liberties Union**
to Government's Supplemental Motion
for Modified Order to Protect Against
Disclosure of National Security
Information

October 12, 2012

1. Timeliness. This application is timely filed under the Military Commissions Trial Judiciary Rules of Court ("RC") and the 2011 Regulation for Trial by Military Commission ("Regulation").¹

2. Overview and Relief Sought. In case there were any doubt, the government's modified proposed Protective Order for these proceedings makes clear that the government is asking the military judge to impose a censorship regime that would prevent the public from hearing any statements by defendants about their memories, "observations[,] and experiences" of their torture and detention in U.S. custody. *See* AE 013L ("Supplemental Motion for Modified Order to Protect Against Disclosure of National Security Information") (Sept. 25, 2012) and "Protective Order #1," Attachment to AE 13L ("Mod. Prop. P.O. #1"), §§ I(7)(e) and I(7)(d)(i)-(v).

¹ RC 3.7(c)(1) provides that, generally, "a response is due within 14 calendar days after a motion is filed . . ." Although the government's supplemental motion was filed on September 25, 2012, it was not made available to the public and the ACLU until October 4, 2012. The ACLU's Response is being timely filed within 14 days of the supplemental motion becoming public. *See also* AE 083 (ACLU motion seeking timely access to sealed filings related to the public's right of access to commission proceedings in order to receive notice and an opportunity to be heard).

UNCLASSIFIED//FOR PUBLIC RELEASE

The government's modified proposed Protective Order fails to meet the First Amendment's strict scrutiny standard and the public access requirements of the Military Commissions Act ("MCA"), Pub. L. No. 109-336, 120 Stat. 2600 (2006) (codified as amended 10 U.S.C. §§ 949–950 (2009)), for the same reasons that the original proposed Protective Order failed to meet that standard: The government has no compelling interest in keeping from the public defendants' testimony about their own knowledge of illegal government conduct when the interrogation, rendition, and detention program is illegal, has been banned by the U.S. President, and cannot be used in the future; copious details about the program and how it was applied to defendants are widely known; and the government purposefully and coercively disclosed its purportedly secret program to defendants by subjecting them to it. The government's proposed categorical restriction on the public's right to hear this testimony by imposing a 40-second broadcast delay of the proceedings also fails as an alternative to closure under First Amendment scrutiny, because it is not narrowly tailored. *See also* AE 013A ("Motion of the American Civil Liberties Union for Public Access to Proceedings and Records" ("ACLU Mot.)) (May 3, 2012); AE 013H ("Reply of the American Civil Liberties Union to the Government's Response to the Motion for Public Access to Proceedings and Records" ("ACLU Reply")) (May 24, 2012).

For these reasons and those set forth in the ACLU's previous filings, the ACLU respectfully requests that the military judge (1) deny the government's motion to enter Protective Order #1 as proposed; (2) revise the modified Protective Order to strike subsection I(7)(e) and provide that Section I(7) does not apply to defendants' personal knowledge, observations, and experiences of their interrogation, detention and treatment

in U.S. custody; (3) strike section VII(C) of the modified protective order, requiring delayed broadcast of the commission proceedings, as unjustified; and (4) in the event that the commission grants the government's request for a 40-second delay, order the public release of unredacted transcripts containing the defendants' statements on an expedited basis to minimize the infringement on the public's right of contemporaneous access to the proceedings.

3. Statement of Facts

(a) **AE 013.** On April 26, 2012, the government filed a "Motion to Protect Against Disclosure of National Security Information" and an accompanying proposed protective order. *See* AE 013 (Apr. 26, 2012); "[Proposed] Protective Order #1" ("Orig. Prop. P.O. #1"), Attachment to AE 013 (Apr. 26, 2012). The ACLU opposed the government's motion, seeking to secure public access to these proceedings as required by the Constitution and the MCA. *See* AE 013A (ACLU Mot.) (May 3, 2012); AE 013H (ACLU Reply) (May 24, 2012). Counsel for Mr. al-Baluchi also filed a response to the government's motion, a filing that remains under seal, *see* AE 013G (May 18, 2012), as did a group of fourteen media organizations, *see* AE 013F (May 16, 2012). On August 24, 2012, this commission issued an Amended Docketing Order setting the government's motion for argument during the next Commission session, beginning October 15, 2012. *See* AE 05F (Aug. 24, 2012). On September 25, 2012, the government filed a supplemental motion modifying its original application for a protective order—the subject of this Response. *See* AE 013L (Sept. 25, 2012).

(b) **AE 083.** On October 3, 2012, the ACLU filed a motion seeking access to sealed commission filings relevant to its pending public-access challenge.² *See* AE 083 (Oct. 3, 2012).

4. Legal Basis for the Relief Requested.

The ACLU's previous filings in this case discuss in detail why the public has a First Amendment right to these military commission proceedings. *See generally* ACLU Mot.; ACLU Reply. The government does not address the public's First Amendment right of access in any of its filings, including 13L, but nor does it contest the ACLU's arguments (and evidence) that the public does indeed possess that right of access. ACLU Mot. at 6–10; Decl. of David Glazer, Attachment to ACLU Mot. Indeed, it would be extraordinary for the American government to take the position that the American public does not have a constitutional right of access to the most important terrorism prosecution of our time. *See* ACLU Mot. at 7–10 (demonstrating that the public's constitutional right of access applies in civilian and military proceedings). The government has not taken that position, and there should be no question that the public's constitutional right of access attaches to these commission proceedings.

Once the public's right of access attaches, as it does here, it may only be overcome if the government meets its high burden of showing, and if the military judge finds, both that there is a compelling interest justifying closure and that closure is narrowly tailored. *See, e.g.,* ACLU Reply at 9. The government's modified proposed protective order, like its original one, fails this constitutional test.

² On October 1, 2012, a group of fourteen news organizations filed a separate but similar motion seeking press and public access to sealed commission filings. *See* AE 081 (Oct. 1, 2012). Like the ACLU, these organizations will argue before the commission during the October 15–19, 2012 session.

UNCLASSIFIED//FOR PUBLIC RELEASE

According to the government, the modified proposed protective order allows “defense counsel [to] treat and handle as classified only information that they know or have a reason to know is classified.” AE 013L at 7. In the government’s view, the modification operates to ease burdens on defense counsel related to their communications with their clients in the course of representation. This modification does nothing, however, to address the core problem with the government’s proposed censorship regime, which still improperly seeks to suppress, as both classified and protected, defendants’ statements about their own knowledge of their abuse and detention in U.S. custody.

Indeed, other changes make pellucidly clear that the modified protective order untenably infringes on the public’s First Amendment right of access to these proceedings. The modified protective order specifically adds to the definition of “classified information” the “observations and experiences of the Accused with respect to matters set forth in subparagraphs 7(d)(i)–(v) above.” Mod. Prop. P.O. #1 § I(7)(e).³ The specifically-referenced subparagraphs include such “matters” as the “enhanced interrogation techniques that were applied to the Accused . . . , including descriptions of the techniques as applied, the duration, frequency, sequencing, and limitations of those techniques,” *id.* § I(7)(d)(iv), and “[d]escriptions of the conditions of confinement of the Accused . . . ,” *id.* § I(7)(d)(v). Thus, the modified protective order seeks to do through subsection I(7)(e) what the original proposed order did through subsection I(7)(d)(vi): categorically suppress *ex ante*, and prevent the public from hearing, the memories,

³ To the extent that the military judge reads the MCA as barring this commission from independently determining the propriety of the government’s decision to classify and suppress the defendants’ personal knowledge of their detention and treatment, the commission should either (1) read the MCA to authorize the withholding from the public of only *properly* classified information, which the defendants’ personal knowledge is not; (2) read the MCA to apply only to evidence presented by the government, in line with the MCA’s plain text; or (3) find the relevant provisions of the MCA unconstitutional as applied. *See* ACLU Mot. at 13–17.

thoughts, and experiences of the defendants about their illegal torture and detention at the hands of the U.S. government.

None of the justifications the government has offered for this censorship regime survive strict scrutiny. As the ACLU has previously shown, the government has no legitimate interest in censoring defendants' personal accounts of the CIA's rendition, detention, and interrogation program when that program was illegal and has been terminated by the President of the United States. *See* ACLU Mot. at 21–24; ACLU Reply at 7–8. Moreover, the government's own disclosures, as well as countless reports by the press, international organizations, and foreign governments, have already made widely public the very information the government seeks to suppress. *See* ACLU Mot. at 24–31; ACLU Reply at 10–11.

Nor can the government prevent the public from hearing defendants' statements based on their personal knowledge by claiming that the information is classified. As an initial matter, classification—whether proper or not—does not in itself determine the First Amendment question of whether the government has met the compelling interest requirement. *See* ACLU Mot. at 19–21; ACLU Reply at 4–9. Here, that requirement is not met for the reasons set forth above, and because Executive Order 13,526, which governs classification, simply does not extend to third parties who are not in a relationship of privity and trust with the government. *See* ACLU Mot. at 17–18; *see also* AE 013 at 13 (“[T]he Accused clearly fall into the category of persons ‘not authorized to received’ classified information.”). Thus, even if information about the CIA's rendition, detention, and interrogation program were otherwise properly classified, the government itself purposefully disclosed that information to defendants—who the government admits

UNCLASSIFIED//FOR PUBLIC RELEASE

are not authorized to receive classified information—by forcibly subjecting them to the program; it cannot now prevent the public from hearing defendants’ testimony. *See* ACLU Mot. at 19–21; ACLU Reply at 6.

This commission should not and cannot judicially bless the government’s proposed censorship regime.

Respectfully submitted,



Hina Shamsi
Brett Max Kaufman
Zachary Katznelson
AMERICAN CIVIL LIBERTIES UNION &
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
125 Broad Street—18th Floor
New York, NY 10004
Tel.: 212.549.2500
Fax: 212.549.2654
Email: hshamsi@aclu.org

Tab 8

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 To make sure, we're done with 9, though.

2 Ms. Baltes, on 13.

3 ATC [MS. BALTES]: Good morning, Your Honor.

4 MJ [COL POHL]: Good morning.

5 ATC [MS. BALTES]: This is the government's motion so I
6 do want to actually get to the protective order, but I would
7 like to respond to some of the argument that we heard from
8 Mr. Schulz yesterday and from Ms. Shamsi yesterday and today.

9 I heard the statement from Ms. Shamsi that no
10 other court has ever ruled or allowed a protective order with
11 the provisions that the ACLU is currently challenging. I want
12 to be clear, and Ms. Shamsi apparently had a copy of the
13 Ghailani order; maybe they don't understand how the protective
14 order worked in that case, but paragraph 2 in Ghailani
15 specifically states that it applies to all stages of the
16 proceeding. It is the standard protective order that the
17 government seeks in federal terrorism cases. That protective
18 order was issued on July 21, 2009, by Judge Kaplan in the
19 Southern District of New York.

20 MJ [COL POHL]: Ms. Baltes, do you see, just to make
21 sure, that this protective order applies to all stages but
22 there's a different, for want of a better term, a different
23 procedure about what's admitted at trial?

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 ATC [MS. BALTES]: Absolutely. The protective order
2 doesn't -- I'll get there. People always say that but I'm
3 going to answer now.

4 The protective order does not say that just
5 because there's definitions in paragraph 7 about what's
6 classified that there's an automatic closure. If that was the
7 case it would have been a shorter order. It would have been
8 paragraph 7, this is the definition of classified, therefore
9 closure will occur. That is absolutely not what the
10 protective order says.

11 The protective order goes through the different
12 stages of the proceedings, of how proceedings will happen.
13 There's obviously the discovery phase, access to classified
14 information; there's the explanation of what a court security
15 officer does; there's an explanation of how the parties file
16 documents that may contain classified information; then
17 there's the part of the protective order that explains if the
18 defense wants to disclose classified information, that would
19 be the 505(g) process. In federal court, it is the Section 5
20 notice.

21 Then the protective order goes through what
22 happens in an actual hearing, what happens for disclosure.
23 That's what it does. There is no, again, automatic closure,

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 and that's certainly not what the government's advocating.

2 In fact, the closure provision for proceedings in
3 this Commission are not even found in MCRE 505. It's in a
4 separate part of the statute and found in a separate rule.

5 MJ [COL POHL]: Just so we're clear on this, which I may
6 be or may not be, the closure rules are governed by 806.

7 ATC [MS. BALTES]: Right. And it is 949(d) in the
8 statute.

9 MJ [COL POHL]: Okay. And specifically there's a
10 separate -- now -- the issue was if it's classified, that does
11 not warrant automatic closure, but there's a separate inquiry
12 that the judge must do to close the court and it would appear
13 that's the reading of 806(b)(2)(B).

14 ATC [MS. BALTES]: That's absolutely correct.
15 806(b)(2)(B) provides that there's a statutory right of access
16 then there's provisions for closure of the courtroom. Again,
17 that's not an automatic. The language is that the military
18 judge may close the courtroom.

19 MJ [COL POHL]: The mere fact it is classified is not
20 sufficient showing by government to close the proceeding.

21 ATC [MS. BALTES]: Right. It is a justification that
22 806 talks about, that is a justification for closing the
23 courtroom, but it is not an automatic closure. We agree that,

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 yes, you, the military judge, have discretion and you must
2 make findings.

3 MJ [COL POHL]: If I make a finding that this
4 information, although classified, must be discussed in open
5 court, then that gives the government options.

6 ATC [MS. BALTES]: Correct.

7 MJ [COL POHL]: Just procedurally -- I think there are
8 two separate issues being connected here of the pretrial
9 discovery phase and what could come out in the course of the
10 trial, both pretrial evidentiary hearings, trial of the merits
11 and sentencing, if any.

12 DTC [MS. BALTES]: Absolutely. I want to respond to
13 this because I think it's an inflammatory allegation for the
14 ACLU to come in and claim they've never seen anything like
15 this. In Ghailani, again the exact definitions that we used
16 in paragraph 7, which is what they are so upset about, are
17 verbatim to what was used in paragraph 3 in the Ghailani
18 protective order.

19 Specifically, the observations and -- let me get
20 the exact language. The term in paragraph 3 in Ghailani
21 specifically says that classified information will include,
22 without limitations, observations and experiences of the
23 defendants with respect to the matters set forth in the

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 several paragraphs above, which is the CIA RDI program. That
2 was classified in that case as well. It's the same here.
3 It's the same in this case.

4 The fact that the ACLU chose not to challenge on
5 First Amendment grounds in Ghailani, I don't have an answer
6 for that, but for them to come into this court and somehow
7 imply that because the government proposed a protective order
8 in this case that somehow we're violating the First Amendment
9 is disingenuous. The same provisions are in Ghailani.

10 In addition, although the protective order in
11 Ghailani doesn't have the 40-second delay, no courtroom in the
12 United States has the technology that we have. There is a
13 40-second delay that was built into this courtroom
14 specifically because of the types of cases that would be tried
15 down here. These are international terrorism cases.

16 And I would submit, and I believe Your Honor noted
17 yesterday, that the 40-second delay actually minimizes the
18 times that closure has to occur, and it provides a very
19 appropriate balance between making sure that the proceedings
20 can be opened without unnecessarily risking the disclosure of
21 classified information from an inadvertent comment.

22 MJ [COL POHL]: Ms. Baltes, how do you respond to the
23 argument which I heard from a number of the press side,

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 including the press objectors, about the government
2 voluntarily disclosing this information to the accused who in
3 some cases involuntarily received it and then somehow it --
4 we're restricting their ability to talk about that?

5 TC [MS. BALTES]: There are a couple of points. Number
6 one, this protective order does not restrict or impose
7 sanctions upon the accused. It would be quite different if we
8 were seeking a contractual obligation from the accused that
9 they're never allowed to talk about this.

10 MJ [COL POHL]: But if you take the protective order as
11 drafted, the accused says something that's covered by your
12 paragraph 7 to their defense counsel, there's no problem with
13 that, they got clearances. Defense counsel wants to convey
14 this information to a mitigation expert, an uncleared
15 mitigation expert, they would not be permitted to do that
16 under this order.

17 TC [MS. BALTES]: That is correct, but I --

18 MJ [COL POHL]: I'm not saying -- just so we all
19 understand, at this point what we're talking about is not
20 communication between the accused and his counsel or, quite
21 frankly, the accused to anybody other than his counsel, but
22 the further dissemination of said information to uncleared
23 people.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 TC [MS. BALTES]: That's correct.

2 MJ [COL POHL]: The protective order is designed at that
3 step for the defense teams and not necessarily within the
4 preparation between the accused and the defense.

5 TC [MS. BALTES]: Right. The protective order does not
6 purport to restrict any communication between -- I know the
7 defense doesn't believe this. I've heard this a number of
8 times.

9 Let me be clear. The protective order does not
10 purport to restrict communication between the accused and the
11 attorneys. They can talk about what -- regardless of whether
12 it's in paragraph 7 or any other definition or anything that
13 the attorneys have been told is classified, the accused can
14 talk to them, to the attorneys, about it.

15 Now, the attorneys holding security clearances are
16 obviously restricted in talking about other classified
17 information that they know back to the accused. I think
18 that -- I think there's clarity on that. I don't think that's
19 necessarily in dispute.

20 But the protective order, again, is supposed to
21 govern how parties handle classified information throughout
22 the proceedings, which is why it goes stage by stage of the
23 different parts that we're going to get to. But certainly

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 when it comes to a trial stage or the disclosure of that
2 information, there's other procedures in place.

3 MCRE 505(g) provides a mechanism for the defense
4 to provide notice to the government if it intends to disclose
5 classified information during any stage of the proceeding.

6 And then typically, as you've seen, the government
7 will file a notice, a 505(h) notice, requesting an opportunity
8 to be heard so that the military judge can determine the use,
9 relevance, and necessity of the disclosure of that
10 information. That can happen at the pretrial stage, which
11 we've seen and certainly most often, particularly in federal
12 court, we see it in the trial stage where the defense believes
13 there's classified information they seek to use at trial and
14 therefore -- that's when we get to a hearing about it.

15 MJ [COL POHL]: Once we complete the 505(h) session, the
16 hearing is kind of a misnomer because that implies it's with
17 the accused, but I know that's how it's referred to. Then the
18 next session is, if necessary, relevant material to the
19 defense, then you go to the 806 issue of how it comes out.

20 TC [MS. BALTES]: Right. And as you have experienced
21 already during a 505(h) hearing or session, I mean, the
22 government proposes alternatives for ways to either minimize
23 the exposure or come up with ways for the defense to present

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 their information in a way that may not lead to the harm to
2 national security.

3 Again, yes, if at that point you determine that
4 the classified information must come in, for whatever reason,
5 whatever your ruling is, then you would go to an 806 analysis
6 of do I then close the courtroom. You're absolutely justified
7 in closing the courtroom because of classified information,
8 but that doesn't mean that you obviously shouldn't make the
9 necessary findings.

10 MJ [COL POHL]: But that's not the end of the inquiry.
11 By that, I mean simply because it's classified, the way I read
12 the rule, there's another inquiry that goes on. It's not
13 declassifying, it is whether or not it meets the test of 806
14 to close the court.

15 TC [MS. BALTES]: Absolutely, and the test of 806 --
16 military courts applied the Press Enterprise factor as well as
17 United States v. Grunden talks about Press Enterprise factors.
18 8016 incorporates the four-part test the Supreme Court showed
19 in Press Enterprise enterprise. The four factors are whether
20 there's a substantial probability of prejudice to a compelling
21 interest, whether there is no alternative to adequately
22 protecting the information, whether the restriction that is
23 sought would be effective and whether it's narrowly tailored.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 I'm sure you're familiar with 806. It
2 incorporates that language that it has to be tailored, have a
3 compelling interest. If we were ever to get to that stage,
4 the parties would be able to articulate. Again, it's not
5 always the prosecution. It typically is the defense that
6 wants to put on the information. But certainly there would be
7 an ability to articulate those factors should Your Honor wish
8 to close a portion of the courtroom. That's not a foregone
9 conclusion.

10 The fact there's a provision in the protective
11 order that talks about closure simply refers to closure is
12 authorized by statute 949(d) and authorized in the rule,
13 Rule 806. So the fact we have paragraph 7, which includes
14 definitions that apparently no one likes, that the statements
15 of the accused about the RDI program are classified, and
16 closure in the same document somehow means government is
17 seeking closure of proceedings in this case, and that is
18 absolutely not accurate.

19 The other -- let me go back to Ghailani for a
20 second. Not to belabor the federal court, which I'm sure
21 you're sick of hearing, but in Ghailani the protective order
22 didn't have provision for closure of the courtroom. But
23 federal courts have inherent authority to close a courtroom as

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 well.

2 In Ghailani, that's what happened on numerous
3 occasions. The courtroom was closed specifically when talking
4 about capture information. So it's again somewhat
5 disingenuous for ACLU to come in and argue that for some
6 reason what government's suggesting in this case is something
7 courts have never done or never seen before with an accused
8 similarly situated to the accused in this case.

9 The other point I believe that the ACLU made was
10 somehow if a third party gets hold of classified information
11 that the government has no legitimate interest in keeping that
12 information classified. And that, as I know you understand,
13 would lead to absolutely absurd results. If for some reason
14 there's a leak or unauthorized disclosure of classified
15 information and then a non-government employee, someone in the
16 public, learns of that information, the government still has
17 an interest in keeping it classified.

18 MJ [COL POHL]: How is that? Better?

19 I don't believe there is much dispute, although
20 I'm sure I'm probably wrong, about the unauthorized leak of
21 classified information doesn't somehow declassify it. Okay?
22 I don't think that's what they're addressing.

23 What they're addressing in this particular case,

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 maybe it is a distinction without difference in your mind, but
2 I believe that's what the issue is. When the government
3 voluntarily discloses classified information to non-cleared
4 people, that somehow that then the government cannot come back
5 and say these non-cleared people, in this case the accused,
6 are somehow bound by the classification restriction of
7 discussing that information.

8 So I don't think it's your scenario -- do you see
9 a difference between ----

10 TC [MS. BALTES]: I do see it differently. Number one,
11 again, I think certainly the government, you know, believes
12 that there's a compelling interest in maintaining the
13 integrity of classified information regardless of whether it's
14 disclosed. I think you're familiar with the line of cases
15 that talks about the official confirmation versus speculation.
16 The Supreme Court clearly established that it is not the same
17 thing.

18 Just because information -- that a reporter may
19 speculate about some classified information is quite different
20 from a government official actually confirming the existence
21 of that, and that there is still a compelling government
22 interest in maintaining the integrity of that classified
23 information. That is -- *Afshar*, *Knopf*, *CIA v. Sims*, *Haig*

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 v. Agee, all are cases that stand for that proposition.

2 What I believe the ACLU is arguing is just because
3 the government involuntarily exposed the accused to --

4 MJ [COL POHL]: Their argument is the government
5 voluntarily exposed accused to this information, they may have
6 involuntarily received it, depending what we're talking about.

7 TC [MS. BALTES]: Right.

8 MJ [COL POHL]: Their argument, appears to me, is not an
9 unauthorized leak going out to a media outlet. The
10 government, by using these techniques, voluntarily exposed
11 this classified information, if you want to call it that, to
12 these accused.

13 TC [MS. BALTES]: I understand their position, and I
14 misspoke when I said "involuntary." I agree, I understand
15 that that's their position. Again, if the government was
16 seeking to exact some type of nondisclosure agreement on the
17 accused at this point to say, "You were exposed to classified
18 information, you're going to face sanctions just like someone
19 with a security clearance if you disclose that," I agree that
20 would be an absurd result. That's not what government's
21 seeking to do. Again, the protective order applies to the
22 parties in this case that hold security clearances that,
23 because of their participation in this case, they are exposed

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 to classified information.

2 MJ [COL POHL]: I may have misunderstood the point but
3 I'm not sure -- what the question becomes is by voluntarily
4 supposing this to people who do not have a clearance, does
5 that somehow waive the classification issue?

6 ATC [MS. BALTES]: No.

7 MJ [COL POHL]: You say no, but that's the way I kind of
8 glean this thing. We all agree that classified information
9 has to be handled a certain way. Their position appears to be
10 that if the government releases this -- voluntarily releases
11 it to somebody without a clearance in this case, in this
12 case -- but, therefore, that relieves the defense of the
13 burden of treating this information as classified.

14 TC [MS. BALTES]: No.

15 MJ [COL POHL]: I know you disagree. I think that's
16 what their position is.

17 TC [MS. BALTES]: I agree that is what their position
18 is. That would lead to absurd results if the government's
19 unable to -- again, we're talking about information that the
20 government still maintains control over at this point.
21 Whether people like to believe it or not, the fact is the
22 accused are held in a detention facility where they don't have
23 access to people other than their attorneys so -- but it is

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 perfectly appropriate for the government, as an original
2 classification authority did in this case, pursuant to the
3 executive order, to look at information about the sources and
4 methods that are at issue in this case and the RDI program and
5 determine that that is currently and properly classified.

6 The fact that they can communicate that
7 information and orally convey that information to their
8 attorneys is what's at issue. So it's the attorneys'
9 obligation who hold security clearances in this case to make
10 sure that that information then is not further disclosed.

11 You're looking at the time. Do you want me
12 to ----

13 MJ [COL POHL]: I just -- how much more do you got?

14 TC [MS. BALTES]: Well, I -- my team won't like this
15 either.

16 MJ [COL POHL]: My concern -- normally, I would not
17 mind, but my concern is we do have a detainee who wanted to
18 join us and we normally recess at 10:15. What we'll do --
19 normally I would let you continue. But because Mr. Mohammad
20 apparently wants to join us, and whether he does or not,
21 that's of course up to him, we'll go ahead and take a
22 15-minute recess now.

23 And then, Mr. Nevin, I'm sure you will tell me

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 whether -- if he doesn't come, indicates he doesn't wish to
2 come, wishes to stay in the holding cell.

3 Court is in recess until 1035.

4 [The Military Commission recessed at 1018, 17 October 2012.]

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 [The Commission was called to order at 1049, 17 October 2012.]

2 MJ [COL POHL]: The Commission is called to order. All
3 parties again are present that were present when the
4 Commission recessed, and Mr. Mohammad has joined us.

5 Yes, General Martins. Somebody not here?

6 CP [BG MARTINS]: No, Your Honor. You may be going
7 there as well, but the government would request that you
8 inquire into Mr. Mohammad as to how he communicated to the
9 guard that he wanted to be here, to make an appropriate record
10 of this. Given the court is looking at the presence and
11 absence, we need to confirm that kind of detail.

12 MJ [COL POHL]: Ms. Baltus, Mr. Nevin.

13 DC [MR. NEVIN]: Your Honor, Mr. Mohammad has a right to
14 remain silent. I understand the testimony regarding his
15 waiver when he is not here, that the court wants it on the
16 record that he has actually waived his right to be present and
17 the questions have been asked and answered appropriately.

18 I object to the court questioning him now. He is
19 here, and it sounds to me as if the government wants in some
20 way to make him a witness as to what he said or did to have
21 him come here, and maybe I am misunderstanding the prosecutor.

22 CP [BG MARTINS]: We seek to confirm that he has changed
23 his mind and that when he changes his mind he is communicating

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 that to the guards and making that a part of the record. The
2 court is looking at this, Your Honor, as you have read, make
3 the changing of one's mind and how consistent they are about
4 how they feel about being present is part of the analysis.

5 When they then go to determine and entertain
6 every, indulge every reasonable presumption against the waiver
7 of a fundamental right for any part of a proceeding, that they
8 will look to that, and the courts do look at when did they
9 change, how frequently did they decide they wanted to be there
10 or didn't, because it is all part of that context of a
11 knowing, voluntary, intelligent waiver.

12 MJ [COL POHL]: Okay. I understand the government's
13 position; however, since he is here, we are talking about his
14 waiver, I don't believe further inquiry of him is required.

15 Now, if you for some reason want to put on
16 evidence of how his waiver or his decision changed and came
17 on, obviously there would be sources that you would have that
18 are unrelated to Mr. Mohammad. I'm not sure it's, quite
19 frankly, necessary, but if you feel --

20 CP [BG MARTINS]: I would seek to do that, then.

21 MJ [COL POHL]: If you do want to do that, that's fine.
22 Let's not do it now though. What I am saying is I don't want
23 to turn each of these into a one-hour hearing that the accused

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 changed his mind, when it is very obvious he is sitting here
2 and he changed his mind. You feel compelled to put on some
3 evidence that that mind was changed, other than passing a note
4 to the guard, which is part of the record, and requested to
5 come in after the next recess and that he transported
6 himself -- or, excuse me, was transported to the holding cells
7 initially per his request and then we took a recess and now he
8 is here, what other evidence would you want to put on the
9 record?

10 CP [BG MARTINS]: Your Honor, it goes to that recess
11 part, to confirm that he was satisfied that it was going to be
12 the next recess and not immediately and that the recess wasn't
13 some overlay based on communication and misunderstanding of
14 what authority there was to bring him in.

15 MJ [COL POHL]: Since his counsel represented that that
16 was his desires, I don't believe further inquiry is required
17 on that issue.

18 CP [BG MARTINS]: The counsel, though, was in court with
19 us when this came in --

20 MJ [COL POHL]: Okay. Mr. Nevin, have you had an
21 opportunity to discuss this with your client? Do you have any
22 issue about the time when he returned?

23 DC [MR. NEVIN]: No, Your Honor. And secondarily, I

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 will just say if Mr. Mohammad has complaints about things, I
2 will raise them with the court. I am not reluctant or afraid
3 to do that.

4 MJ [COL POHL]: I expect you will. I understand at the
5 time it came out, General Martins, he was here, and Mr. Nevin
6 was here. All counsel, if they have an issue about their
7 client, any issue, I am sure they are more than willing to
8 raise it, and I don't believe any further inquiry on that is
9 required at this time.

10 CP [BG MARTINS]: Your Honor, I am satisfied with that
11 record now. Thank you.

12 MJ [COL POHL]: I was going to say that I have reviewed
13 the actual AE 37, I forget what the letter designation of what
14 the order is, in that sometimes when orders go through a
15 number of iterations the line that I put in somehow didn't
16 make it, and so a corrected copy, which was in the order I
17 intended to go out, will be sent out, and that's the one that
18 references the provision you are talking about.

19 CP [BG MARTINS]: Thank you, Your Honor.

20 MJ [COL POHL]: Ms. Baltes.

21 DTC [MS. BALTES]: Let me go back to my last point about
22 the position of the ACLU, about whether something can be
23 classified and whether there can be harm to national security

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 and who actually makes that determination. I believe the
2 ACLU's position is that there is no compelling or legitimate
3 interest for the government to classify the information that's
4 contained in paragraph 7 in the protective order because there
5 is already information out there about the accused's treatment
6 and capture.

7 The ACLU has previously made this assertion in
8 other cases. DOD v. ACLU in the D.C. Circuit where it was
9 squarely rejected, that just because information may be out
10 there doesn't mean that the government still cannot classify
11 the information, and it certainly doesn't justify its
12 disclosure. That was also an intervenor motion.

13 MJ [COL POHL]: Do you agree with -- well, let me ask
14 you this: There was an issue about previously classified
15 information that's no longer classified and that parts of this
16 order, at least some could read that it covers that
17 information.

18 DTC [MS. BALTES]: The government has no intention of
19 covering declassified information in the protective order.
20 And again, the definition in paragraph 7(d) specifically talks
21 about information that the defense have been notified either
22 orally or through guidance that is classified, and then it
23 goes through the separate subparagraphs about information

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 about capture, location, things of that nature.

2 So no, there is no -- this protective order
3 certainly does not seek -- again, the protective order is
4 merely a way to obviously explain to the parties what the
5 obligations are and what the examples are of the classified
6 information that's in this case. So it is certainly not
7 necessarily an exhaustive list. Again, as we discussed
8 yesterday, the defense counsel certainly have an obligation
9 because of their security clearances to handle information
10 that is classified if they know it is classified and if they
11 have so been so advised.

12 MJ [COL POHL]: The draft of the order only covers
13 classified information. Again, if one were to read it, at
14 least some were reading it to cover information that's not
15 classified, that's an incorrect interpretation, in your view,
16 of what the order says?

17 DTC [MS. BALTES]: Absolutely. Absolutely.

18 MJ [COL POHL]: All right.

19 DTC [MS. BALTES]: The other case I wanted to raise was
20 United States v. Moussaoui, which I believe the parties are
21 well aware of, but in the oral argument stage the government
22 sought in that case to seal certain portions of oral argument
23 with the Fourth Circuit and the media groups filed an

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 intervenor motion in that case requesting that the court
2 consider not closing and not sealing certain of the records.

3 Again in that case -- now, the court did go
4 through kind of the analysis that in federal court CIPA alone
5 does not justify a closure of the courtroom, which is
6 consistent with the government's position here. Other courts,
7 United States v. Pelton, have also found that, and I believe
8 that's what we were discussing before the break, that just
9 because something is classified doesn't necessarily mean that
10 there is a closure, and neither CIPA nor MCA 505 in Military
11 Commissions contain that language.

12 But what's important in the decision in Moussaoui
13 is that they squarely rejected the intervenor -- the media's
14 interpretation that the court should review the classified
15 information to determine whether or not it was actually
16 classified.

17 Again, the court said, relying on United States v.
18 Smith, which is a prior espionage case in the Fourth
19 Circuit --

20 MJ [COL POHL]: Ms. Baltes, I am going to ask you to
21 slow down a little bit. I am getting a lot of notes from the
22 interpreters.

23 DTC [MS. BALTES]: The government may determine what

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 information is classified. A defendant cannot challenge it, a
2 court cannot question it. Again, the Fourth Circuit
3 reiterating the position that United States v. Smith held.

4 Another, it is one thing for a reporter or an
5 author to speculate or guess that a thing may be so or even
6 quoting from undisclosed sources to say that it is so, but it
7 is quite another thing for one in a position to know of it to
8 officially say that it is so, and this is from the Alfred
9 Knopf v. Colby cases that I mentioned earlier.

10 Also, United States v. Pelton again, there is a
11 difference between speculation and confirmation, and that goes
12 to the ACLU's assertion in this case that because there is
13 some publicly available information about the treatment of the
14 accused, that all of a sudden there is no justification for
15 the government or no compelling interest for the government
16 to, number one, have information that's classified or, number
17 two, that that information could ever justify closure of the
18 courtroom.

19 And as to the second point, we are not there yet.
20 No one is seeking to close the courtroom, so I don't even
21 think that's an appropriate avenue for us to have to go down,
22 other than there are certain provisions in place that --

23 MJ [COL POHL]: Just so it is clear, I am simply

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 addressing the protective order on the discovery -- quite
2 frankly, mostly discovery issues. Closure of the courtroom or
3 the Commission is a different issue altogether that will be
4 addressed in the normal course of business.

5 DTC [MS. BALTES]: I couldn't agree more. I couldn't
6 agree more.

7 And just the last point on that, because I think
8 that's one of the major concerns from the media, is that that
9 you are, in the event that happens, for some reason you are
10 not going to make findings. And again, they have used this
11 protective order as a vehicle to bring it up because there is
12 a provision of closure of the courtroom in the protective
13 order.

14 But it's the government's interpretation of
15 Rule 806, again, that in the event there is a proposed closure
16 of the courtroom, that you would have to make findings and the
17 government would certainly propose that the appropriate
18 findings that should be made would be those as articulated by
19 the Supreme Court in Press Enterprise factors.

20 I know that's an issue for another day, but I
21 believe that's one of the reasons that the media outlets have
22 challenged the protective order, because they are concerned
23 that the court would immediately go from a 505(h) hearing and

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 determine yes, something is classified, someone wants to
2 disclose it, to an immediate closure of the courtroom. That's
3 certainly not the way that we believe Rule 806 should be read.

4 And again, we can leave that for another day
5 because I don't believe that that's what the protective order,
6 says at all, but I understand that that is one of the concerns
7 of the media outlets.

8 MJ [COL POHL]: Why don't we just pull out that
9 reference to closed proceedings from the protective order
10 since that's covered by different rules altogether.

11 DTC [MS. BALTES]: That's fine. Again, I don't think
12 that -- that provision in the protective order certainly is
13 not meant to imply that there is an automatic closure, and
14 that's not what it says.

15 So I think if you allow every outside party to
16 decide that they think that something means what it means, we
17 are going to be here for a long time with a protective order
18 that has 51 paragraphs in it, but it is contained in another
19 provision, and again it's in there to explain how things can
20 happen throughout this case with respect to classified
21 information.

22 MJ [COL POHL]: But a lot of the protective order is --
23 maybe the confusion is, is the protective order, a lot of it

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 is redundant with other procedures in 505, 806.

2 DTC [MS. BALTES]: Right.

3 MJ [COL POHL]: And, quite frankly, how the classified
4 information is supposed to be handled by people that have it.

5 DTC [MS. BALTES]: Right. And I think there is
6 certainly no intention by the government to put -- to say that
7 the protective order presumes obligations that the parties
8 don't have. I mean, again, the point of the protective order,
9 and going back to the history of the protective order, is that
10 typically in a national security case, where the defense
11 counsel are receiving security clearances, it's likely to be
12 their first foray into dealing with classified information.
13 This is not something that attorneys typically do.

14 I heard Ms. Shamsi mention yesterday that there
15 are hundreds of terrorism cases across the country that are
16 tried and that this is somewhat normal. But in fact there may
17 be hundreds of terrorism cases that the government has brought
18 since 9/11, but I don't believe there have been hundreds of
19 trials. And it is a relatively unique situation where an
20 attorney has a security clearance by virtue of their
21 participation in the case.

22 So the protective order, as envisioned under CIPA
23 Section 3, was to again lay out the parties' obligations and

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 to explain that there is this procedural framework called CIPA
2 in federal court that applies to the proceedings, so that's
3 why it goes through.

4 Again, we are in a slightly different situation
5 here, but still I'm sure many of the attorneys in this case,
6 prior to their participation, had never dealt with classified
7 information, so it's appropriate to lay that out in a
8 protective order.

9 505(e), I think Congress' intent to make sure that
10 this was squarely addressed in Military Commissions is obvious
11 by the language that upon an order or a motion by the
12 government, the military judge shall issue a protective order
13 in the case. That's 505(e), which is what the government has
14 done here.

15 So let me finally get to the provisions in the
16 protective order, and I know that there has been a lot of
17 objections raised by the defense, so I am going to try and go
18 through those, assuming I am not going to have an opportunity
19 to respond after the defense makes their objections. But I
20 believe we have discussed that there is -- in the protective
21 order there are certain stages of the proceedings, and that
22 again it's intended to convey what happens in these types of
23 cases and what other obligations the parties have either

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 through 505 or through their security clearance. So it's a
2 practical guide for the parties to go through when they are
3 dealing with these types of cases.

4 I think one of the defense objections that came in
5 in 13 Charlie, maybe, I have lost count, but the primary
6 deference objection that I believe was filed by Mr. Connell,
7 raised the issue of the government's use of a declaration in
8 support of its motion for a protective order, and there is
9 some insinuation that the government has to disclose that ex
10 parte declaration that it filed in support in order to invoke
11 a privilege.

12 And I think it's been very confusing, but I would
13 like to explain to the court that the ex parte declaration
14 that was submitted in support of the government's motion for a
15 protective order does not invoke a privilege over information
16 that the government is seeking to keep from the defense.

17 Again, the protective order is supposed to lay out
18 what the parties' obligations are. We are not seeking to
19 assert a privilege of information that we are telling the
20 defense at this point that they can't have. There may be a
21 time throughout the discovery phase where the government does
22 utilize that process, but that's not before it.

23 And the case law that the defense has cited, is

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 completely inapposite. *Ellsberg v. Mitchell*, *United States*
2 *v. Reynolds*, which is in the defense brief, those are state
3 secrets cases and this is not a state secrets case.

4 State secret cases are civil cases in which the
5 parties have brought suit or they are seeking evidence and the
6 government asserts a privilege, and in common law rights it's
7 always been called a states secrets privilege. That has long
8 been recognized as an evidentiary privilege for the government
9 to decline to provide information that could cause damage to
10 national security. And so in a states secrets case the courts
11 have been clear, in *United States v. Reynolds* and in *Ellsberg*,
12 that if the United States is seeking to invoke such a
13 privilege, yes, it should be done in an adversarial proceeding
14 and it should be done on the record. And again, that's
15 because in a civil context when the government asserts that
16 kind of a privilege, they are actually depriving the parties
17 an opportunity to use that information.

18 That is absolutely not what goes on in a criminal
19 prosecution. And although there have been two cases in the
20 criminal context that have cited the state secrets privilege
21 when applying CIPA, even those cases, the *United States*
22 *v. Aref* in the Second Circuit, *United States v.*
23 *Klimavicius-Viloria* in the Ninth Circuit, which these are

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 cases that we previously cited in our briefs, those cases,
2 although they maintain that the government media asserting a
3 state's secrets case in a CIPA context and they wanted a
4 declaration to come from the head of an agency, they have
5 nevertheless followed the CIPA procedures in allowing ex parte
6 declarations, and these have all been in the CIPA Section 4
7 context, which is again the discovery phase, which is not
8 before the court now.

9 But that may be where the government in the past
10 has utilized procedures where we take discovery to the court
11 to make sure that the court is comfortable with any
12 substitutions or summaries that we intend to use to provide to
13 the defense in discovery.

14 MJ [COL POHL]: Just to be clear, the declarations are
15 designed to support the classification?

16 DTC [MS. BALTES]: There are two.

17 MJ [COL POHL]: Not to invoke a privilege.

18 DTC [MS. BALTES]: Correct. Correct. There may be -- I
19 mean, there may be, theoretically, yes, there is a possibility
20 that you would invoke a privilege to preclude the disclosure
21 of some information, but that would only be after a
22 determination that it's, in fact, relevant.

23 I mean, typically when the government in a

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 criminal case is bringing forth classified information to the
2 military judge or to a federal district court judge to
3 determine whether summaries are appropriate, it's because the
4 balance of the information that we are seeking to delete is
5 not relevant.

6 MJ [COL POHL]: I just want it clear what we are talking
7 about, because we spend a lot of time talking about things
8 that I am not sure we are talking about. And what I'm saying
9 is these declarations are not, this is not a
10 privilege-invoking declaration that would trigger, for
11 example, the 505 summary process.

12 DTC [MS. BALTES]: Right. I mean, that's again if we
13 are filing declarations, it is not necessarily that we are
14 invoking any type of privilege. But even if we were, there is
15 nothing in 505 and there is nothing in CIPA that requires the
16 invocation of a privilege to be made in an adversarial
17 setting.

18 MJ [COL POHL]: Just so I am clear, we are not talking
19 about a privilege invocation, we are simply saying this
20 negotiation is classified ----

21 DTC [MS. BALTES]: Correct.

22 MJ [COL POHL]: ---- and must be handled in this manner.

23 DTC [MS. BALTES]: Correct. And it may go into the

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 harms to national security should disclosure happen, which is
2 something, again, not -- that information may be privileged,
3 but that's not relevant to the extent the defense doesn't have
4 a need to know, but certainly the declaration would provide,
5 yes, the information is classified.

6 And part of that, if you go back to the executive
7 order, information could only be classified if there is some
8 damage to national security. So that's part and parcel of the
9 determination of whether something is classified. And then
10 it's just secret, is it damage to national security; top
11 secret, is there grave damage; and then SCI, compartment
12 information, would be exceptionally grave damage to.

13 But I wanted to address that because there seems
14 to be some confusion in the defense filings that the
15 declarations that we filed somehow are invoking some type of a
16 privilege and that they would be entitled to some adversarial
17 process with respect to that privilege and that those cases
18 that are cited by the defense are again state secrets cases
19 that are absolutely inconsistent with Rule 505 or CIPA.

20 In fact, the United States v. Rosen in the Fourth
21 Circuit had an opportunity to address the Second Circuit's
22 discussion of the state secrets privilege and specifically
23 rejected it, that although it wasn't clear to the Fourth

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 Circuit, that the Aref court properly adopted and even applied
2 state's secrets in the criminal context, but even absent that,
3 Aref in the Second Circuit followed CIPA. And in that case,
4 it was a Section 4 like our 505(h) process in the discovery.

5 The defense security officer -- I know we covered
6 that yesterday in the discussion about presumptive
7 classification -- but the protective order that the defense
8 has proposed in 13(m) has a couple of paragraphs about how --
9 their request for a defense security officer.

10 In the colloquy you had with defense counsel
11 yesterday there was a question of, well, how does this
12 declassification challenge occur in federal court? If the
13 parties don't have their own security officer to advocate on
14 their behalf, how does a court security officer do that?

15 And let me be really clear that that doesn't
16 happen in federal court. There is no classification challenge
17 by the defense in a federal criminal proceeding where
18 classified information is at issue.

19 MJ [COL POHL]: The government's position is that, and I
20 am assuming this, is substantive classification issues are
21 beyond the purview of challenge at court.

22 DTC [MS. BALTES]: Absolutely.

23 MJ [COL POHL]: Now, procedural -- what I am saying, you

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 follow the proper procedural classification issues, would you
2 consider that separate or is that the same?

3 DTC [MS. BALTES]: I guess I don't understand what you
4 mean.

5 MJ [COL POHL]: What I am saying is that there are
6 certain procedures in executive orders in how a document is
7 classified.

8 DTC [MS. BALTES]: Yes.

9 MJ [COL POHL]: Okay. Okay. Okay. But you would put
10 that in the nonchallengeable category, too, that they are
11 presumed to have been followed if a document is classified?

12 DTC [MS. BALTES]: Yes. Yes.

13 MJ [COL POHL]: I just want to make sure.

14 DTC [MS. BALTES]: Yes. Absolutely.

15 MJ [COL POHL]: So at the end of the day it's the
16 government's position that if a piece of paper says "secret"
17 on it, that's the end of the inquiry of its classification,
18 why it's classified and everything else, that's all off the
19 table, it's now treated as a secret document.

20 DTC [MS. BALTES]: Right.

21 MJ [COL POHL]: Okay.

22 DTC [MS. BALTES]: I mentioned United States v. Smith,
23 which is the Fourth Circuit case that says the government may

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 determine what information is classified, a defendant cannot
2 challenge it, a court cannot question it.

3 United States v. Aref, the Second Circuit case,
4 also addressed this issue and specifically talked about that
5 the Court's function in CIPA, which is our 505 analog, is not
6 to hold mini-trials in which the judiciary, not the executive
7 branch, becomes the arbiter of this country's national
8 security. There would be no way to move forward with a
9 criminal prosecution involving classified information if the
10 defense, who obviously are in an adversarial position with the
11 government, challenges every single piece of paper that the
12 government says is classified. Sorry about that.

13 MJ [COL POHL]: You have got to slow up, Ms. Baltes.

14 DTC [MS. BALTES]: Sorry about that.

15 Again, the Moussaoui court also reiterated the
16 Court's holding in Smith and Aref that it is not up to the
17 defense to challenge the information.

18 MJ [COL POHL]: So there would be no need for a defense
19 security officer to have the ability to sit down informally
20 and discuss why something is classified with the OCA or an OCA
21 representative.

22 DTC [MS. BALTES]: Right. To the extent that the
23 defense has a question about, look, I am looking at this

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 document, it says classified, and yet I see a New York Times
2 article that mentions the same thing, can you let me know
3 whether I should treat that New York Times article as
4 classified based on my access to classified information?
5 Again, am I allowed to repeat what The New York Times said and
6 assume that it's then unclassified? That's the type of
7 question certainly that the OCA, that the court security
8 officer, could advise; because if there is genuine confusion
9 about I have got a document marked this and then I am seeing
10 something out in the public, that's fine.

11 MJ [COL POHL]: But your view is that -- and I used the
12 term "Western Union" yesterday, which was perhaps
13 inaccurate -- but to transport that request is what you
14 envision the court security officer function and all he is
15 doing is carrying the mail from the defense to the OCA, the
16 OCA's response back to the defense, and having no role over
17 and above a courier role.

18 DTC [MS. BALTES]: On that scenario.

19 MJ [COL POHL]: On that scenario, right.

20 DTC [MS. BALTES]: I think it's helpful that a ----

21 MJ [COL POHL]: Why couldn't a defense court security
22 officer do the exact same thing?

23 DTC [MS. BALTES]: Number one, it's not appropriate, I

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 think, for the defense to have access to the original
2 classification authority, for a whole host of other reasons,
3 that -- they are a member of the intelligence community, they
4 hold a clearance, they may not have an overt identity, they
5 may have a covert status. That's somewhat typical in the
6 intelligence community.

7 MJ [COL POHL]: So you believe this part of the role
8 should not be a member of the defense office. But what about
9 other parts of the proposed defense court security officer
10 advising them?

11 DTC [MS. BALTES]: To the extent that they, you know,
12 they say that their defense security consultant can't perform
13 those duties, I am not sure. They have a security clearance.
14 Do they want someone who has had a security clearance longer,
15 that has more experience, that they can advise them? I am not
16 clear about what it is that they expect to get out of a
17 security officer, but it's certainly not a function that a
18 defense -- I think what they want to get is almost like an
19 OCA, someone that can go through their material that's in a
20 privileged setting and then advise them whether something is
21 classified or not.

22 But again, as we discussed yesterday, you can't
23 have an original classification authority work for the defense

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 because they work for the owner of the information. That's
2 just not possible.

3 So I don't know what they are trying to get that
4 they wouldn't already have by virtue that they have a security
5 clearance. If they need additional training about their
6 security clearance or about handling procedures, I believe
7 that there are opportunities through the office to do that.

8 MJ [COL POHL]: If you look at their proposed protective
9 order, I know you have a stack of paper there, I believe it's
10 attachment C to Appellate Exhibit 13(m), starting on page 8.

11 DTC [MS. BALTES]: Yes.

12 MJ [COL POHL]: They list four functions of the defense
13 security officer, and let's assume we are not talking about
14 Charlie.

15 DTC [MS. BALTES]: Okay. So assist the defense with
16 applying classification guides, including reviewing pleadings
17 and other papers prepared by the defense to ensure that they
18 are unclassified or properly marked as classified.

19 MJ [COL POHL]: I am just trying to figure out, none of
20 this other stuff -- the defense made some reference earlier
21 that the government says yes, you should have that, should
22 have something to assist you in the classification issues.

23 DTC [MS. BALTES]: I mean, I think that it's

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 appropriate. If they have their own space, they have security
2 clearances, they are in a SCIF, then typically organizations
3 like that have a physical security officer who can advise,
4 hey, you can't leave top secret information out, you need a
5 cover sheet, here is the safe, here is how to store
6 information in the safe. That seems to be the role of the
7 security officer.

8 The roles here that are listed in A and B, that's
9 what you are supposed to do if you have a security clearance.
10 I mean, you are supposed to be able to look at classified
11 material and determine, based on your classification guidance,
12 whether or not it should be marked. And again, if they have a
13 question with that, that's more appropriately directed towards
14 the CSO to the OCA, because who else is going to do that?
15 It's just going to be what someone else with a security
16 clearance says, well, I don't know, I think that's classified,
17 do you? That seems to me not ----

18 MJ [COL POHL]: Basically what you are saying is except
19 for the -- I am going to call it the courier function, which
20 is something to clarify with the OCA whether something is
21 classified, not properly classified, simply whether it's
22 classified, because they got it from a source that it's
23 unclear, that can be easily performed by the court security

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 officer who works for the judge.

2 DTC [MS. BALTES]: Correct.

3 MJ [COL POHL]: Then there is advocacy or any role
4 there, it's simply a matter of the defense provides
5 information to them in a written form, it's then taken from
6 the court security officer to the OCA, they provide a written
7 response through the court security officer who then takes the
8 envelope and hands it back to the defense?

9 DTC [MS. BALTES]: That's correct.

10 MJ [COL POHL]: All this other stuff is just part of
11 handling classified information that they should know to begin
12 with.

13 DTC [MS. BALTES]: Yes.

14 MJ [COL POHL]: And if they have questions about it,
15 they need to talk to ----

16 DTC [MS. BALTES]: There is nothing specific in here
17 that anyone other than someone with a security clearance --
18 maybe it's someone who had a security clearance before that is
19 more comfortable with material. But absent that, I don't know
20 what they think they will be getting with that.

21 The other piece that it appears that the defense
22 wants is, you know, this defense security officer so they can
23 perform declassification. And let me be clear, it is not the

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 job of the defense to seek declassification. That is
2 completely inconsistent with the procedural framework of 505
3 and CIPA.

4 If the defense wants to use classified information
5 and it's marked "classified" or they know, based on their
6 classification guidance, that it's classified, they have to go
7 through a 505. It's 505(g). They file a notice of intent to
8 use it.

9 If for some reason the government gets that notice
10 and looks at it and says it's classified, but for that limited
11 purpose, or there is a way to declassify the portion of it
12 they need for those proceedings, that's where that process
13 happens. It's not that the defense has a security officer or
14 they themselves should be advocating to some other entity that
15 information can be declassified.

16 MJ [COL POHL]: This comes back to your point that once
17 a document is classified, as I understand the government's
18 position, that's the end of the inquiry as to whether it's
19 classified or not.

20 DTC [MS. BALTES]: Absolutely.

21 MJ [COL POHL]: Because when I say it means I understand
22 your arguments, not that you agree with it.

23 DTC [MS. BALTES]: I would like it, you agree with

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 everything I say, but that might not be the case.

2 The government had an Exhibit, Defense Exhibit 30,
3 for a Navy security officer that again seemed to incorporate
4 some of the items that they wanted. And again I want to
5 distinguish, first of all, that's not necessarily a standard
6 practice. I think the Navy has used it in certain cases, but
7 it's certainly not something that has ever been adopted in
8 federal court.

9 And I think the big distinction is this. In Navy
10 practice, in a court-martial practice, to the extent
11 classified information comes up in a case, it is going to be
12 an espionage or leak case, it is by virtue of the
13 jurisdiction, that it is a service member who is being
14 prosecuted for something. That service member typically would
15 have had access to classified information or had a security
16 clearance.

17 So in a certain context I understand that the Navy
18 has determined that it's helpful if you are dealing with large
19 volumes of information that someone may have had access to,
20 and if that is part of the element of the charge, that they
21 have a person that helps go through the actual classified
22 information.

23 The reason why you have never seen it in federal

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 court, I believe, and in practice, particularly in terrorism
2 trials, is that the accused don't have a security clearance.
3 And I don't want to open another can of worms about the
4 exposure of classified information, because certainly we
5 concede that the accused in this case have access and have
6 been exposed to classified information, but certainly not the
7 type or the volume of information which justifies adding a
8 defense security officer that the Navy has found to be
9 appropriate in certain cases, and I'm not sure if they have
10 used it in the Bradley Manning case, the Wikileaks, but that's
11 the type of cases where those types of people may have been
12 used.

13 MJ [COL POHL]: That's an Army case.

14 DTC [MS. BALTES]: I know that's an Army case. I don't
15 know whether they have used it in the Army or not. I have
16 only heard of it in the Navy, but that would be an example of
17 the case potentially where that may have been used.

18 Finally, I think we mentioned this yesterday, but
19 federal law does anticipate that the government authorities
20 are the ones that are going to be protecting classified
21 information. 505(e) provides that the protective order that's
22 issued to the defense may include that the Convening Authority
23 authorizes the assignment of government personnel in the

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 provision of government storage facilities, which again is
2 consistent with the security procedures issued pursuant to
3 CIPA by the Chief Justice of the Supreme Court that lays out
4 the roles and obligations of a court security officer that is
5 a neutral body.

6 And I understand many of the defense counsel are
7 employees of the United States government, but
8 notwithstanding, it is they are employees by virtue of their
9 defense in this case. And so it's appropriate again that it's
10 a neutral body and that it is someone that doesn't necessarily
11 have an allegiance to the defense in this case.

12 Mr. Connell also -- there are a number of other
13 paragraphs in the proposed protective order. For the most
14 part, with the exceptions of four paragraphs in the proposed
15 protective order that he submitted in 13(m), the government
16 objects to all of those changes.

17 The only change is paragraph 3, that would be
18 acceptable to the government, that the language is changed to
19 people that would fall under the supervision of defense
20 counsel, and that's an acceptable change to the government,
21 and paragraph 4 about who is actually covered by the
22 protective order, the government has no problem, I think as we
23 discussed yesterday.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 And I'm happy to take the ----

2 MJ [COL POHL]: I thought you said there was four you
3 agree with.

4 DTC [MS. BALTES]: I do. I mean to say I didn't have
5 access, I'm sorry, down here to the actual Word version of the
6 protective order, but I am happy to go through and redline it
7 and resubmit it to Your Honor.

8 MJ [COL POHL]: That's okay. Just tell me of their
9 proposed protective order what you agree on.

10 DTC [MS. BALTES]: Paragraph 3, the change of paragraph
11 4, and then paragraph 31 and 38, I would suggest a
12 modification, not ones that the defense suggested, but based
13 on our discussions yesterday, paragraph 31, the parties had an
14 issue with because it used the term "presumptive
15 classification." That was the discussion we had yesterday.

16 So I think it would be appropriate to use language
17 that refers to information that is classified at the TS code
18 level, including classified statements of the accused
19 described in paragraph 7(d)(1)(G).

20 MJ [COL POHL]: Looking back to that definition.

21 DTC [MS. BALTES]: Right, so it is clear, and looking
22 back to paragraph 38, there is some confusion about that
23 paragraph, so we would propose that because some statements of

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 the accused are classified at TS code word, the defense must
2 provide notice in accordance with the protective order and
3 505(g) if the defenses intends to offer statements or offer
4 testimony in any proceeding that relates to information
5 contained in paragraph 7(d)(1)(G), which again refers
6 back ----

7 MJ [COL POHL]: Which paragraph would that be?

8 DTC [MS. BALTES]: That would be paragraph 38. We would
9 alter any other statement the defense counsel know or have
10 reason to know was classified, because paragraph 38 mentioned
11 because all statements of the accused are presumptively
12 classified, so we would alter that language so it is clear
13 that they would only have to file a notice in the event that
14 it's information that they know is classified or that relates
15 to something that goes back to the definitions section.

16 MJ [COL POHL]: Now, yesterday we discussed language in
17 your motion that says defense must treat as classified
18 information, information that they know or have reason to know
19 was classified.

20 DTC [MS. BALTES]: Uh-huh.

21 MJ [COL POHL]: Mr. Connell, as we have bled over into
22 13 yesterday ----

23 DTC [MS. BALTES]: Right.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 MJ [COL POHL]: ---- believe the language should track
2 more with the executive order. Do you have any objection to
3 that?

4 DTC [MS. BALTES]: I like know or reason to know because
5 there is a certain element of trust involved in granting
6 someone a security clearance and taking that information. I
7 think it's appropriate.

8 MJ [COL POHL]: Ms. Baltes, you may like it, but I am
9 saying is the standard in the executive order, what is the
10 appropriate legal standard, but we may want to parse it, we
11 may want to say if I wrote the executive order because I would
12 write it definitively.

13 DTC [MS. BALTES]: I am not disagreeing with what the
14 executive order says, but it is not written contemplating that
15 this would be the only document that parties look to when they
16 are involved in a criminal proceeding involving classified
17 information. That's not it. So that legal, you know,
18 justification is sound in the executive order, but that's not
19 for the purpose that we are here today. And I believe that
20 that language in the executive order refers to the interim
21 classification, and that's not what we are talking about here.

22 MJ [COL POHL]: Okay.

23 DTC [MS. BALTES]: So, I mean, I can go paragraph by

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 paragraph or for all the reasons that we object to the other
2 defense proposals.

3 MJ [COL POHL]: Would it be fair to say what's in their
4 protective order, except for the ones you just talked about
5 that aren't in your protective order, you object to?

6 DTC [MS. BALTES]: We object to, and there are various
7 reasons. I don't want to take up any more time than I need
8 to. I can go through and specifically articulate why it is
9 that we objected to those or I can wait and see if the defense
10 still wants those. I'm assuming they do.

11 MJ [COL POHL]: Just because this issue has been shown
12 that we are on, M, is going back and forth and back and forth,
13 what my proposal would be is that at the end of this
14 discussion today I will make some decision and issue, probably
15 issue -- because there may be an argument, I shouldn't issue
16 any protective order, but you and the other side will get an
17 order on this. And if there is a protective order and you
18 want to revisit the wording I have chosen, you can do it.

19 But it seems to me as we speculate back and forth
20 as to this provision versus that provision, we will be here
21 forever because this is like a tennis match going back and
22 forth.

23 DTC [MS. BALTES]: I agree.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 MJ [COL POHL]: I have the position of the parties. I
2 am going to let the defense argue it, but I have the position
3 of the parties. I will send an order out which will be
4 applicable, if I send one out, and again there may be an
5 argument that there shouldn't be one, but if one should be
6 sent out, that will be applicable until it is changed.

7 But if there is something in there that either
8 side objects to and wants me to revisit, I certainly will.
9 But it just strikes to me if we wait for a complete discussion
10 of changing positions -- rephrase that, revise positions,
11 this, that, we are going to be here forever without any
12 protective order, which, in my view, is going to slow down
13 discovery in this case, which at least we can get started
14 within the confines of what's ever issued, with the
15 understanding that if defense or the government wishes to
16 revisit it after you see what I actually issue -- again, I am
17 going issue something -- it seems to me that would be a more
18 disciplined process than to speculate back and forth of what
19 an order you may or may not have seen, because the government
20 has got their version, the defense has got their version, and
21 now we are arguing against each other's version.

22 But why don't you get my version and then argue
23 against my version and it seems to me that's a more efficient

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 way to do this.

2 So I understand your position, Ms. Baltes, I
3 certainly understand the defense position, and I am not
4 limiting the argument at this time, but to go back and forth
5 on each subparagraph or paragraph, I've got it; you disagree
6 with what you disagree with, the defense disagrees with what
7 they disagree with in their briefs, your rationalization for,
8 but let's move the process along.

9 DTC [MS. BALTES]: I think that's an appropriate
10 approach here. And I just want to leave the court with this
11 statement, then. 505, Congress clearly manifested an intent
12 under 505 that the body of case law applying CIPA should be
13 authoritative and interpretive, weren't to classification of
14 information in proceedings, and in 505(e) the protective order
15 we are seeking, it's the government motion that seeks the
16 protective order that you sign, that we hope that you sign,
17 that Congress says you shall sign. We understand you have
18 discretion to sign the order that you want.

19 But I just -- I think it's really important to
20 note that the government has the compelling interest in
21 protecting the information, and that's not to say because of
22 their security clearances the defense don't also understand
23 the obligation.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 But, quite frankly, we are in an adversarial
2 position and the entire reason why CIPA was enacted was to
3 make sure that the government could prosecute individuals
4 without compromising national security. And again, there
5 is -- it's not a substantive statute, it's a procedural
6 statute, but there is an important policy in making sure the
7 government can bring a case in a case like this, where almost
8 3,000 people were murdered, and we are not compromising
9 national security where we can no longer bring these cases.

10 So the provisions in the government's protective
11 order have again, these are tried and true provisions that
12 have been used in federal courts, so I would submit to the
13 court that that is consistent with the language that Congress
14 has clearly manifested its intent that that is the body of
15 federal case law we should be looking towards for the
16 protective order, not necessarily the language that the
17 defense is proposing in their protective order.

18 MJ [COL POHL]: Thank you, Ms. Baltes.

19 Mr. Connell.

20 DC [MR. CONNELL]: Your Honor, I have previously shown
21 our slide deck to the court security officers or the
22 Commission security officer. May I have permission to publish
23 that?

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 MJ [COL POHL]: Go ahead.

2 DC [MR. CONNELL]: Before we come to this document,
3 Colonel, I want to be clear that I am going to focus, with one
4 minor exception, exclusively on issues that we did not discuss
5 yesterday regarding 13 and not 9. I want to respond to the
6 new arguments that the prosecution made about the defense
7 security officer. But other than that, I am going to focus
8 exclusively on the issues in 13. I am not going to do a
9 paragraph-by-paragraph analysis, except for where it is useful
10 to the court to see the two paragraphs side-by-side.

11 The fundamental problem with the protective order
12 is that the government's position here suffers from a
13 fundamental flaw, which is that what we need is a very basic,
14 very redundant protective order that tells us no, no, no, do
15 not release classified information, which we know, but at the
16 same time does not allow us to address the nuances of what is
17 actually classified that we struggle with every day at the
18 Office of the Chief Defense Counsel.

19 That redundant primer becomes the law of the case.

20 MJ [COL POHL]: If it's redundant, what difference does
21 it make?

22 DC [MR. CONNELL]: Because it has padding on it as I
23 described yesterday.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 MJ [COL POHL]: It would seem to me if it is redundant
2 with other provisions of law, then you are under those
3 obligations and therefore saying it again wastes ink but
4 doesn't waste intellectual energy. So let's talk about what
5 is not redundant.

6 DC [MR. CONNELL]: And that's exactly the point, Your
7 Honor, and that's the position that I took yesterday, is we
8 have an obligation to protect classified. You know, this has
9 come up several times today already, of when the government
10 takes a protective order and rewords an existing obligation in
11 a way that lowers its floor or raises the bar for the defense,
12 then that's not the same as being redundant.

13 MJ [COL POHL]: Exactly. I agree with that.

14 DC [MR. CONNELL]: And the point that I want to make
15 before I go to the slide show, and if we can have that page
16 now, is the government said that the reason why this doesn't
17 come up in federal court is that there are no classification
18 challenges, typically defense counsel don't have security
19 clearances. Essentially, it doesn't come up.

20 In fact, the executive order imposes a duty upon
21 us to bring classification challenges. And if we could
22 highlight footnote 5 please.

23 MJ [COL POHL]: Which exhibit is this from?

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 DC [MR. CONNELL]: This is the government's brief 0009 A
2 and it's paragraph 5.

3 MJ [COL POHL]: 009?

4 DC [MR. CONNELL]: 009 A. The government notes in its
5 brief that Section 1.8 of Executive Order 13526 encourages
6 authorized holders of classified information to challenge the
7 classification status in accordance with established agency
8 procedures if in good faith they believe that the
9 classification status is improper.

10 The reason why I bring this up is to show how
11 wrong it is for the government to argue this morning that as
12 authorized holders of classified information we don't have any
13 authority, any basis, any reason to challenge classification
14 decisions. We are required to challenge classification
15 decisions. And I went last night after the Court's question
16 and looked up ----

17 MJ [COL POHL]: Let me ask you this: Do you think
18 that's intended in this scenario or intended for members of an
19 organization to challenge improper classifications?

20 DC [MR. CONNELL]: I am a member of an organization,
21 Your Honor, the Department of Defense.

22 MJ [COL POHL]: If you read the executive order in total
23 context, do you think this is designed for a third-party,

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 nonmember of the organization to challenge it, or a member of
2 the organization who believes it is being improperly
3 classified?

4 DC [MR. CONNELL]: It is -- the phrase "authorized
5 holder" in the executive order is a term of art. That
6 authorized holder is any person who is authorized to have
7 access to particular classified information. For example, an
8 authorized holder is allowed to make a need-to-know
9 determination. An authorized holder of classified information
10 has certain duties. So it is not simply the originating
11 agency, if that's the distinction that the court is drawing,
12 it is any authorized holder of classified information.

13 The Obama administration has put out several
14 policy statements, which we cited in our brief, on this
15 statement explaining the importance of the duty of holders of
16 authorized information to challenge the classification status
17 if they disagree with it in good faith.

18 The regulation on this --

19 MJ [COL POHL]: But it is your position that because you
20 all have clearances and a need to know, that you have
21 authority -- or, excuse me, maybe even an obligation ----

22 MS. COHEN : Obligation.

23 MJ [COL POHL]: ---- to go back to the OCA and say this

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 is improperly classified, why is this classified? You believe
2 that's your position?

3 DC [MR. CONNELL]: If we in good faith believe that the
4 classification status is improper, we have an obligation to do
5 so. Let me tell the court how this comes up. This generally
6 does not come up with there is a new secret weapon X and we
7 don't think it should be classified.

8 It comes up when someone else has done a
9 derivative marking, which is what happened in AE 52. The
10 government did a derivative marking of AE 52. That's the only
11 challenge that I ever brought, because when I read it I
12 thought, there is nothing classified in this document; I have
13 a duty to challenge it. And so that's how I attempted to do
14 my informal classification challenge.

15 MJ [COL POHL]: You challenged it with who, the OCA or
16 the government?

17 DC [MR. CONNELL]: Ultimately the OCA through an
18 intermediary. In fact, the regulation is that 32 CFR 2001
19 .14, which is the regulation of the security oversight
20 officers on classification challenges.

21 MJ [COL POHL]: So if you are correct on that, then you
22 already established a procedure to do it. Why are you asking
23 me to do something different?

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 DC [MR. CONNELL]: Because it was an extraordinary
2 effort on behalf of the security officer involved. It was not
3 part of her normal duties, and I very much appreciate her
4 assistance.

5 MJ [COL POHL]: Somebody else does extraordinary effort.

6 DC [MR. CONNELL]: A lot of us do extraordinary effort.

7 MJ [COL POHL]: I am saying if you have somebody who can
8 currently do it, why somebody else? I am not disputing this.
9 I am just trying to figure out, you say you did this once
10 before, so you know how to do it. You had somebody who could
11 do it.

12 DC [MR. CONNELL]: No, Your Honor. Do you remember what
13 I said yesterday on this point? I know a lot of people said
14 everything ----

15 MJ [COL POHL]: I remember some of what was said, yes.
16 If you wish to refresh my memory, proceed.

17 DC [MR. CONNELL]: My classification challenge was
18 rejected because it was not brought in the proper forum. And
19 when I asked what is the proper forum, I couldn't receive any
20 answer about what is the proper forum. There really does need
21 to be a person in whose bailiwick this issue is.

22 MJ [COL POHL]: That's simply a defense -- what you are
23 asking, what it appears to me on that issue, you are asking

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 for procedures, how do I challenge. You believe you have the
2 right to challenge the classification of a document.

3 DC [MR. CONNELL]: Yes.

4 MJ [COL POHL]: You have a document that is classified.

5 DC [MR. CONNELL]: Yes.

6 MJ [COL POHL]: I am holding a piece of paper that's not
7 classified. But for the sake of discussion, you have a
8 document that you believe is classified. You believe it
9 shouldn't be classified, for whatever reason. You want to
10 know how you challenge the classification.

11 DC [MR. CONNELL]: I have a piece of paper that is
12 marked as classified ----

13 MJ [COL POHL]: Exactly, I've got you. It's marked as
14 classified and you can't understand why it is classified.

15 DC [MR. CONNELL]: Right.

16 MJ [COL POHL]: So you want to challenge that.

17 DC [MR. CONNELL]: Correct.

18 MJ [COL POHL]: You believe you can. I believe
19 Ms. Baltes has a contrary view, but that's okay.

20 DC [MR. CONNELL]: It's not what they wrote in their
21 brief.

22 MJ [COL POHL]: We will get there. Now you want a
23 mechanism for doing that. There is nothing in place that

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 permits you to do that.

2 DC [MR. CONNELL]: In the attachments to 13 are e-mail
3 after e-mail from me asking about how these processes work,
4 how do I accomplish these processes.

5 MJ [COL POHL]: What's the answer you get?

6 DC [MR. CONNELL]: Silence.

7 MJ [COL POHL]: Silence or no, you can't challenge it?

8 DC [MR. CONNELL]: Silence.

9 MJ [COL POHL]: Who do you send these e-mails to?

10 DC [MR. CONNELL]: The Convening Authority.

11 MJ [COL POHL]: Okay, I got you.

12 DC [MR. CONNELL]: I will move on unless the court has
13 more questions about that.

14 MJ [COL POHL]: No, I'm good.

15 DC [MR. CONNELL]: If we can move to the slides, please,
16 Colonel.

17 Just as a refresher from yesterday, go to the next
18 slide, please. Thank you. It strikes me that we are really
19 trying to answer three questions here: What role for the
20 adversarial process; what information is actually classified;
21 and how can we both protect national security and create a
22 safe harbor?

23 There has been bleed-over, but this is the second

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 of ten motions in this hearing that address this question. So
2 let's come to what I want to identify. Here are the five
3 problems at large that I see with the protective order that we
4 haven't already discussed.

5 The first is the procedure for the invocation of
6 classified information privilege or ex parte filings.

7 The second is the definition of classified
8 information.

9 The third is the procedure for a need-to-know
10 determination.

11 The fourth is the lack of meaningful guidance or
12 any safe harbor for the defense.

13 And the fifth is the procedure for closing
14 hearings.

15 There has been a lot of discussion of does
16 classification end the inquiry, what happens after that. Most
17 of that discussion has taken place in the context of closure
18 of a hearing. But there is another piece of it as well, which
19 is the invocation of the classified information privilege.

20 Now, the government made a remarkable argument
21 that Reynolds v. United States does not govern --

22 THE INTERPRETER: Your Honor, the interpreter is not
23 able to keep up.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 DC [MR. CONNELL]: Thank you.

2 MJ [COL POHL]: We are going to move the buttons around,
3 because I am seeing it and you're not.

4 DC [MR. CONNELL]: Your Honor, my screen is blank.

5 MJ [COL POHL]: Okay.

6 DC [MR. CONNELL]: I have tried to tap it. See, I tap
7 it and nothing happens.

8 MJ [COL POHL]: I'm not vouching for technology. We
9 will try to address that at the break, but mine apparently is
10 working and that's why -- why, when I say "slow down," that's
11 what I am saying.

12 But go ahead, back to the government's remarkable
13 assertion.

14 DC [MR. CONNELL]: The remarkable assertion is that
15 Reynolds v. United States does not have anything to do with
16 Rule 505. I think the drafters of Military Rule of Evidence
17 505 would be surprised to learn that because the discussion to
18 Military Rule of Evidence 505 says this rule is drawn from
19 Reynolds v. United States. Now, that bit of the discussion
20 did not make it into MCRE 505, it's in Military Rule of
21 Evidence 505, but MCRE 505 is drawn in substantial part from
22 Military Rule of Evidence 505. We cited the specific language
23 in our brief.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 Reynolds establishes, which is the fountainhead of
2 all government information privilege, it became both 505 and
3 506 in the Military Rules of Evidence, has four elements for a
4 claim of privilege: A formal claim lodged by the head of the
5 department or agency after actual personal consideration of
6 the matter and in a classified information privilege ascribing
7 the danger to national security. Slightly different for other
8 government information privilege.

9 MJ [COL POHL]: You have a variation of that theme in
10 505(c), you would agree?

11 DC [MR. CONNELL]: Exactly right. That language in
12 505(c) is drawn from Reynolds.

13 MJ [COL POHL]: Again, it's not the exact same language
14 out of Reynolds, but one certainly could infer the Reynolds
15 requirements, what that language is.

16 DC [MR. CONNELL]: There is a variation off it as well
17 in 505(f)(1)(A). There are two different places in 505 that
18 this Reynolds language in, as you say, in slightly changed
19 form has made it into 505. One of those is the general
20 invocation of classified information, in 505(c); and the other
21 one is, as the court referred to earlier, the specific
22 invocation of classified information, the privilege with
23 respect to specific information which would trigger the

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 substitution.

2 MJ [COL POHL]: Mr. Connell, why are we discussing the
3 invocation of privilege when the government's position is that
4 has got nothing to do with the protective order?

5 DC [MR. CONNELL]: Well, it is because they are
6 mistaken. That's the position they take today. They didn't
7 file a reply about it or anything. They have invoked the
8 classified information privilege for these two -- for
9 declaration A and B, the attachment to their AE 13. They have
10 submitted ex parte declarations for which they have claimed
11 the classified information privilege. That's what we are here
12 discussing. We briefed it extensively in 13 Golf.

13 MJ [COL POHL]: Is this a privilege question or simply a
14 classified, how to handle classified information in the
15 context of your pretrial preparation?

16 DC [MR. CONNELL]: Those two questions are the same
17 question. They are very much intertwined.

18 MJ [COL POHL]: Do you believe that a document that's
19 labeled with a security classification requires an additional
20 invocation of some privilege before it would trigger any type
21 of protective order?

22 DC [MR. CONNELL]: Absolutely it does.

23 MJ [COL POHL]: So let me see, I want to make sure I

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 understand your position.

2 DC [MR. CONNELL]: Well, I am trying to explain it.

3 MJ [COL POHL]: You seem to be taking -- you are saying
4 that whenever a document that on its face is properly
5 classified, excuse me, is classified ----

6 DC [MR. CONNELL]: Is marked as classified.

7 MJ [COL POHL]: ---- marked as classified, that the
8 government has the responsibility to go through the privileged
9 invocation process on that document before it is properly
10 what?

11 DC [MR. CONNELL]: No, that's not our position. Our
12 position is if a document is marked as classified, whether I
13 believe it should be classified or not, whether it is marked
14 as classified, that invokes all of the restrictions I am
15 subject to as a government employee.

16 MJ [COL POHL]: I got that. I am trying to figure out
17 where you believe the privileged part is.

18 DC [MR. CONNELL]: That is before the government can
19 withhold information from the court or from the defense, they
20 have to invoke classified information privilege.

21 MJ [COL POHL]: Is that what we are talking about here?

22 DC [MR. CONNELL]: Yes, with declaration A and B.

23 MJ [COL POHL]: No, but what I am saying is I don't

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 disagree that there is a procedure that the government can
2 employ to prevent relevant, arguably relevant information to
3 go to the defense by invoking a privilege. Okay, I am being
4 very generic here. I got that. Okay. But that's not what we
5 are talking about here today.

6 What we are talking about here today is a proposed
7 protective order of how, defining what is classified
8 information and how it should be handled, regardless of the ex
9 parte declarations. Let's say they weren't even included.
10 This is saying if you get a piece of paper that you know or
11 have reason to believe is classified, here is how you handle
12 it.

13 DC [MR. CONNELL]: Your Honor, and the reason why --
14 there are two reasons why this is the place for the argument.
15 The first is that the government's entire argument is based on
16 its attachments A and B to 13 and which are ex parte, which is
17 seeking to invoke the privilege, the privilege that the
18 defense don't get to see it.

19 But the second is, in paragraph 36 of our proposed
20 protective order, we set forth a -- we propose the way that
21 this should take place. Colonel, could you skip to slide 15,
22 please? I will pull it up for you, Your Honor.

23 MJ [COL POHL]: I got it.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 DC [MR. CONNELL]: Can we go back to slide 10, please.

2 [No audio.]

3 MJ [COL POHL]: I will tell you, it slides sometimes, so
4 just tell me if you can't hear it.

5 My point is, the 505 procedures I don't believe
6 are what is before me now. Do you believe they are before me
7 now?

8 DC [MR. CONNELL]: The government has language in its
9 proposed protective order essentially modifying and restating
10 the 505 procedure. What we are trying to do, and so that's
11 how they believe 505 procedure gets implemented and they want
12 that to become the law of the case. I have a different view
13 of how 505 procedure gets implemented, and I am trying to have
14 my version represented in the protective order.

15 MJ [COL POHL]: Again, it is kind of what I said earlier
16 about as we debate your two protective orders through exhibit
17 after exhibit, if the protective order does not address the
18 final version, if any, it doesn't address 505, because I have
19 concluded that that's a separate issue altogether, then we
20 don't really need to have this discussion.

21 DC [MR. CONNELL]: Correct. If the court says -- if the
22 court says, "Mr. Connell, I am not adopting the 505 paragraphs
23 from the prosecution. We are going to have a different

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 hearing on that a different day, so we can focus on that
2 exclusively," then if you say that to me, we skip ahead.

3 MJ [COL POHL]: I will tell you what, for now skip
4 ahead. If, in the order that comes out, you think I didn't do
5 what I intend to do at this point in time, we will revisit it.
6 But I don't think that's the issue before me; that's all I'm
7 saying.

8 DC [MR. CONNELL]: So the only thing left to say about
9 that topic, Your Honor, is -- and if you could skip to slide
10 19, please -- whether the court is going to grant the relief
11 that the government seeks in its AE 13 attachment Foxtrot, the
12 government argues that the Military Commission should seal its
13 two declarations, attachment A and B, and because it has
14 successfully invoked classified information privilege.

15 And our position, which we document at great
16 length in 13 Golf, is that they have not successfully done so.
17 That's where the Ellsberg compliance comes in, and that's our
18 paragraph 36, which makes the situation Ellsberg-compliant.

19 Now, I do want to digress for a second and address
20 a question the court asked yesterday. The court asked
21 yesterday, people are citing to me all kinds of things, all
22 kinds of authorities all the time. There are two federal
23 courts that are in the chain of review for this court.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 Obviously there is the CMCR first and then the D.C. Circuit
2 and then the Supreme Court. My position is that the Supreme
3 Court of the United States and D.C. court are the most
4 authoritative courts. If they haven't addressed an issue,
5 which is why we cited *Ellsberg v. Mitchell*, the D.C. case on
6 the classification of information privilege, just like any
7 other forum, if there is not binding authority, then other
8 jurisdictions may be persuasive.

9 MJ [COL POHL]: Mr. Connell, I did not mean to minimize
10 that. If we are going strictly on black-letter law, as of
11 yesterday three appellate decisions have addressed
12 commissions, so it is not there is a whole library of
13 decisions, so almost everything is going to be by analogy or
14 interpretation. I got that. You were moving around so
15 quickly from the Navy to some other court, but that's okay. I
16 understand, that's the nature of this procedure. I got it.

17 DC [MR. CONNELL]: Okay. So I will leave independent
18 invocation of class information privilege now on the
19 Commission's representation. But I don't want to leave that
20 point without saying that if the court grants attachment F,
21 the relief that the prosecution seeks there, it is honoring an
22 invocation of classified information privilege which we
23 extensively briefed as to how the government has not done that

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 correctly.

2 Our brief itself is classified, so I am trying to
3 dance around the specific arguments.

4 MJ [COL POHL]: I got it.

5 DC [MR. CONNELL]: Just so it is specifically clear, I
6 know there was a problem with the court getting its copy of
7 13 Golf, because there is always a problem with transmitting
8 information, but the court has its copy and if there are any
9 problems with the issues, let me know.

10 So let's move to the next slide, please. This is
11 the issue that got addressed by some of the parties earlier.
12 And all of the problems with paragraph 7 can be solved by
13 using the definition of classified information that Congress
14 provided and the Secretary of Defense provided.

15 In fact, it's my suggestion that the Military
16 Commission is not really at liberty to come up -- to adopt the
17 government's decision. MCRA 505(b)(1) defines classified
18 information as any information or material that has been
19 determined by the United States Government pursuant to an
20 executive order, statute, or regulation to require protection
21 against unauthorized disclosure for reasons of national
22 security and any restricted data, as defined in 42 U.S.C.
23 2014(y). This is the one definition which Congress provided

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 in the Military Commissions Act which is different from
2 similarly defined terms in the executive order.

3 It's our position, which we put in our protective
4 order, that the Military Commission should use the definitions
5 in the executive order except for where Congress has provided
6 otherwise. This is the one place that Congress has provided
7 otherwise.

8 The Secretary of Defense in MCRE in 505 B 1 is not
9 the first to use this definition. This is the same definition
10 that appears in the Military Commissions Act at 949 -- excuse
11 me, 948 Alpha (2). It also appears in the Rule for Military
12 Commission 103 sub 7. It is the same definition in CIPA
13 Section 1(a) and as well as appearing in the Military
14 Commissions Rule of Evidence.

15 The government's proposed protective order,
16 however, far exceeds this. Now, at various times the court
17 has asked could I solve this problem by just putting in the
18 word "classified." If what the court means is can the court
19 solve the problem by limiting the information to actually
20 classified information? Yes. But that means that our
21 definition of classified information then would then say
22 classified information is defined as the following classified
23 information, which would become redundant and not very helpful

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 to the parties.

2 The starting point the court indicated earlier is
3 whether something is marked classified or not, and I couldn't
4 agree more, but the -- if the court adopts the definition that
5 Congress provided and the Secretary of Defense provided, then
6 it solves all of these problems. It then moves the problem to
7 how do we know what is classified, which is the problem of
8 meaningful guidance and the problem of the defense security
9 officer.

10 I do want to address a new argument that we have
11 never heard before today, which is that the government argued
12 yesterday and again today that the protective order places no
13 restrictions on the accused themselves. I found this to be a
14 fascinating argument. And if that's true, it certainly should
15 be in the protective order. I have a proposed language about
16 that, but if that's true, if that's their position, it should
17 be in the protective order.

18 But in that situation there would no longer be
19 505(g) notice because if the defendants were going to testify,
20 they could simply testify. And if what they have to say isn't
21 classified, then it can be broadcast, 40-second delay or no
22 40-second delay, because the protective order doesn't put any
23 restrictions on the accused, as I understand it.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 In that case, it makes the defense function very
2 awkward because in fact what they really need is ----

3 MJ [COL POHL]: That bell had nothing to do with us --
4 go ahead -- to my knowledge.

5 DC [MR. CONNELL]: I thought the translators had really
6 gotten sick of me.

7 MJ [COL POHL]: No. They will turn the lights off,
8 then.

9 Go ahead. I'm not sure that that's what she
10 meant, but --

11 DC [MR. CONNELL]: What did the Commission understand
12 her to mean by that?

13 MJ [COL POHL]: She was talking about the -- the
14 protective order covers what it covers, i.e., the attorneys,
15 okay?

16 DC [MR. CONNELL]: Well, if Mr. al-Baluchi testifies,
17 for example -- I'm not vouching for anything. If he
18 testifies, if the protective order doesn't cover him, then I
19 don't really have to give 505(g) notice because nothing he has
20 to say is classified.

21 MJ [COL POHL]: That's not what she said. Okay, I
22 believe you're misunderstanding. Go ahead with the current
23 practice of the 505(g) notice and if it turns out it's not

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 classified, we will take care of it. I don't think that's
2 what she said and I would be very surprised that's what she
3 meant, but I understand your position on that, but let's --

4 Let me ask you this: In paragraph 7, assuming we
5 add the word "classified" ahead of the word, after the word
6 "any" in paragraph 7(f), isn't this just kind of a form of a
7 classified guidance for you? I'm saying you talk about the
8 definition of classified here. I have got that. This is just
9 simply saying this information is classified.

10 DC [MR. CONNELL]: That's the proper function of the
11 classification guide, to tell us what is classified.

12 MJ [COL POHL]: Isn't this a variation of that theme?

13 DC [MR. CONNELL]: It's a variation of that theme and I
14 have said the same thing myself before, but it is not an
15 effective or authorized variation of that theme. Let me show
16 you a couple of examples.

17 So in subparagraph A, for example, it allows
18 classification outside the scope of the executive order. It
19 says information classified in the interests of national
20 security or of the executive order.

21 In subsection B it makes information classified if
22 it is derived from classified information, regardless of
23 whether that actual -- the information is actually classified.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 Let me give you an example that affects my life enormously in
2 this situation.

3 There is a classified document that contains my
4 client's date of birth. Under this definition, if I were to
5 refer to his date of birth in an unclassified setting, then
6 that would be information derived from classified information,
7 regardless of its actual classification.

8 MJ [COL POHL]: Does that strike you as a strange
9 result?

10 DC [MR. CONNELL]: It does strike me as very strange.

11 MJ [COL POHL]: So let me say I got your position. Just
12 so I understand it, a piece of information, date of birth, is
13 classified.

14 DC [MR. CONNELL]: I am not saying it's classified. I
15 am saying it appears in a document marked.

16 MJ [COL POHL]: This is an example. When you put it in
17 a brief it's now, you don't believe it should be classified,
18 is that your -- I am trying to figure out what your position
19 is here ----

20 DC [MR. CONNELL]: My position is that, and this is not
21 just my position ----

22 MJ [COL POHL]: ---- if you start with a piece of
23 classified information.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 DC [MR. CONNELL]: ---- it's not classified information.

2 MJ [COL POHL]: Then why are we talking about it?

3 DC [MR. CONNELL]: Because it appears in a document that
4 is marked classified. That doesn't mean that every piece of
5 information in a document is actually classified. That's what
6 an original classification authority does and that's why we
7 need classification guidance, which pieces of information in
8 this document are classified and which are not.

9 MJ [COL POHL]: Because they are labeled by paragraph.
10 Okay, I got it.

11 DC [MR. CONNELL]: And lots of times -- we have had
12 examples in this case. For example, I sent a classified
13 request for information to the prosecution. They changed one
14 word and sent it back to me unclassified. Now, that's because
15 I am sure they have a person in their office who can tell
16 them, well, if you take out that word and you change it to a
17 different word, then it's unclassified. We don't have any
18 equivalent of that.

19 MJ [COL POHL]: But isn't that a governmental function,
20 though?

21 DC [MR. CONNELL]: And I work for the government, sir.

22 MJ [COL POHL]: I know you get paid by the government.
23 I know you work for the government. But what I am saying is

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 you are not the stakeholder in classified information.

2 DC [MR. CONNELL]: That's right. That's why we need
3 some access to the stakeholder.

4 MJ [COL POHL]: My point is that if you had somebody
5 working in your office who says take that word out, but nobody
6 in your office is a stakeholder, whereas the government is the
7 stakeholder, so therefore by them taking the word out they
8 have either changed, clarified the classification issue, or in
9 some ways -- I know this is not the right term, so don't jump
10 down my throat on it, in essence declassified the document
11 because the big G is the stakeholder.

12 If you had somebody assigned to your office who
13 did the exact same thing, okay, could you say with any
14 confidence therefore the document now is no longer classified?
15 And the answer is no. That's a rhetorical question. The
16 answer is no, because you're not the stakeholder.

17 DC [MR. CONNELL]: The rhetorical question has an
18 improper premise. The OCA is the stakeholder.

19 MJ [COL POHL]: I understand that.

20 DC [MR. CONNELL]: They have someone in the offices who
21 can liaise with the OCA and say OCA, if we take this word out,
22 will it be unclassified? They say yes, and then they take it
23 out and it can come back properly. That's what I am asking

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 for, some way to liaise with the OCA. The prosecution is not
2 the OCA, whatever government agency is the OCA. I am asking
3 for some pipeline in the same way.

4 MJ [COL POHL]: Okay.

5 DC [MR. CONNELL]: I know the court is going to produce
6 sort of a draft document and we are going to comment on it,
7 but let me propose --

8 MJ [COL POHL]: Just to be clear. What I propose is not
9 a draft. What I will produce will be the applicable document
10 until changed.

11 DC [MR. CONNELL]: An interim document perhaps or
12 tentative.

13 MJ [COL POHL]: Might be, might not be. No, it's a
14 final document subject to amendment. Just be clear, it's not
15 going to be sent out, here is a draft you guys, comment and
16 come back. It will be here is my -- here is my protective
17 order, but I will reconsider if counsel wish me to. That's
18 what it is.

19 I just want to make sure it's not going to be a
20 draft to be circulated and we come back two months from now
21 and discuss what it is, because there will be a protective
22 order. If I issue one -- well, I will issue a protective
23 order and that will govern the case until that protective

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 order is changed.

2 DC [MR. CONNELL]: Understood, sir. And just so my
3 position is clear, and I don't speak for anybody else on this,
4 my position is we need a protective order, which is why I have
5 proposed one and why it's important.

6 Here is what we propose as the definition of
7 classified information. And let me tell you, if I could
8 direct the Commission to the bottom of the slide which is
9 definition T out of 6. -- Section 6.2 out of executive
10 order -- no, sorry, please go back one. The definition, the
11 executive order, and this is the bottom paragraph, T, defines
12 information, and many of the problems that all the different
13 parties have talked about have come from ignoring this
14 executive definition of information. And the information is
15 any knowledge that can be communicated or documented material,
16 regardless of its physical form or characteristics, that is
17 owned by, is produced by or for, or is under the control of
18 the United States Government.

19 The owned by, produced by, or under the control of
20 the United States Government language is so integral to the
21 executive order understanding of classification that it
22 appears in the definition, not just the word "classified" but
23 the word "information" itself.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 So if we -- we would solve a lot of problems with
2 the protective order if the court were to adopt the definition
3 of information that the precedent has provided.

4 MJ [COL POHL]: If I adopt that, does it change
5 anything?

6 DC [MR. CONNELL]: Yes. If we could move on to slide 27
7 I will show you what I mean. The thing that it changes is the
8 understanding of the accused's statements. Now, the court
9 told me that my understanding of the government's argument was
10 not correct, but the government's argument, summarized here,
11 this comes from their brief.

12 MJ [COL POHL]: I didn't say it was necessarily not
13 correct. Well, if I said that, it is not what I meant. What
14 I said was I would be surprised if that was their argument.

15 DC [MR. CONNELL]: Fair enough. Fundamentally, the
16 government's argument is because the accused participated in
17 the CIA program they were exposed to classified sources and
18 activities due to their exposure, due to classified
19 information, the accused are in a position to disclose
20 classified information publicly through their statements.

21 This is the classification by euphemism that the
22 definition of information addresses. If we actually use the
23 precedence definition of the word "information," it has to be

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 information owned by the government, and the government
2 doesn't own people after the 13th Amendment. It has to be
3 produced by or for the government, which is not the case here.

4 That brings us to control. The argument that the
5 government made was that it controls this information because
6 it holds the defendants in a location and it restricts their
7 access to people with -- they said restricts their access to
8 their attorneys, which is not precisely correct because
9 certainly there are people other than attorneys who visit from
10 the defense.

11 But one fundamental flaw with that reasoning is
12 that it's not in fact true that the government restricts the
13 communications of the defendants to people with security
14 clearances because of the ICRC. The government allows the
15 detainees to communicate with their families, the ICRC through
16 restricted means, and with the ICRC themselves.

17 MJ [COL POHL]: Are they unfettered communications with
18 no government agents listening to them?

19 DC [MR. CONNELL]: Can I answer that question in this
20 form, Your Honor?

21 MJ [COL POHL]: Answer it in any form you feel
22 comfortable in answering it, because I understand what you are
23 saying, but it seems to me, it strikes to me is --

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 DC [MR. CONNELL]: The answer to that question is
2 classified, to my understanding.

3 MJ [COL POHL]: Then don't answer it.

4 DC [MR. CONNELL]: That's what I was asking.

5 MJ [COL POHL]: I understand. When we go to this kind
6 of colloquy and you think it may be a classified answer, just
7 say that.

8 DC [MR. CONNELL]: All right.

9 MJ [COL POHL]: We don't need to be more opaque than
10 that. I got it. Continue on with what you are saying and we
11 will move on.

12 DC [MR. CONNELL]: As I understand it, communication
13 with the ICRC itself is unfettered.

14 MJ [COL POHL]: Okay.

15 DC [MR. CONNELL]: It is not in fact true that --
16 assuming that is the kind of control that the executive order
17 was talking about, which I dispute, but assuming -- because
18 that's the kind of control that the Bureau of Prisons
19 exercises over 200,000 people. Simply holding someone in
20 custody does not mean that you control their thoughts and
21 their experiences and their observations.

22 The thoughts, observations, and experiences
23 question, in my mind, is resolved by the definition of

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 information in the executive order because of the control,
2 production or ownership requirement.

3 MJ [COL POHL]: So at the end of the day, the issue is
4 do they fit any of those four categories.

5 DC [MR. CONNELL]: Three categories, yes.

6 MJ [COL POHL]: Three categories. And the government
7 says we basically control them now and therefore we can
8 restrict their communication of classified material.

9 DC [MR. CONNELL]: Yes.

10 MJ [COL POHL]: And your position is?

11 DC [MR. CONNELL]: Our position is --

12 MJ [COL POHL]: Not under control?

13 DC [MR. CONNELL]: The information is not under control,
14 no, sir, because that's what we are talking about is
15 information. It is not whether the physical body of a person
16 is under control. The government can't stop me by sticking me
17 in handcuffs and putting me in a room.

18 MJ [COL POHL]: They can stop you from talking to who
19 you are talking to, isn't that the position? Someone can be
20 in a cell and babble, talk anything they want, that's not the
21 issue. The issue is do they communicate that outside that
22 cell.

23 DC [MR. CONNELL]: Which is the point that I was making

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 earlier, that even if that's the standard, that it's not ----

2 MJ [COL POHL]: I'm not saying standard, just trying to
3 figure out what "control the information" means.

4 DC [MR. CONNELL]: Let me give you an example of
5 information that's controlled. We know restricted data is
6 restricted information, so a person who works on nuclear
7 secrets is controlled by a nondisclosure agreement.

8 MJ [COL POHL]: But as discussed earlier, that would be
9 somebody in privity with the government. Give me an example
10 of somebody who doesn't fall in that category, privity with
11 the government, who signed stuff, like I am sure you guys have
12 had to, that would be in control of the government for these
13 purposes.

14 DC [MR. CONNELL]: The Invention Secrets Act. There is
15 a third way that information can become classified. One is by
16 executive order, one is by restricted data, and the third is
17 the Invention Secrets Act, and that is if I invent a widget
18 and I can do anything I want with that widget. I can post on
19 the Internet how to make such a widget. I can hand out and
20 make the widgets and hand them out to all my friends.

21 But if I apply for a patent, then the government
22 gets to review my patent and say, "I'm taking your widget and
23 now your widget is going to be classified." It's only if I

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 applied for a patent. I am not in privity with the government
2 in any way.

3 MJ [COL POHL]: But applying for a patent you become at
4 least contractually related to the government. You want the
5 government to protect your invention.

6 DC [MR. CONNELL]: A patent is not a contractual
7 relationship with the government because otherwise I could
8 enforce my patent against the government as opposed to
9 enforcing it against another.

10 MJ [COL POHL]: You ask the government to perform an
11 official function to protect your patent.

12 DC [MR. CONNELL]: A registry, yes.

13 MJ [COL POHL]: I got that. What I am saying is that
14 you guys, a detainee or an individual who has access to
15 classified information who is under the control of the United
16 States Government, who can control who that detainee or
17 individual communicates with is not under the control of the
18 government.

19 DC [MR. CONNELL]: I am saying their attorneys are not
20 under the control of the government. Clearly Mr. al-Baluchi
21 himself is under the control of the government. I am not
22 saying ----

23 MJ [COL POHL]: You are saying the government has no

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 right to control what Mr. al-Baluchi communicates to any
2 third-party who has no clearance.

3 DC [MR. CONNELL]: That's a law-of-war question. The
4 law-of-war question is whether they get to control whether he
5 communicates with different people. But I am saying they
6 don't have any right to classify that information because the
7 government's right to classify things comes exclusively from
8 the Executive Order, the Registered Data, the Nuclear Secrets
9 Act and the Inventions Secrecy Act.

10 MJ [COL POHL]: I don't think we are talking about
11 inventions here.

12 DC [MR. CONNELL]: You led me down that path before.

13 MJ [COL POHL]: Well, you chose the invention path, but
14 that's okay. What I am saying is if Mr. al-Baluchi has access
15 to classified information due to his experiences, whatever
16 those be, you are saying that he does not meet this definition
17 under control and therefore the information is not classified,
18 or he is under no restriction as to his ability to disseminate
19 said information?

20 DC [MR. CONNELL]: Well, physically he is clearly under
21 restrictions. It is that the information is not classified
22 which is why we are talking about this in the context of a
23 protective order.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 MJ [COL POHL]: The information itself you are saying is
2 not classified. Therefore, if he could talk to somebody he
3 could tell it to them without --

4 DC [MR. CONNELL]: Say the ICRC. He could tell them.
5 They could write a report.

6 MJ [COL POHL]: But your basic premise is it's not
7 classified.

8 DC [MR. CONNELL]: Correct.

9 MJ [COL POHL]: I got it.

10 DC [MR. CONNELL]: Next slide, please.

11 There are two other -- in addition to the
12 ownership, production and control, there are two other reasons
13 why nongovernmental RDI information is not classified. We
14 talked about the first one a lot, but the second one is the
15 authorized disclosure idea. And that, in fact, refers to our
16 AE 34, which is our request for the production of
17 Mr. Rodriguez, who would testify that this information was
18 provided to the detainees in an authorized fashion, that it
19 wasn't unauthorized, that it was done -- this was an
20 authorized disclosure of information to the detainees. That's
21 public source information. He has written a book about it. I
22 just quoted from his book.

23 But these sort of third parties -- so let's talk

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 about a different type of third-party for a moment, because
2 the court raised the question about third parties earlier.
3 Let's talk about a farmer. The government is operating flying
4 classified vehicle X in country Y and classified vehicle X
5 crashes in a field, right, and the farmer in country Y goes
6 out and looks at it, sees what color it is, sees how long it
7 is, sees what kind of fins and guns it has on it. That farmer
8 is not -- the observation, experiences of that farmer are not
9 classified.

10 Now, they might have to be controlled in a certain
11 way if a -- then a member of the United States Army goes out
12 and talks to that farmer and gets the information; the notes
13 that the U.S. Army representative wrote down can be controlled
14 by the government because they are under a nondisclosure
15 agreement.

16 MJ [COL POHL]: Would he be considered under the control
17 of the government?

18 DC [MR. CONNELL]: The farmer?

19 MJ [COL POHL]: Yes.

20 DC [MR. CONNELL]: No.

21 MJ [COL POHL]: If a detainee is released from
22 Guantanamo Bay and goes back to his home, wherever that may
23 be, is he under the control of the United States

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 Government ----

2 DC [MR. CONNELL]: No.

3 MJ [COL POHL]: ---- or covered by any protective order
4 in their case?

5 DC [MR. CONNELL]: I don't know, Hamdan may be coming
6 back and he has been released.

7 MJ [COL POHL]: I have my suspicions that we won't see
8 Mr. Hamdan again, but that's neither here nor there.

9 DC [MR. CONNELL]: You could see the case again.

10 MJ [COL POHL]: Let's say we have a detainee and some
11 have just been released without strings and they may have been
12 exposed to classified information, are they, does that make
13 the information now not classified or they have no obligation
14 not to disclose it? It is a double negative but you
15 understand my question I hope.

16 DC [MR. CONNELL]: I do. And the distinction I want to
17 come back to is, is the distinction between control of a
18 person and control of observations, experiences and memories
19 of a person, that in a free society we don't control people's
20 memories, their thoughts, their observations, their
21 experiences. We control a number of people's physical bodies,
22 not just in Guantanamo, but across the United States. People
23 are incarcerated under government control.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 MJ [COL POHL]: Control of information, not bodies.

2 DC [MR. CONNELL]: Your question was people who have
3 been released or the farmer in his field. The operative
4 distinction is that those people are not figures strictly
5 under United States control, the operative distinction is
6 their operations or experiences are not under government
7 control. My operations and experiences are under government
8 control.

9 MJ [COL POHL]: Is that because the information was
10 disclosed voluntarily by the government?

11 DC [MR. CONNELL]: Not in a crash situation.

12 MJ [COL POHL]: So what I am saying is if individuals
13 stumble across a classified document -- for example, there
14 have been examples of where classified documents have been
15 found or a disk has been found by somebody, that doesn't make
16 that information less classified, does it?

17 DC [MR. CONNELL]: In that person's hands it means that
18 the information is unclassified with respect to them. I am
19 fully on board with the idea the information can be classified
20 when I say it and not classified when a New York Times
21 reporter says it. I get that.

22 MJ [COL POHL]: I'm sorry, I'm sorry, let me see if I
23 got this straight and then we are going to take a recess for

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 lunch.

2 It is your position that a piece of classified
3 information that comes in the hands of a member of the media,
4 okay, loses its classification protection because he is not --
5 that's what you just said?

6 DC [MR. CONNELL]: It's the opposite. It never acquires
7 it in the first place. Let me give you an example. It --

8 MJ [COL POHL]: I want to finish on this point. I
9 believe you may get a remarkable -- you just said a piece of
10 information that comes into the hands of The New York Times is
11 no longer classified. That was a blanket statement you just
12 said.

13 DC [MR. CONNELL]: Right. Let me tell you what I mean,
14 because I think you are talking about leaks and I am not. The
15 name of a country where a detainee was held under the
16 classification guidance is classified when I say it. Right?
17 Country X, the identity of country X is classified if I say
18 it.

19 If a politician from country X says it, if a
20 reporter says it, if my second cousin says it, none of those
21 people are under nondisclosure agreements. When they say the
22 name of country X, it is not classified to them. It has been
23 explained to us over and over and over again, in fact to me it

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 seems to be the government's number one concern, is that if I
2 say the name of country X, it's classified; when somebody else
3 in the public says it, it's not classified.

4 MJ [COL POHL]: Isn't that part of the theme of
5 verifying information in the public domain? And that is the
6 concern, if it comes from somebody in a position to know that,
7 therefore it is inferred that the United States Government is
8 verifying the information as opposed to a third-party who says
9 there is a secret facility in country X? You don't see a
10 distinction between those two things?

11 DC [MR. CONNELL]: I do, and I put that in our
12 protective order because if I endorse or verify the
13 information, my client says that -- let me say country X has a
14 black site and I know that to be true.

15 MJ [COL POHL]: I know I was promising to quit, but I am
16 curious about this point, but does that then make that
17 information unclassified as opposed to there is no sanction
18 against that third-party?

19 DC [MR. CONNELL]: The name of country X is unclassified
20 and it is unclassified when somebody who is not under a
21 nondisclosure agreement to the United States Government says
22 it. When I say it, it's classified.

23 MJ [COL POHL]: Okay. I think I understand what you are

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 saying.

2 Let's go ahead and we will break for lunch and
3 reconvene at 1330. The Commission is in recess.

4 [The Military Commission recessed at 1230, 17 October 2012.]

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 [The Military Commission was called to order at 1335,
2 17 October 2012.]

3 MJ [COL POHL]: Please be seated. The Commission is
4 called to order. All parties again are present that were
5 present when Commission recessed.

6 Mr. Connell.

7 LDC [MR. CONNELL]: Thank you.

8 TC [MR. SWANN]: Housekeeping, you asked about
9 Mr. Bin'Attash. We went back to Mr. Bin'Attash at the camp.

10 DC [CDR RUIZ]: I cannot hear the prosecutor.

11 TC [MR. SWANN]: We went to the camp, asked
12 Mr. Bin'Attash if he wanted to attend -- went to the camp,
13 asked if Mr. Bin'Attash wanted to come. He indicated that he
14 did not want to come. I have informed his counsel, offered
15 them a copy of the document again. Should you make any
16 inquiry, that is all I have to offer at this time.

17 MJ [COL POHL]: Does counsel for Mr. Bin'Attash take any
18 issue about that?

19 LDC [MS. BORMANN]: No, Judge.

20 MJ [COL POHL]: It was kind of quiet on the record
21 there. The answer from the defense was "no."

22 Mr. Connell.

23 LDC [MR. CONNELL]: Thank you. One last observation to

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 make on this definition of information before I move on to
2 another subject. That's with the example that the court gave
3 me as we were closing. Is this on? Okay. This is me further
4 away from it, can everyone hear?

5 DC [CDR RUIZ]: Not too well.

6 MJ [COL POHL]: If you are looking at me for how to work
7 the microphone, Mr. Connell, it will be a long look. Try now.

8 LDC [MR. CONNELL]: Is that any better? Okay. The
9 example the court gave me just before the break, the
10 distinction between my naming country X as a host site, as a
11 host of a black site the president of that country naming
12 country X as a black site, is legal control, the third prong
13 of definition of information. Neither of us is in custody,
14 neither the president of the country nor I is in custody I'm
15 in privity with the government.

16 Nobody seems to believe me, but I work for the
17 government. But he is not, or she is not. But the thing I
18 want to make clear is that if the Commission adopts the
19 position that I, my position that I believe the executive
20 order requires, after the -- if the court adopted that
21 position, I could still not name country X, I'm still in
22 privity with the government, still under legal control, still
23 under the name country X.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 But the difference is that I can't explain the
2 fear, the humiliation, the pain my client was in as a result
3 of the United States Government actions. Those things are
4 currently classified -- I don't know if they're currently
5 classified or not. There's an argument from the government
6 they should be classified, but they cannot be under the
7 executive order. That is the same reason the fact people who
8 are not owned, produced or controlled by United States, the
9 same reason I'm not allowed to interview non-United States
10 witnesses overseas or anyplace not inside of a SCIF. It is
11 what that person has to say is not information.

12 Now, when I control the information I have to
13 reduce it to, I have to take appropriate security measures. I
14 have to reduce it to the security procedures of the United
15 States as fast as possible, as fast as reasonably possible, at
16 least.

17 The fact I interview someone in country X does not
18 have to take place in a SCIF because what they have to say is
19 not information as defined by the executive order.

20 MJ [COL POHL]: Let me ask you one question, the way you
21 started out, then go on to something else.

22 LDC [MR. CONNELL]: Yes.

23 MJ [COL POHL]: This may be a safe harbor argument, I

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 want to make sure. You have access to information that is
2 classified, that same information is released with no
3 declassification ----

4 LDC [MR. CONNELL]: Say that again, sir. I want to make
5 sure I follow.

6 MJ [COL POHL]: You have information that you know is
7 classified. That information appears in The Washington Post,
8 the same information.

9 LDC [MR. CONNELL]: Yes.

10 MJ [COL POHL]: Do you believe that as long as you cite
11 The Washington Post as the source of the information,
12 therefore you can disclose it at unclassified briefing?

13 LDC [MR. CONNELL]: This is a tricky situation. If I
14 endorse it or verify it or advocate for its truth in any way,
15 then it is classified, because I am adding something.

16 MJ [COL POHL]: If it is in one of your pleadings with
17 your name attached to it, since we are talking about it here,
18 if your name is attached to it, you said, "According to The
19 Washington Post, X occurred," can you do that under your --
20 again, I may be misinterpreting your safe harbor analysis.

21 LDC [MR. CONNELL]: If I'm implying that therefore it is
22 true, no. If I am stating it for the fact that it was said,
23 it is almost like a hearsay question. If I'm stating it for

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 the fact it was said, some sources have claimed that X, other
2 sources have claimed that Y, in that situation, I'm not adding
3 to or verifying or endorsing the information in any way and I
4 can state it.

5 MJ [COL POHL]: You believe that you can do it now?

6 LDC [MR. CONNELL]: I have never done it because I act
7 out of an extreme abundance of caution ----

8 MJ [COL POHL]: You believe as long as you apply your
9 hearsay analysis to it, to show the statement appeared in The
10 Washington Post, which is really what you are saying, that's
11 okay, even though you know it is classified?

12 LDC [MR. CONNELL]: That is my understanding of
13 classification law ----

14 MJ [COL POHL]: Okay.

15 LDC [MR. CONNELL]: ---- that I cannot endorse, verify
16 in any way. But the fact that, it is the same reason that I
17 can read The Washington Post on my unclassified system. We
18 know, 100 percent, that I cannot access classified information
19 on my unclassified system. But I can read The Washington Post
20 on my unclassified system, I can read The Early Bird on my
21 unclassified system, I can read Open Source Intelligence
22 Center, I'm a subscriber, I can read their information on my
23 unclassified system because I'm not endorsing or adding

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 anything to or verifying that information. I'm simply
2 accessing information that I know in another forum to be
3 classified on an unclassified system because we are allowed to
4 do that. In fact, there is an example.

5 MJ [COL POHL]: That is not what I'm talking about,
6 though. I'm not talking about you reading classified
7 information that has been released in unclassified context by
8 a third party.

9 LDC [MR. CONNELL]: Okay.

10 MJ [COL POHL]: That's not the question. The question
11 is can you repeat it in pleadings and other legal documents
12 when you know it is classified by simply attributing it to an
13 unclassified source?

14 LDC [MR. CONNELL]: No. And that is what I'm saying.
15 If I'm simply attributing to an unclassified source is not the
16 question. The question is whether I endorse or verify it. If
17 I endorse or verify it, that makes unclassified -- I'm not if
18 I simply know of it's existence, then I am not providing
19 endorsement or verification.

20 MJ [COL POHL]: Okay.

21 LDC [MR. CONNELL]: Moving on to slide 29, please. The
22 third protective order is the need-to-know provision that
23 appears in the protective order. This need-to-know provision

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 is also a legacy of the first round of Military Commissions.
2 I know that it was in Protective Order Number 3 and it was
3 wrong then and it is wrong now. The paragraph 15(c), Charlie,
4 of the government's proposed protective order, paragraph 15
5 lists the three standard requirements for access to classified
6 information. Charlie paragraph is a need to know the
7 classified information at issue, which is perfectly correct.
8 It appends a sentence, as determined by the OCA of that
9 information, which is not correct. It has, the past 50 years
10 it has not been the situation that OCA determines the need to
11 know. There are in fact specific provisions of the executive
12 order on this topic.

13 In this slide, the top paragraph is paragraph
14 Z ----

15 MJ [COL POHL]: Who do you believe determines the need
16 to know?

17 LDC [MR. CONNELL]: An authorized holder of classified
18 information.

19 MJ [COL POHL]: That could be an OCA?

20 LDC [MR. CONNELL]: Certainly could be OCA. Or their
21 superior.

22 MJ [COL POHL]: So if this read "as determined by the
23 OCA or their superior," you would be okay with it?

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 LDC [MR. CONNELL]: No.

2 MJ [COL POHL]: Okay.

3 LDC [MR. CONNELL]: It is much more expansive than that.
4 OCA is a subset authorized holder of information. Talked
5 about authorized holder of information, a term of art, which
6 is any person who has access to information in an authorized
7 fashion. OCA falls into that, I fall into it, my paralegal
8 falls into it.

9 MJ [COL POHL]: So it is your -- your position that need
10 to know can be determined by your paralegal.

11 LDC [MR. CONNELL]: Can be determined by an authorized
12 holder of information.

13 MJ [COL POHL]: Didn't you tell me your paralegal is an
14 authorized holder of information?

15 LDC [MR. CONNELL]: Assuming they are, yes.

16 MJ [COL POHL]: Assuming they are, the paralegal can
17 determine your need to know, then?

18 LDC [MR. CONNELL]: That's right, if we were to go
19 within ----

20 MJ [COL POHL]: I'm not saying that you are the one that
21 wants to change it. You say anybody with an authorized need
22 to know can authorize a need to know by anybody else who meets
23 A and B.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 LDC [MR. CONNELL]: Let's look at the authority for
2 that. The court sounds a little incredulous that's the law.
3 That's been the law for 50 years.

4 MJ [COL POHL]: I'm just want to know what your position
5 is.

6 LDC [MR. CONNELL]: Right. That is why my paralegal --
7 if my paralegal does first draft of a classified brief, that
8 is why they get to send it to me via classified e-mail as
9 opposed to having to send it to an OCA who then has to
10 determine whether I have the need to know and send it to me.
11 That is what the current situation would require, because only
12 OCA can determine need to know. There are hundreds --
13 probably, in the country, millions -- of need-to-know
14 determinations made each day not by OCAs but by authorized
15 holders of information.

16 MJ [COL POHL]: I think I understand the distinction. I
17 got it.

18 LDC [MR. CONNELL]: The prior executive order, paragraph
19 Zebra of Executive Order 13392 played that out explicitly and
20 need to know as a determination made by authorized holder of
21 classified information perspective recipient requires
22 classified information --

23 MJ [COL POHL]: You say on a particular piece of paper.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 LDC [MR. CONNELL]: Correct.

2 MJ [COL POHL]: I was thinking more the generic.

3 LDC [MR. CONNELL]: Right.

4 MJ [COL POHL]: Programs and things.

5 LDC [MR. CONNELL]: No, they determine that.

6 MJ [COL POHL]: I got you. That was my confusion. I
7 got what you said, okay.

8 LDC [MR. CONNELL]: The one way to address this, I don't
9 think it is necessary, but if the court wants to have a
10 belt-and-suspenders approach, the way the habeas protective
11 order addresses this problem is that explicitly puts in the
12 habeas protective order the habeas counsel have a need to know
13 information relevant to their client relating to issues in the
14 case. I'm sorry.

15 So if the court wanted to be clear on it, it could
16 import similar language to this. I propose that in 17 Charlie
17 of our proposed protective order defense has need-to-know
18 related issues in the case. That's the difference between the
19 current executive order and president Bush's executive order.

20 The current executive order says that not only
21 authorized holders can determine need to know, but their
22 superiors can also determine need to know. The reason for
23 that is because of the expansion of the classified systems,

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 SIPR -- for example, if I create an analysis, I put it on SIPR
2 for anybody who, you know, wants to read it, I can't make an
3 individualized need-to-know determination for each person who
4 holds a SIPR account because I don't know who they are. I
5 don't know whether they actually need to know the information.

6 So my superior can essentially make a blanket
7 need-to-know determination to say, yes, you can put this up on
8 SIPR, SIPR account holders as a group need to know this
9 information. That's the change that was made in the current
10 Executive Order, but it really just reflected existing
11 practice.

12 Moving on to the fourth issue, that is the
13 meaningful guidance issue. This is where I started my
14 argument with the question that protective order as drafted
15 has a lot of redundant information but is actually short on
16 meaningful guidance.

17 I accepted paragraph 30 here, which says that we
18 should not under any circumstances reveal classified
19 information. We know that. We are, our livelihoods depend on
20 it. But there are a number of situations our actual
21 day-to-day operations performing the defense function come
22 into conflict with this. And I could not exaggerate the
23 number of times that we deal with the question of is this

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 information classified or not. It comes up every day. And it
2 is one of the reasons why, regardless of other considerations,
3 it may not be that practical to have the court staff handle
4 these sorts of questions because there are just so many of
5 them, they come up all the time.

6 One of those I mentioned earlier is open source
7 information, something that appears in The Washington Post, on
8 Early Bird, or from the open source collection, how that
9 information gets handled, whether it has been declassified or
10 not, whether it is classified in the first place.

11 You know, The Washington Post doesn't come stamped
12 "classified" at the top. Sometimes we know information is
13 leaked. It says according to, you know, a government unnamed
14 government official, then we treat it accordingly because we
15 know that is at some level some kind of a leak.

16 But if it reports a foreign dignitary, human
17 rights organization, those sorts of things, if it is reporting
18 that third-party information, it is difficult for us to tell
19 what rules to apply to it.

20 I mentioned earlier the witness situation. And I
21 want to raise the specific question of leaked information now,
22 because leaked information seems to be on everybody's mind
23 because people keep asking us about it. The reason that I, as

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 a -- as a security clearance holder cannot go to WikiLeaks.com
2 or dot-org, whatever it is, and look at information there that
3 is relevant to this case, even though someone else, you know,
4 a lawyer in another situation could do so is not because of my
5 security clearance. My security clearance doesn't stop me
6 from accessing that information.

7 What stops me is the fact that it is on NIPRNET,
8 right, it is in the unclassified internet. So my orders from
9 the Department of Defense are that I cannot access classified
10 information on an unclassified system. That's the reason why
11 I can't do it. It is an orders violation for me to review it,
12 not a violation of the terms of my nondisclosure agreement or
13 violation of the terms of my security clearance. And various
14 orders from the Department of Defense made this clear, we
15 can't access that sort of information, leaked information on
16 an unclassified system.

17 There is an easy solution, there is an easy
18 workaround to that, which is that -- I don't know this for a
19 fact, but it would amaze me if somewhere on SIPRNET was not a
20 collection of this leaked information that various analysts
21 use to analyze, either analyze leaks or analyze the
22 information themselves and the government could simply provide
23 us a copy of it on SIPRNET and then we would be in a situation

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 where we would have the same access as the rest of the world
2 to the information but we wouldn't violate our DoD orders.

3 There are multiple, there is another, the fourth
4 situation that we keep running into is possibly classified
5 information. We have been briefed -- I have issues with the
6 quality of the briefing. We have been briefed about
7 rendition, detention, and interrogation information. We run
8 into other possibly classified information all the time
9 relating to electronic communications monitoring capacities,
10 relating to unmanned flying vehicles, relating to the sort of
11 thing that permeates many books which have been written about
12 the experiences of CIA agents and others in the 9/11 period.

13 We didn't have any classification guidance on
14 those. There's a word that I don't know if I can say it in an
15 unclassified situation.

16 MJ [COL POHL]: Then don't.

17 LDC [MR. CONNELL]: Right. It comes up over and over,
18 that there are, there is commonly available information which
19 might be classified, we want to handle it properly, and we
20 need guidance on how to do so.

21 The last situation is declassification requests.
22 It is different from a classification challenge. A
23 classification challenge, of course, is, I think this

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 information is improperly classified, it should be classified
2 at a different level. Declassification request is I have this
3 piece of information, I know it is properly classified, I
4 would like an OCA to review it with my request to declassify
5 it.

6 The regulation for trial by Military Commission
7 and, in fact, Rule 505 itself both refer to the authority of
8 the trial counsel to seek declassification for certain
9 information, but provide no authority or mechanism for the
10 defense to seek declassification of certain information.

11 In fact, the Military Commissions Act requires
12 the, that information that the government seeks to use against
13 the accused be provided to them, that their -- they can't have
14 any information which is secret from them used against them
15 which, as I read the law, the only way to do that is to seek
16 declassification.

17 That's the sort of high-level problems that we
18 need help with. But there are a lot of other very basic
19 things, like it's amazing this protective order does not tell
20 us what cover sheet to use.

21 MJ [COL POHL]: Do you want it to?

22 LDC [MR. CONNELL]: Yes, please. I have been on an
23 eight-month campaign to find out the proper cover sheet. I

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 thought I was going to be on to something, Your Honor, because
2 the government has been serving classified pleadings on us, I
3 thought I will use whatever cover sheet they use, but they
4 didn't put any cover sheet on it at all.

5 So what I would like is a cover sheet. That is
6 what I mean by safe harbor, if you or somebody said to me if
7 you use this cover sheet for this type of information, you're
8 operating correctly. If that were to occur, that is what I
9 would like. That's the kind of basic classification guidance
10 we are seeking here in many situations.

11 MJ [COL POHL]: So what do you do now?

12 LDC [MR. CONNELL]: I do my best.

13 MJ [COL POHL]: Has your best been good enough so far?

14 LDC [MR. CONNELL]: No one has attempted to put me in
15 jail or anything.

16 MJ [COL POHL]: Well, then the answer is yes.

17 LDC [MR. CONNELL]: I shouldn't have to, I shouldn't --

18 MJ [COL POHL]: -- cover sheet? You want some order to
19 cover every possible permutation of cover sheets?

20 LDC [MR. CONNELL]: No, Your Honor. What I really want
21 is the Classification Guide. This document that I'm talking
22 about already exists. The executive order requires OCAs to
23 produce classification guides that tell derivative

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 classifiers, that is me, I'm a derivative classifier, that
2 tells derivative classifiers how to mark documents at what
3 level, different types of information are classified.

4 MJ [COL POHL]: You have not gotten that guidance?

5 LDC [MR. CONNELL]: Correct.

6 MJ [COL POHL]: You asked for it, and the response?

7 LDC [MR. CONNELL]: In the attachments we moved for it,
8 AE 54, we asked the prosecution for it, asked the Convening
9 Authority for it, we filed a motion with the court about it.
10 That would solve our problem. The court doesn't have to put a
11 spreadsheet in its protective order saying every possible
12 cover sheet because that spreadsheet already exists, we are
13 just asking for it.

14 MJ [COL POHL]: Okay. You told me you asked for that in
15 another motion.

16 LDC [MR. CONNELL]: Yes, that is 54.

17 MJ [COL POHL]: Okay, go ahead.

18 LDC [MR. CONNELL]: I won't belabor the point but, you
19 know, one of the problems with -- that Classification Guide
20 would solve so many problems. Like we don't know whether the
21 tri graphs governing this program are classified or not.
22 We've asked and asked and asked we don't know.

23 We don't know what banner markings to use. The

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 government use would different banner markings. We are
2 required derivative classifiers to mark every document we mark
3 as classified to put a declassification date on it. That is
4 right there in executive order in fact we are sanctionable if
5 we don't do it. We have no idea what the declassification
6 dates are, it is not our call we don't get to make up
7 declassification dates.

8 MJ [COL POHL]: Would it be fair to say with all the
9 handling issues you have done the best you can so far, you are
10 not currently in jail and you want to make sure you don't go
11 some future time?

12 LDC [MR. CONNELL]: Correct, you summarized my argument,
13 Your Honor.

14 MJ [COL POHL]: Got it.

15 LDC [MR. CONNELL]: Because these things overlap I
16 provided a paragraph in proposed order paragraph 21 that the
17 court could order the prosecution to provide us with the
18 existing written classification guidance. I'm not asking for
19 something new but to be provided existing information that
20 should be provided to us. And we can handle that in 54, we
21 can handle it here. But it is the same way either way.

22 The other -- sounds like the court has read the
23 other safe harbor provisions that I proposed. I won't go

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 through them one by one, but if the court has any other
2 question about those I am happy to answer them.

3 Let's move to slide 41, please. What I heard the
4 court say earlier, and correct me, I speak under correction,
5 is that one good way to solve the whole hearing closure debate
6 is to take paragraphs 40 through 42 out of the protective
7 order because those, if those -- those provisions -- take a
8 look at 40 for a second.

9 Paragraph 40 says while proceedings shall
10 generally be publicly held, the Commission may exclude the
11 public from any proceeding sua sponte upon motion by either
12 party in order to protect information the disclosure of which
13 could reasonably be expected to damage national security.

14 As the intervenors have argued, if that were the
15 standard, that would substantially lower the standard for
16 closure below the First Amendment floor. So that means one of
17 two things: Either this provision, the government argued this
18 provision refers to Rule 806, which it doesn't, but the, it
19 either means what 806 says, in which case it is redundant. So
20 it is at best useless, at worst changing violation of the law.

21 MJ [COL POHL]: You don't believe 806 has that standard
22 in it, for closure?

23 LDC [MR. CONNELL]: 806 has a standard for closure,

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 certainly.

2 MJ [COL POHL]: The same as what is in the protective
3 order?

4 LDC [MR. CONNELL]: No.

5 MJ [COL POHL]: I understand how you read it.

6 LDC [MR. CONNELL]: In fact, the standard has
7 essentially three elements to it, one of which we haven't
8 talked about here, one of them is notice and opportunity to be
9 heard. Before some -- the Supreme Court has not addressed
10 this yet but the circuit has said before you close a hearing
11 there has to be some kind of notice and opportunity to be
12 heard. Obviously we have intervenors here. They had their
13 opportunity to be heard.

14 MJ [COL POHL]: You heard my discussion of the closure
15 issue, you think that is before me now?

16 LDC [MR. CONNELL]: Paragraphs 40 through 42 are before
17 you. If you take those out all together, which there is a
18 suggestion you might.

19 MJ [COL POHL]: I'm saying no matter what is in the
20 proposed protective order, closure is determined by its own
21 rules, right?

22 LDC [MR. CONNELL]: That is an interesting question. If
23 what the court is saying is that the protective order has no

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 force and doesn't supercede any other rules --

2 MJ [COL POHL]: If there is a statute and a rule that
3 says here is how you handle closure of the proceedings, then
4 what is interesting is this language that I read in 40 appears
5 to be identical to the language in 806, you don't say it is,
6 but that's okay. But my point is that there is a certain
7 procedure to go through prior to closure. Okay?

8 LDC [MR. CONNELL]: Yes.

9 MJ [COL POHL]: Implicates 505, 505(g) notice, 505(h),
10 Section 806 determination of whether anything needs to be
11 closed.

12 LDC [MR. CONNELL]: Yes.

13 MJ [COL POHL]: That is the procedure laid out.

14 LDC [MR. CONNELL]: We don't need 40 through 42.

15 MJ [COL POHL]: I'm saying that is the procedure laid
16 out, that is the procedure I intend to follow. If this
17 language is in there again I don't think it necessarily needs
18 to be in this order because that's the procedure that is laid
19 out in the regulations of what to do in a closure.

20 So all this discussion about closure is not the
21 issue before me. I understand what your position is and we
22 may want to revisit the standard for closing because this
23 standard in 806 appears to be virtually identical in language.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 What you are saying is constitutionally deficient, I got that.
2 I'm simply saying it is the same language. I suspect this was
3 included in there -- well, I won't speculate.

4 Anyway, at the end of the day, closure is a
5 separate issue and I will address it at the time.

6 LDC [MR. CONNELL]: In that case, speaking of closure, I
7 will close with slide 44, which is our proposal to lay out the
8 procedure. Essentially what the court just said, if the court
9 wants to put this in the protective order, the only thing that
10 this adds is there be unclassified notice of the intent to
11 close to go to the public so that intervenors, if they choose
12 to oppose closure, they can do so.

13 The public has a right, the victims have a right,
14 the general public, the world has a right to -- it is not an
15 unqualified right -- they have the right to be heard on this
16 topic, but they can't be heard if they don't have notice there
17 is about to be a closure. So that is what our proposal does,
18 incorporate that procedure.

19 MJ [COL POHL]: I would have some questions about that
20 procedure but since we are not going to talk about closure in
21 this protective order, I understand your position Mr. Connell.

22 LDC [MR. CONNELL]: Thank you, sir.

23 MJ [COL POHL]: Any other defense counsel wish to be

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 heard on AE 13? Mr. Nevin?

2 LDC [MR. NEVIN]: Your Honor, thank you. I want to say
3 that, really just a few things. And just so the record is
4 unmistakably clear, in any way that I understand the word
5 "participate," Mr. Mohammad did not participate in any
6 classified programs.

7 Everything that -- all of his observations were
8 imposed on him against his will. Everything that he saw or
9 heard was done not by, at his request or at his demand or in
10 exchange for, for giving anything on his behalf, such as a
11 promise to keep materials secret, it was all imposed on him
12 from the outside.

13 And I think this connects to the questions that
14 the court has heard, and I'm not going to repeat them because
15 they have been said very well, but they connect to the
16 questions the court's heard about whether this material may be
17 classified at all in the first instance.

18 Just a couple remarks on some points that the
19 government made during its argument to you. I heard counsel
20 say that we are -- the only limitation that is imposed on
21 counsel in our conversations with our clients is that we may
22 not tell them classified information, that everything else is
23 acceptable.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 I just want to call the court's attention to the
2 fact that that's not what the mail and communications order
3 says. We are going to argue this in 18 and 32 later, at some
4 point. Not going to get into it now, but I just wanted to
5 flag it for the court, that is really not true.

6 Counsel made the point that the government isn't
7 attempting to sanction the accused for revealing classified
8 information. I think what she said was something to the
9 effect that if we attempted to sanction them for revealing
10 classified information, that would be absurd, we couldn't do
11 that.

12 I just want to point out to the court that we are,
13 the government is sanctioning them for the revelation of
14 classified information, for the revelation of their
15 observations, because they are not allowed to speak out about
16 what they observed. They are not allowed to pass that
17 information to other people. They are not allowed, as a
18 result of the concern that they would pass classified
19 information, they are not allowed to have communications with
20 anyone outside of the few limited exceptions that you heard
21 about. They are not allowed to, most important, they are not
22 allowed to speak to their families about any subject. So they
23 very clearly are sanctioned.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 I think counsel was talking about the idea of
2 maybe prosecuting them for releasing classified information,
3 something to that effect. But that statement that was made
4 was too broad.

5 [Inaudible].

6 MJ [COL POHL]: Okay, I think it is back on.

7 Mr. Nevin, when she said that, I took it the same
8 way. At least I took it as criminal sanctions, not certain
9 limits on their ability to communicate this time which
10 certainly could fall within a sanction on their freedom to
11 communicate, for want of a better term. Go ahead.

12 LDC [MR. NEVIN]: Yes, sir. Thank you. A couple of
13 times the issue of redundancy came up. For example, in
14 arguing about the request for a defense security officer,
15 counsel made the point that we're supposed to understand the
16 rules, we have security clearances and what do we want, just
17 someone around who has more experience with security
18 classification to give us advice? We probably already have
19 someone like that, why do we need someone else?

20 A little bit later or a little bit earlier in the
21 arguments, we, we address the question of whether we need a
22 protective order for classified information at all.

23 So one might well say if what counsel says is

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 true, if we are presumed to understand this, and if we have
2 received the clearances, why do we need the additional
3 elaboration that comes out of this protective order?

4 The rule says the court shall issue a protective
5 order but it doesn't say what it must contain. It says it may
6 contain a number of things, but it needn't contain anything.
7 There is no requirement under the rule that it contain
8 anything in particular.

9 And the effect for us is that, you know, and I
10 think Mr. Connell lays this out in some detail, this is more
11 than maybe an academic consideration. These, when rules
12 appear in different ways in different places, and when we've
13 been told we are subject to criminal prosecution if we do
14 something that the rules forbid, and we read these rules
15 carefully, as I know the court does as well, but when these
16 rules appear in slightly different variations in different
17 places, the effect is that one is frozen, one ends up not
18 knowing what to do.

19 And I raised this point with the court yesterday
20 that at my read-on information was provided to me that what
21 the court did with inquiring of these men in open court,
22 whether they waived, was seeking the revelation of classified
23 material. I understand the government has filed 13 Lima in

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 which they step back from the idea of presumptive
2 classification in various ways.

3 And if the government -- if the lawyers for the
4 United States who filed that pleading with you have the right
5 to change what I take to be a representative of the OCA, what
6 that person told me, okay, I am certainly willing to accept
7 that. That's not really how I understand the rules to work.

8 The problem for us is that when these rules appear
9 in different ways in different places, we end up not able
10 to ----

11 MJ [COL POHL]: You understand the government's
12 position. The term "presumptive classification" is not a
13 classifying device. It is simply a handling device, by that
14 meaning is that some information you may get orally from your
15 client may or may not be classified but to treat it as such
16 until its status is determined. It doesn't make the
17 information classified, as I understand it.

18 So therefore, I understand what you are saying.
19 If you take the words to mean that you hear something brand
20 new from your client and therefore it is classified until it
21 is determined not to be, I understand. I think that's where
22 the confusion of the term is, that there is a classification
23 process and the accused says, "I want a tuna sandwich today,"

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 I understand the old rule would seem to imply you've got to
2 treat that as classified until you know it is not classified;
3 but that doesn't make it classified.

4 That's my point. That's where I'm not sure to run
5 it all the way down to OCA. I can understand your confusion,
6 though, because the first time I heard it, I had some of those
7 same concerns.

8 LDC [MR. NEVIN]: And I think we made the point in
9 briefing, in our moving papers, that it requires that there is
10 no authority for treating material as being classified unless
11 it is classified, and that's already been argued to you.

12 MJ [COL POHL]: Gone down to their current standard of
13 know or should know it is classified.

14 LDC [MR. NEVIN]: Yes. Just my other point, Your Honor,
15 when the court says the old rule, actually that is not the old
16 rule. The old rule was something like what we've gotten back
17 to today. There have been -- I've been around here since
18 2008, and there have been a series of rules. And we went
19 through a long period of time where there were certain
20 subjects that we couldn't communicate information from our
21 clients about, but we could communicate everything else.

22 So as I say ----

23 MJ [COL POHL]: I understand the rules appear to be,

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 like my scheduling order, somewhat of a living document, but
2 go ahead.

3 LDC [MR. NEVIN]: And then finally, Your Honor, I just
4 want to make this point: It has come up several times that
5 because of the sensitivity of the information that the accused
6 has, that many restrictions have to apply to who is permitted
7 to talk to them and what they are allowed to say.

8 My information is that that isn't a rule that is
9 not uniformly honored by the government. My understanding is
10 that there are persons within the guard force who have contact
11 with the accused, who don't possess TS/SCI clearances. I'm
12 advised, for example, when I meet with Mr. Mohammad, I do it
13 in a facility that is not SCIFed, that doesn't constitute a
14 SCIF.

15 I see variations in the way these matters are
16 dealt with that lead me to think that for the most part the
17 difficulties and the limitations, the barriers to going
18 forward mostly apply to me. But that when the government
19 wants to have a, wants to approach a problem in a more
20 flexible way it does so for its own reasons.

21 There will be at a later time a more comprehensive
22 discussion of the barriers to representation that are present
23 in many of the things that we do in this capital case. I

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 think they are inconsistent with delicacy and comprehension
2 that is required for the defense of a capital case. That is
3 one of them; I flag it for the court's attention.

4 That is what I have. Thank you.

5 MJ [COL POHL]: Ms. Bormann.

6 LDC [MS. BORMANN]: First, I want to adopt everything
7 argued by learned counsel who preceded me. I want to address
8 a few issues that merit some passing comment. One, we talked,
9 you talked with Mr. Connell a little bit about ICRC, whether
10 or not that was an unfettered communication between an accused
11 and the ICRC.

12 And without getting into classified information, I
13 can tell you that I was a witness to that concept and it is
14 indeed unfettered in a way, actually, that client-attorney
15 communications are not. Because when the ICRC visits with
16 Mr. Bin'Attash, there is no video camera, there is no video
17 monitoring and there is no monitoring whatsoever, so it is
18 truly unfettered, unlike my communications with him. So I
19 want to put that on the record.

20 Additionally, I want to talk a little bit about
21 the concept of control. We talked about the executive order
22 that is the beginning of any analysis with respect to what
23 classified material is. And when President Obama came into

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 office they actually amended the executive order with respect
2 to that, because the Obama administration said we want to do
3 away with the overclassification of material. So we are going
4 to change the executive order and make provisions that allow
5 for easier declassification or challenge of improperly
6 classified material.

7 Now, we talked about, Mr. Connell talked about the
8 prong of control under the executive order. And that's the
9 prong that the government uses here, the government, with a
10 small "g," to justify stopping everything that my client says,
11 shutting down these hearings and barring me from telling the
12 world what it is he suffered.

13 The question is control. What is control? And
14 what control, what product is controlled? So this is a
15 commonsense evaluation. The government is not trying to
16 prevent my client's body from being exhibited. In fact, they
17 argued earlier this week that my client must have his body
18 exhibited, must come to court. So they are not saying that it
19 is my client's body that is classified. What they have
20 attempted to classify, and we believe improperly, are the
21 thoughts, perceptions, ideas, sensations and thoughts of my
22 client.

23 Those things, that information, is what they've

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 sought to classify because that is the information that they
2 believe that they are arguing will cause damage to national
3 security. That information they cannot and do not control.
4 And that is why the term "information," as used in the
5 executive order, is really a term of art. Because it is only
6 the information sought to be classified that needs to be
7 controlled by the government. And in this case they don't do
8 that.

9 MJ [COL POHL]: Okay. Let me see if I have got this
10 correct. If your client is aware of information X, let's use
11 the example that is a public thing that Mr. Muhammad was
12 waterboarded 183 times. For sake of this discussion, we're
13 going to say that is classified. Okay?

14 LDC [MS. BORMANN]: Okay.

15 MJ [COL POHL]: Is it your view that what -- is there a
16 distinction between that and the thoughts, impressions and
17 memories?

18 LDC [MS. BORMANN]: Absolutely.

19 MJ [COL POHL]: Under my example, the thought,
20 impression and memories could not mention the 183 times, but
21 could say -- I'm just trying to see; thoughts, impression,
22 memories, you imply that is a separate category than the
23 information that generated thoughts, impressions, memories.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 LDC [MS. BORMANN]: Two different concepts here.
2 Discovery tendered by the government is one. Discovery
3 tendered by the government generally, unless they involve
4 statements of my client reported by CIA agents or FBI agents,
5 are not going to contain impressions, thoughts, sensations,
6 experiences, delved into my client's brain. Okay?

7 So Mr. Muhammad being waterboarded 183 times is
8 that type of classification material for purposes of this
9 argument. What I'm talking about is what Mr. Muhammad
10 experienced during that 183 times of waterboarding; how he
11 felt, what he saw, the experience of pain.

12 MJ [COL POHL]: Do you think there would be a firm line
13 between the fact and the thought, impression, and memories?
14 That is where I'm having a tough time metaphysically
15 approaching this, the thoughts, impressions, memories, how he
16 felt, what he experienced, what he thought was going to happen
17 to him. Those can all be thoughts, impressions, memories but
18 only in the context, for the sake of discussion, the
19 classified information.

20 So you seem to think that -- do you see there is a
21 firm line between those two?

22 LDC [MS. BORMANN]: What I see is that the government
23 cannot properly classify those thoughts, experiences because

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 they are not either owned by the government, produced for the
2 government, or in any other way controlled by the government.

3 So what Mr. Mohammad felt with respect to, let's
4 say, waterboarding episode number 52 versus waterboarding
5 episode number 150, the difference in those experiences and
6 how he experienced those sensations and what he thought, those
7 things cannot possibly be either owned by, produced for, or
8 controlled by the United States Government. And if they do
9 not fit into one of those three categories, they cannot be
10 properly classified, period.

11 MJ [COL POHL]: I understand.

12 LDC [MS. BORMANN]: Now I want to address the need for a
13 defense security officer, or whatever you want to call this
14 person. And Mr. Connell did a really good job of laying out
15 some of the problems that we have.

16 I am not military. Mr. Connell is not military,
17 Ms. Baltes is not military, and neither is Mr. Nevin. But I'm
18 sitting between two guys over here who are. And I am here to
19 tell you, because I have had to argue this issue before, that
20 not only does the Navy in their Code 30 situation provide
21 security officers to the defense, but the Air Force does it as
22 well. And they do it in every single case as a matter of
23 course when you are dealing with classified information.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 MJ [COL POHL]: What do they do?

2 LDC [MS. BORMANN]: They provide -- they provide
3 information to the defense with respect to everything that
4 surrounds us and they provide a conduit to a place, wherever
5 the OCA is, because it depends on case to case, a conduit for
6 determining questions surrounding classification guidance.

7 MJ [COL POHL]: You say "conduit," you mean a courier?

8 LDC [MS. BORMANN]: I mean a way to ask a question.
9 Because unlike a situation where, let's say, we were talking
10 about CIPA earlier, so my experience is civilian, right? In
11 CIPA very rarely are you in a situation where your clients'
12 own words are sought to be classified by the government.

13 So under a CIPA analysis, very rarely would you
14 have to go to a court security officer with 20 pages of your
15 client's version of events and say please tell me if these
16 thoughts, experiences, ideas, sensations are classified; and,
17 if they are classified, at what level?

18 Now, in this case, however, that's exactly what we
19 are asked to do if we want either to declassify them or if we
20 want to subject them to a challenge for classification; two
21 different issues. We don't have the ability to do that.
22 Mr. Connell was not flippant when he talked about how
23 difficult this really is. I have sent innumerable questions

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 on the SIPR side of things to the Office of Military
2 Commissions in order to seek guidance about very difficult
3 issues. All of them, by the way, involving attorney-client
4 work product, and I try, at least, try to take that concept
5 out of it and make it as general as possible. I have no place
6 to go when I have a question that exposes privileged
7 information, no place.

8 My Bar rules under the Supreme Court of the State
9 of Illinois don't allow me to ask those questions of somebody
10 who doesn't fall within a privileged team. So we are stymied
11 when we have these issues. And we want to follow the law. I
12 mean, nobody here, sitting here, wants to leak classified
13 information that could cause damage to national security.
14 None of us want to do that.

15 But we want to make sure that it's properly
16 classified, number one; and, number two, that we have a way of
17 challenging that issue when it arises.

18 Lastly, I want to talk a little bit about, and I
19 know you are not going to address the 505 things, so I will
20 skip that. But counsel for the government, when she got up,
21 said that their proposed protective order does not limit
22 communication between, for counsel -- I'm sorry, doesn't limit
23 communication between counsel and the accused and it doesn't

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 really limit counsel in doing their job.

2 And it is clear to me that Ms. Baltes has never
3 been a defense attorney because if she had, she would
4 understand what it is that we are tasked with doing here.

5 So let's just assume for argument sake that my
6 client tells me something about something that happened to him
7 over the time period between 2003 and 2006, the time period
8 covered by the RDI. And I am, as part of my duties as learned
9 counsel, tasked with the, and obligated to, investigate what
10 he says to me because it is relevant and necessary to his
11 case.

12 So I have to hire an investigator. That
13 investigator may not be somebody who is an American citizen
14 because, of course, the investigation in this case spanned
15 numerous continents. And maybe the person that I need to hire
16 speaks a language that may not be spoken regularly by
17 investigators here in the United States who would be capable
18 of getting a TS clearance.

19 So now I have to somehow figure out a way to use
20 an investigator who can't possibly get a TS clearance, inform
21 him of the relevant information he needs to investigate
22 without using classified information. And as Mr. Connell
23 correctly noted, the idea of classification is because I am a

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 classified holder, the very fact that I give a sense of
2 imprimatur to -- let's say country X is actually a violation
3 of the classification guidance we have been given.

4 So I can't even tell an investigator to go to
5 country X. This is a huge issue.

6 Then let's assume that I could. Let's assume we
7 took care of that issue, and I could tell an investigator to
8 go to country X.

9 Now that investigator comes back to me says,
10 "Cheryl, this is what I learned in country X. I want you to
11 verify it with your client, and please let me know if there is
12 any follow-up that needs to be done," and I learn some
13 additional facts.

14 Now, in a regular case where they haven't
15 classified everything that comes out of my client's mouth,
16 where they haven't classified actual locations of places, I
17 can go in to my client and say this is what the defense
18 investigator found and say, "I want to know whether or not
19 this is accurate and, if it is not, I need you to let me know
20 where it is not accurate because we need to follow up on it."

21 I can't do that here, because simply mentioning
22 any of the information regarding country X may be classified.
23 And I am barred from telling my client anything that is

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 classified.

2 I mean, I fastidiously stick to these rules but it
3 really has made this case incredibly difficult. And for
4 counsel for the government to stand up and just flippantly
5 claim that it doesn't affect our very ability to practice law
6 here is incorrect.

7 MJ [COL POHL]: On the proposed protective order they
8 talk about, specifically about the RDI program, specific
9 times, okay? All obviously postdate the alleged offenses.

10 Do you believe you have those difficulties on
11 investigating the pre-capture time? Are you with me on this?

12 LDC [MS. BORMANN]: Yes, I am.

13 MJ [COL POHL]: What I'm saying is that at the crux
14 of -- a lot of the order deals with post-capture of the
15 accused, which are unrelated to a degree, unrelated at least
16 on its face to the charged offenses in terms of factual
17 predicate. That is all I'm saying.

18 I'm not making any conclusion. What I'm saying,
19 that's that limitation. But if you want to say you believe
20 this limits your ability to investigate pre-capture ---

21 LDC [MS. BORMANN]: Let me give you an example of that
22 if I might. The government has not yet provided discovery,
23 I'm assuming at some point they will.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 MJ [COL POHL]: Probably because they are awaiting the
2 protective order.

3 LDC [MS. BORMANN]: I understand, although I do have to
4 note for the record, I am a holder of a TS clearance; and if
5 the protective order is simply repeating the status of the
6 law, I could have been provided discovery a long time ago.

7 That notwithstanding, that issue is going to arise
8 very quickly because I am going to assume that at some point
9 I'm going to receive a report that says something happened
10 somewhere else. Pick a country. And I'm going to have to
11 hire an investigator to talk about, to investigate what
12 happened in that country somewhere else.

13 And if that investigator, in the process of
14 investigating that comes across anything that is -- this will
15 make me crazy, comes across anything that might possibly
16 involve either, well, intelligence issues, and any of the
17 issues there, we have a problem, right?

18 So I can't go to him and say, well, the
19 investigator determined that this was happening in this
20 country at this time but I can't tell you about it,
21 because ----

22 MJ [COL POHL]: The "you" you are referring to is your
23 client?

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 LDC [MS. BORMANN]: To my client.

2 MJ [COL POHL]: Got it.

3 LDC [MS. BORMANN]: So really, there are blocks pretty
4 much wherever you turn. And the pre-capture stuff is one
5 issue, the post-capture stuff is another issue. The truth is
6 both are essential in putting together both a defense to the
7 guilt/innocence portion of this trial and to the sentencing
8 issue of this trial, which, of course, as Your Honor knows or
9 maybe is learning, and I certainly know over my past, the two
10 certainly go hand-in-hand. I can't ignore mitigation in hopes
11 my client is acquitted, so I have to look towards that at
12 every phase of this investigation.

13 MJ [COL POHL]: I understand that.

14 LDC [MS. BORMANN]: So what I'm asking you to do is one,
15 don't just duplicate a protective order that tells me what the
16 law is. I already know what that is; I'm a practicing lawyer.
17 If you are going to issue a protective order, then
18 you ought to issue a protective order that requires the
19 government do the things they need to do, too, which is
20 provide existing guidance that is out there that we are sworn
21 to uphold without -- that we promised to uphold when we signed
22 the agreements on our read-on and we don't have access to,
23 despite numerous attempts.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 If you are going to issue a protective order, make
2 sure the protective order covers what it needs to cover but
3 doesn't make our jobs more difficult. And the government's
4 protective order, in all of the relevant ways that Mr. Connell
5 has argued, does that.

6 So I suggest to Your Honor, I argue to Your Honor,
7 that you adopt the proposed protective order suggested by
8 Mr. Connell. Thank you.

9 MJ [COL POHL]: Thank you.

10 DDC [LCDR BOGUCKI]: Good afternoon, Your Honor.

11 MJ [COL POHL]: Good afternoon.

12 DDC [LCDR BOGUCKI]: Kevin Bogucki for Mr. Ramzi bin al
13 Shibh.

14 Your Honor, as a preliminary matter, I would like
15 to adopt the argument ----

16 [The security button was pushed.]

17 MJ [COL POHL]: Hold on. Is it coming through now?

18 Just for the record, the reason that the red light
19 went on was concern that the generic discussion from the
20 defense counsel was a specific reference to a classified
21 technique.

22 DDC [LCDR BOGUCKI]: I was trying to characterize
23 hypothetical, sir.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 MJ [COL POHL]: Let me finish. And what he indicated
2 was the Commission does not find that it was such and it
3 simply was a hypothetical of what potentially could happen.
4 But, Counsel, I'm assuming you were given the briefing of
5 which techniques -- you guys may disagree what is classified
6 or not, I got it -- but you know which techniques have been
7 still classified and which are not, correct?

8 DDC [LCDR BOGUCKI]: Yes, sir.

9 MJ [COL POHL]: So don't get into any type of
10 hypothetical that could be construed as that. For the record,
11 what he indicated -- you may begin where you were on the
12 hypothesis, but that is the last time you do it.

13 DDC [LCDR BOGUCKI]: Understood.

14 MJ [COL POHL]: Just for the record, the public record,
15 start your argument again exactly as you did before.

16 DDC [LCDR BOGUCKI]: Right now, sir?

17 MJ [COL POHL]: Yes.

18 DDC [LCDR BOGUCKI]: Your Honor, if I beat you, I'm not
19 providing you information. If I chain you to the ceiling, I'm
20 not providing you information. I'm doing something to you.

21 MJ [COL POHL]: The record shall reflect that that's
22 actually what he said earlier when the red light went on.
23 Proceed.

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 DDC [LCDR BOGUCKI]: Thank you, Your Honor.

2 When I do those things to you, I'm not providing
3 you information. At most, I'm providing you with a memory of
4 my conduct and that conduct, your memory of my conduct cannot
5 reasonably be classifiable.

6 And if that memory cannot be classified, then I as
7 defense counsel should not be required to treat that memory as
8 classified simply because I hold a security clearance. My
9 holding a security clearance does not change the nature of
10 that particular piece of information, my client's memory.

11 As Mr. Nevin suggested, to characterize our
12 clients as having been participants in the CIA program would
13 be like characterizing an assassination victim as a
14 participant in the assassination program. It is ridiculous to
15 suggest that somehow they've been afforded access to
16 classified information and that therefore their memories need
17 to be treated as classified information. But that is
18 precisely what the protective order will be doing, Your Honor.
19 And that is why I come back to this point.

20 We would ask that this Commission not execute a
21 protective order that forces us to treat as classified
22 information something that is not properly classifiable.

23 And ----

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 MJ [COL POHL]: Let me ask you this: If it is
2 classified, am I to determine that it is not?

3 DDC [LCDR BOGUCKI]: Here's the problem, Your Honor, we
4 come back to the issue of control. Clearly --

5 MJ [COL POHL]: Here is a very simple question.

6 DDC [LCDR BOGUCKI]: Right.

7 MJ [COL POHL]: The government proffers that information
8 known to your clients is classified. Okay. Okay. The
9 threshold inquiry is, is it classified? Maybe it shouldn't
10 be, I got that, maybe it is overclassified, maybe some other
11 reason, okay. But if it is classified, is it my role then to
12 make it unclassified or declassified somehow?

13 Yesterday you seemed to think I have this power,
14 you still think I have this today.

15 DDC [LCDR BOGUCKI]: I do, Your Honor, for the reason
16 that it all revolves around control. Pursuant to the
17 executive order ----

18 MJ [COL POHL]: If the agency involved says this piece
19 of information is classified, okay? And then you tell me no,
20 look at the executive order, it doesn't fall within the
21 executive order, then I can say I make an independent
22 decision, yeah, you are right, it is not in the order,
23 Commander, you are exactly right, therefore it is not properly

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 classified, therefore you may treat it unclassified, that is
2 what you are asking me to do?

3 DDC [LCDR BOGUCKI]: No, sir. Sir, there could be a
4 separate determination regarding the classification of this
5 information and there might be some mechanism by which we can
6 challenge that. What I'm saying, for purposes of Appellate
7 Exhibit 13 we would ask that this court essentially not define
8 within the terms of the protective order a requirement that we
9 treat this type of information as automatically classified.
10 Paragraph 7 of the proposed protective order purports to
11 define what is classified and what is not classified. It
12 doesn't reference other classification.

13 MJ [COL POHL]: Do you believe it defines it or labels
14 it?

15 DDC [LCDR BOGUCKI]: I believe it defines it, sir.

16 MJ [COL POHL]: They can't define it. Isn't, at this
17 stage of the game, the government's role is simply to label
18 information that has been classified?

19 DDC [LCDR BOGUCKI]: Sir, Section 2, where paragraph 7
20 appears, labeled "Definitions," and paragraph Delta says any
21 document or information as to which the defense has been
22 notified orally or in writing that such document or
23 information contains classified information including --

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 MJ [COL POHL]: That's defining the term "classified
2 information," I don't dispute that. But I'm saying it is
3 not -- it says here is what classified information is and, oh,
4 by the way, here it is, here are parts of the information that
5 are classified. That is what I'm referring to.

6 DDC [LCDR BOGUCKI]: Understood, sir.

7 MJ [COL POHL]: Go ahead.

8 DDC [LCDR BOGUCKI]: In paragraph 7 Echo, sir, they
9 specifically say, "In addition, the term 'information' shall
10 include, without limitation, observations and experiences of
11 the accused, meaning observations and experiences of the
12 accused relating to the other sections defined in paragraph 7,
13 must be treated by us as classified in the context of this
14 protective order.

15 Now, whether some other requirement upon us
16 imposes burdens, obviously ----

17 MJ [COL POHL]: Let me ask you this. Does it say treat
18 it as classified or is classified? Do you understand the
19 distinction here?

20 DDC [LCDR BOGUCKI]: I understand the distinction, sir,
21 but this is where we get back to -- I know you hate this, sir.
22 We'll get back to the Lebron James problem. If we have to
23 treat something as classified, that means for two to three

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 months we cannot use that information. And I'm not talking
2 about a situation where I'm going to go out and put an
3 official endorsement on a piece of classified information.

4 But if, for example, my client were to tell me
5 that he was ----

6 MJ [COL POHL]: No, we don't need to go -- I'm simply
7 saying that if a piece of information is classified, you may
8 disagree with that. I got that. Okay. But I come back to
9 if -- I'm not faulting the logic of any of the defense counsel
10 when you deal with this amorphous, you know, leaving it to the
11 observation and experience of the accused with respect to what
12 does that mean, okay.

13 But I'm saying that if that information is
14 classified, you think I have the authority under the
15 protective order to say, no, it is not, or it is improperly
16 classified, you shouldn't treat it as classified it doesn't
17 meet the executive order.

18 What I'm trying to get here is, I heard this again
19 and again, is that there is this category that should never
20 have been classified to begin with, and I'm just saying
21 sequentially then -- let's say I agree with you it doesn't
22 fit, let's say for the sake of this discussion I agree that
23 this does not meet the executive order, appears to be a

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 strained reading of control, or whatever term you want to use,
2 okay.

3 But isn't the clear case authority that I -- that
4 a judge, federal judge, Commission judge, court-martial judge
5 doesn't have authority to second-guess the classification
6 determinations?

7 DDC [LCDR BOGUCKI]: Precisely, Your Honor, and that is
8 not what we are asking. What we are asking is that you not
9 endorse it or create a category of classification that ----

10 MJ [COL POHL]: Let's say I don't issue this out at all,
11 I don't sign anything ----

12 DDC [LCDR BOGUCKI]: Fantastic.

13 MJ [COL POHL]: ---- and you guys get the classification
14 guidance absolutely consistent with paragraph 7, then what do
15 you do?

16 DDC [LCDR BOGUCKI]: We have an obligation to obey those
17 orders consistent with our security clearance. What I'm
18 asking is you not include this in the protective order there
19 by number 1, judicially endorsing it; or, number 2, creating a
20 category of classification that is not otherwise classified by
21 some other source.

22 MJ [COL POHL]: So it is your view that they are
23 creating classification, classes in this protective order that

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 aren't classified anywhere else.

2 DDC [LCDR BOGUCKI]: That very well could be, sir, this
3 protective order will be binding upon us.

4 MJ [COL POHL]: Just like no authority to declassify,
5 how do I have authority to classify?

6 DDC [LCDR BOGUCKI]: You don't have authority to
7 classify. We are going to be bound by the terms of this
8 order.

9 MJ [COL POHL]: What I'm saying is if this order is
10 restricted only to classified information, that term, that
11 adjective "classified" is determined by the OCA, not by me.

12 DDC [LCDR BOGUCKI]: Yes, sir. As you said, there is a
13 distinction of something being classified and obligation of
14 defense counsel to treat it as classified. The protective
15 order would require us to treat it as clarified.

16 MJ [COL POHL]: You don't know standard of know or
17 reasonably should know treat as classified is a reasonable
18 standard to apply?

19 DDC [LCDR BOGUCKI]: Not when the guidance, not when the
20 guidance, as it appears in paragraph 7, is so unclear, so
21 all-encompassing.

22 When you take together all the various categories
23 under paragraph 7 Delta, then we are talking about everything

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 that happened to the accused since the time they came into
2 United States' control; their apprehension, their detention,
3 their interrogation, and the conditions of their confinement.

4 MJ [COL POHL]: Until 6 September 2006.

5 DDC [LCDR BOGUCKI]: Absolutely.

6 MJ [COL POHL]: You think this is an unreasonable
7 burden?

8 DDC [LCDR BOGUCKI]: Yes, sir. For the exact reasons I
9 described yesterday, sir. I'm not endorsing a piece of
10 information if I go to a witness and I say my client says
11 something happened to him in 2006 and that you were there. Is
12 that, in fact, the case? I'm passing on what my client said.
13 It clearly fits within the definitions of paragraph 7. I'm
14 not endorsing it. I'm in no way using my privileged status as
15 a holder of a Top Secret security clearance to give that some
16 sort of, you know, aura of credibility. What I'm doing is
17 using it in a proper way as defense counsel to investigate
18 potential defenses in my case.

19 Therefore, Your Honor, we would ask that whether
20 this information is purported to be classified elsewhere, we
21 ask that it simply not -- that we not be required to treat it
22 as classified pursuant to the terms of the protective order.

23 MJ [COL POHL]: But if the protective order is read to

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

1 only protect currently classified information, doesn't that
2 meet your goal?

3 DDC [LCDR BOGUCKI]: Not within the broad definition as
4 it exists under paragraph 7, Your Honor.

5 MJ [COL POHL]: Okay. I understand your position.
6 Thank you.

7 DDC [LCDR BOGUCKI]: Thank you, Your Honor.

8 MJ [COL POHL]: Mr. Nevin, your client has his hand up.
9 I really don't -- I'm not sure why.

10 DC [CDR RUIZ]: If I may, in the meantime, on behalf of
11 Mr. Hawsawi, we adopt all arguments and objections to 9 and
12 13.

13 MJ [COL POHL]: Anything you wish to add separately?

14 DC [CDR RUIZ]: No, Your Honor. I would just like to
15 adopt all arguments and objections on behalf of Mr. Hawsawi.

16 MJ [COL POHL]: Mr. Nevin, don't we raise 505(h) issues
17 right now if this were to occur? I don't know what he is
18 going to say. I don't know whether you do or not. Do you
19 understand? I'm not sure we can -- I will make it very clear.

20 I'm not restricting the accused's right to say
21 things. Given the nature of where we are at, we would have to
22 have a 505(h) hearing before we can determine whether or not
23 he can say it in open court, because you are telling me you

UNOFFICIAL/UNAUTHENTICATED TRANSCRIPT

Tab 9

**MILITARY COMMISSIONS TRIAL JUDICIARY
GUANTANAMO BAY, CUBA**

UNITED STATES OF AMERICA	AE 0130
v.	RULING
KHALID SHAIKH MOHAMMAD, WALID MUHAMMAD SALIH MUBARAK BIN ATTASH, RAMZI BINALSHIBH, ALI ABDUL-AZIZ ALI, MUSTAFA AHMED ADAM AL HAWSAWI	Government Motion To Protect Against Disclosure of National Security Information
	6 December 2012

1. The Government requested this Commission issue a Protective Order regulating the use and safeguarding of classified information during the pendency of *United States v. Khalid Shaikh Mohammad, Walid Muhammad Salih Mubarak BinAttash, Ramzi Binalshibh, Ali Abdul Aziz Ali, and Mustafa Ahmed Adam al Hawsawi*.

2. The American Civil Liberties Union and the American Civil Liberties Union Foundation (ACLU) subsequently filed an *amici* motion regarding "Public Access to Proceedings and Records" (AE 013A) challenging the portions of the Government's proposed protective order that, in their estimation, would permit the government to suppress accuseds' statements about their detention and treatment. Each of the accused adopted and joined the ACLU motion.

3. A response in opposition to the Government's motion was collectively filed by The Miami Herald, ABC, Inc., Associated Press, Bloomberg News, CBS Broadcasting, Inc., Fox News Network, The McClatchy Company, National Public Radio, The New York Times, The New Yorker, Reuters, Tribune Company, Wall Street Journal, and the Washington Post requesting this Commission deny the Government's request to deny public access to all records and proceedings involving any classified information as being overly broad.

4. Military Commission Rule of Evidence (M.C.R.E.) 505(e) directs that upon a motion by the Government, the military judge shall issue an order to “protect against the disclosure of any classified information that has been disclosed by the United States to any accused or counsel, regardless of the means by which the accused or counsel obtained the classified information, in any military commission under the M.C.A. or that has otherwise been provided to, or obtained by, any such accused in any such military commission.”

5. An alliance between this Commission rule and that applied generally in Article III criminal proceedings is established by M.C.R.E. 505 (a)(4) directing:

The judicial construction of the Classified Information Procedures Act (18 U.S.C. App.) shall be authoritative in the interpretation of this rule, except to the extent that such construction is inconsistent with the specific requirements of this rule.

6. The language of M.C.R.E. 505(e) closely parallels language from the Classified Information Procedures Act (CIPA) (18 U.S.C. App. (2000), enacted by P.L. 96-456 (Oct. 15, 1980), 94 Stat. 2025-32) stating:

§ 3. Protective Orders

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

and is reinforced by the Security Procedures Established Pursuant to PL 96-456, 94 Stat. 2025, by Chief Justice Burger:

Para 8

Except as otherwise authorized by a protective order, persons acting for the defendant will not be given custody of classified information provided by the government. They may, at the discretion of the court, be afforded access to classified information....

7. Based upon CIPA and the guidance of the Chief Justice, the use of protective orders is evidenced in most, if not all, cases involving national security since the inception of the Act. *U.S. v. Bin Laden*, 2001 WL 66393 S.D.NY, 2001; *U.S. v. Rezaq* 156 F.R.D. 514 (D.D.C. 1994); *U.S. v. Musa*, 833 F.Supp. 752 (E.D.MO. 1993). *Also see generally* Reagan, Robert Timothy, Federal Judicial Center, National Security Case Management (2011).

8. The Military Rules of Evidence (M.R.E.), used in courts-martial involving issues of national security, provide another reference point for the issuance of a protective order for classified information in a criminal trial. *U.S. v. Pruner* 33 M.J. 272 (C.M.A. 1991); *Schmidt v. Boone* 59 M.J. 841 (A.F.Ct.Crim.App. 2004). By its language and provisions, M.C.R.E. 505(e) is drawn directly in large part from M.R.E. 505 (g) and, while apparently used infrequently, a protective order can be used to frame classified discovery in courts-martial.

FINDINGS

1. A protective order directed by CIPA is a procedural predicate for providing discovery in cases concerning matters deemed of national security and has become *de rigueur* in Article III courts and courts-martial. (Protective Order *United States v Hanssen*, 5 Mar 2001(E.D. VA); Protective Order, *United States v Moussaoui*, 22 Jan 2002 (E.D. VA); Protective Order, *United States v Ghailani*, 21 Jul 2009, (S.D. NY); *and generally* Reagan, Robert Timothy, Federal Judicial Center, National Security Case Management (2011))The protective order is to guard against the compromise of classified material and generally serves as the security procedural guide for the case.

2. As a procedural guide, the protective order does not address the relevance, materiality, or admissibility of evidence. The propose protective order neither expands the traditional rules of discovery nor addresses what use, if any, can be made of the disclosed information during the course of a trial. Rather, it provides the framework for defense counsel to obtain and assess classified information while at the same instance permitting the Government to preserve information relevant to our national security. *U.S. v. Pappas* 94 F.3d 795 (E.D. NY),1996; *U.S. v. Aref* 533 F.3d 72 (N.D. NY),2008.

3. The draft protective order provided by the Government, while closely mirroring that used in *US v Ghailani* and other federal cases, is not totally appropriate for use in the Commissions. In Article III courts, a court security officer (CSO), at the direction of the judge, is made available to help the court address issues concerning the use of classified material during a trial. Many of the functions performed by the federal CSO are accomplished as part of the routine support mission of the Office of Military Commissions (OMC); these include obtaining security clearances, maintaining storage facilities for classified documents, and providing secure communication technology. In light of the OMC support, most of the provisions in the draft pertaining to the CSO are not applicable. In Article III courts, the CSO provides support to defense counsel to help them navigate the maze of security regulations. The Defense has requested assistance in this regard.

4. The Government's draft order does not specifically address the issue of defense counsel working together, to include sharing classified information, in preparing the presentation of a joint defense. As now styled the draft would seem to preclude counsel from freely sharing information as they develop joint trial strategy and tactics.

5. As part of their motion, the Government requested the Commission to institutionalize a practice that has been in use for several years- the so called "40 second rule." Because of the security constraints at the Expeditionary Legal Center courtroom (Courtroom 2) there is a 40 second delay between something said in the courtroom and when those viewing the trial in the gallery or at closed circuit television (CCTV) sites actually hear what was said. The ACLU and collective press, as well as the accused, object to this delay as an unwarranted closure of the court. The Commission is acutely aware of its twin responsibilities of insuring the transparency of the proceeding while at the same instance preserving the interests of national security. Commission finds the brief delay is the least intrusive and least disruptive method of meeting both responsibilities. The delay permits the Commission to assess and remedy any negligent or intentional disclosure of classified information without unduly impacting on the ability of the public and press to fully see and understand what is transpiring. *U.S. v. Lonetree*, 31 M.J. 849 (N.M.C.M.R. 1990); *Denver Post Corp. v. U.S.*, 2005 WL 6519929 (Army Ct.Crim.App. 2005).

6. In support of its motion the Government submitted declarations, filed ex parte and under seal, from representatives of the CIA, DoD, and FBI invoking the classified information privilege and explaining how disclosure of the classified information at issue would be detrimental to national security in that the information relates to the sources, methods, and activities by which the United States defends against international terrorism and terrorist organizations. This information is therefore properly classified by the executive branch pursuant to Executive Order 13526, as amended, or its predecessor Orders, and is subject to protection in connection with this military commission. *U.S. v. Musa* 833 F.Supp.752

A Protective Order will be issued forthwith.

So ORDERED this 6th day of December, 2012.



JAMES L. POHL
COL, JA, USA
Military Judge

Tab 10

**MILITARY COMMISSIONS TRIAL JUDICIARY
GUANTANAMO BAY, CUBA**

UNITED STATES OF AMERICA	AE 013P
v.	PROTECTIVE ORDER #1
KHALID SHAIKH MOHAMMAD, WALID MUHAMMAD SALIH MUBARAK BIN ATTASH, RAMZI BINALSHIBH, ALI ABDUL AZIZ ALI, MUSTAFA AHMED ADAM AL HAWSAWI	To Protect Against Disclosure of National Security Information
	6 December 2012

Upon consideration of the submissions regarding the Government's motion for a protective order to protect classified information in this case, the Commission finds this case involves classified national security information, including TOP SECRET / SENSITIVE COMPARTMENTED INFORMATION (SCI), the disclosure of which would be detrimental to national security, the storage, handling, and control of which requires special security precautions, and the access to which requires a security clearance and a need-to-know. Accordingly, pursuant to authority granted under 10 U.S.C. § 949p-1 to p-7, Rules for Military Commissions (R.M.C.) 701 and 806, Military Commissions Rule of Evidence (M.C.R.E.) 505, Department of Defense Regulation for Trial by Military Commissions (2011) ¶ 17-3, and the general judicial authority of the Commission, in order to protect the national security, and for good cause shown, the following Protective Order is entered.

1. SCOPE

a. This Protective Order establishes procedures applicable to all persons who have access to or come into possession of classified documents or information in connection with this case,

regardless of the means by which the persons obtained the classified information. These procedures apply to all aspects of pre-trial, trial, and post-trial stages in this case, including any appeals, subject to modification by further order of the Commission or orders issued by a court of competent jurisdiction.

b. This Protective Order applies to all information, documents, testimony, and material associated with this case that contain classified information, including but not limited to any classified pleadings, written discovery, expert reports, transcripts, notes, summaries, or any other material that contains, describes, or reflects classified information.

c. Counsel are responsible for advising their clients, translators, witnesses, experts, consultants, support staff, and all others involved with the defense or prosecution of this case, respectively, of the contents of this Protective Order.

2. DEFINITIONS

a. As used in this Protective Order, the term "Court Security Officer (CSO)" and "Assistant Court Security Officer (ACSO)" refer to security officers, appointed by the Military Judge, to serve as the security advisor to the judge, to oversee security provisions pertaining to the filing of motions, responses, replies, and other documents with the Commission, and to manage security during sessions of the Commission. The CSO and ACSO will be administered an oath IAW Rule 10, Military Commissions Rules of Court.

b. The term "Chief Security Manager, Office of Military Commissions" refers to the official within the Office of Military Commission responsible for all security requirements and missions of the Office of Military Commissions.

UNCLASSIFIED//FOR PUBLIC RELEASE

c. The term "Defense" includes any counsel for an accused in this case and any employees, contractors, investigators, paralegals, experts, translators, support staff, or other persons working on the behalf of an accused or his counsel in this case.

d. The term "Defense Security Officer" (DSO) refers to a security officer, serving as security advisor to the Defense, who oversees security provisions pertaining to the filing of motions, response, replies, and other documents with the Commission.

e. The term "Government" includes any counsel for the United States in this case and any employees, contractors, investigators, paralegals, experts, translators, support staff or other persons working on the behalf of the United States or its counsel in this case.

f. The words "documents" and "information" include, but are not limited to, all written or printed matter of any kind, formal or informal, including originals, conforming and non-conforming copies, whether different from the original by reason of notation made on such copies or otherwise, and further include, but are not limited to:

(1) papers, correspondence, memoranda, notes, letters, cables, reports, summaries, photographs, maps, charts, graphs, inter-office and intra-office communications, notations of any sort concerning conversations, meetings, or other communications, bulletins, teletypes, telegrams, facsimiles, invoices, worksheets, and drafts, alterations, modifications, changes, and amendments of any kind to the foregoing;

(2) graphic or oral records or representations of any kind, including, but not limited to: photographs, maps, charts, graphs, microfiche, microfilm, videotapes, and sound or motion picture recordings of any kind;

(3) electronic, mechanical, or electric records of any kind, including, but not limited to: tapes, cassettes, disks, recordings, electronic mail, instant messages, films, typewriter

ribbons, word processing or other computer tapes, disks or portable storage devices, and all manner of electronic data processing storage; and

(4) information acquired orally.

g. The terms “classified national security information and/or documents,” “classified information,” and “classified documents” include:

(1) any classified document or information that was classified by any Executive Branch agency in the interests of national security or pursuant to Executive Order, including Executive Order 13526, as amended, or its predecessor Orders, as “CONFIDENTIAL,” “SECRET,” “TOP SECRET,” or additionally controlled as “SENSITIVE COMPARTMENTED INFORMATION (SCI);”

(2) any document or information, regardless of its physical form or characteristics, now or formerly in the possession of a private party that was derived from United States Government information that was classified, regardless of whether such document or information has subsequently been classified by the Government pursuant to Executive Order, including Executive Order 13526, as amended, or its predecessor Orders, as “CONFIDENTIAL,” “SECRET,” “TOP SECRET,” or additionally controlled as “SENSITIVE COMPARTMENTED INFORMATION (SCI);”

(3) verbal or non-documentary classified information known to an accused or the Defense;

(4) any document or information as to which the Defense has been notified orally or in writing that such document or information contains classified information, including, but not limited to the following:

UNCLASSIFIED//FOR PUBLIC RELEASE

(a) Information that would reveal or tend to reveal details surrounding the capture of an accused other than the location and date;

(b) Information that would reveal or tend to reveal the foreign countries in which: Khalid Shaikh Mohammad and Mustafa Ahmed Adam al Hawsawi were detained from the time of their capture on or about 1 March 2003 through 6 September 2006; Walid Muhammad Salih Bin Attash and Ali Abdul Aziz Ali were detained from the time of their capture on or about 29 April 2003 through 6 September 2006; and Ramzi Binalshibh was detained from the time of his capture on or around 11 September 2002 through 6 September 2006.

(c) The names, identities, and physical descriptions of any persons involved with the capture, transfer, detention, or interrogation of an accused or specific dates regarding the same, from on or around the aforementioned capture dates through 6 September 2006;

(d) The enhanced interrogation techniques that were applied to an accused from on or around the aforementioned capture dates through 6 September 2006, including descriptions of the techniques as applied, the duration, frequency, sequencing, and limitations of those techniques; and

(e) Descriptions of the conditions of confinement of any of the accused from on or around the aforementioned capture dates through 6 September 2006;

(5) In addition, the term "information" shall include, without limitation, observations and experiences of an accused with respect to the matters set forth in subparagraphs 2g(4)(a)-(e), above.

(6) any document or information obtained from or related to a foreign government or dealing with matters of U.S. foreign policy, intelligence, or military operations, which is known to be closely held and potentially damaging to the national security of the United States or its allies.

h. "National Security" means the national defense and foreign relations of the United States.

i. "Access to classified information" means having authorized access to review, read, learn, or otherwise come to know classified information.

j. "Secure area" means a physical facility accredited or approved for the storage, handling, and control of classified information.

kj. "Unauthorized disclosure of classified information" means any knowing, willful, or negligent action that could reasonably be expected to result in a communication or physical transfer of classified information to an unauthorized recipient. Confirming or denying information, including its very existence, constitutes disclosing that information.

3. COURT SECURITY OFFICER

a. A Court Security Officer (CSO) and Assistant Court Security Officer(s) (ACSO) for this case have been designated by the Military Judge.

b. The CSO and any ACSO are officers of the court. *Ex parte* communication by a party in a case, to include the Office of Military Commissions, DoD General Counsel or any intelligence or law enforcement agency, with the CSO/ASCO is prohibited except as authorized by the M.C.A. or the M.M.C. This is to preclude any actual or perceived attempt to improperly influence the Commission in violation of 10 U.S.C. § 949b. This does not include administrative

matters necessary for the management of the security responsibilities of the Office of Trial Judiciary.

c. The CSO/ACSO shall ensure that all classified or protected evidence and information is appropriately safeguarded at all times during Commission proceedings and that only personnel with the appropriate clearances and authorizations are present when classified or protected evidence is presented before Military Commissions.

d. The CSO shall consult with the original classification authority (OCA) of classified documents or information, as necessary, to address classification decisions or other related issues.

4. DEFENSE SECURITY OFFICER

a. Upon request of defense counsel for an accused, the Convening Authority shall provide a Defense Security Officer for the defendant

b. The Defense Security Officer is, for limited purposes associated with this case, a member of the defense team, and therefore shall not disclose to any person any information provided by the defense, other than information provided in a filing with the court. In accordance with MCRE 502, the Defense Security Officer shall not reveal to any person the content of any conversations he hears by or among the defense, nor reveal the nature of documents being reviewed by them or the work generated by them, except as necessary to report violations of classified handling or dissemination regulations or any Protective Order issued in this case, to the Military Judge. Additionally, the presence of the Defense Security Officer, who

has been appointed as a member of the defense team, shall not be construed to waive, limit, or otherwise render inapplicable the attorney-client privilege or work product protections.

c. The Defense Security Officer shall perform the following duties:

(1) Assist the defense with applying classification guides, including reviewing pleadings and other papers prepared by the defense to ensure they are unclassified or properly marked as classified.

(2) Assist the defense in performing their duty to apply derivative classification markings pursuant to E.O. 13526 § 2.1(b).

(3) Ensure compliance with the provisions of any Protective Order.

d. Any CSO or other security entity shall not disclose to any other entity any information provided by a Defense Security Officer, including any component of the Office of Military Commissions, except that the entity may inform the military judge of any information that presents a current threat to loss of life or presents an immediate safety issue in the detention facility. This does not include administrative matters necessary for the management of the security responsibilities of the Office of Military Commissions.

5. ACCESS TO CLASSIFIED INFORMATION

a. Without authorization from the Government, no member of the Defense, including defense witnesses, shall have access to classified information in connection with this case unless that person has:

(1) received the necessary security clearance from the appropriate Department of Defense (DoD) authorities and signed an appropriate non-disclosure agreement, as verified by the Chief Security Manager, Office of Military Commissions;

UNCLASSIFIED//FOR PUBLIC RELEASE

(2) signed the Memorandum of Understanding Regarding Receipt of Classified Information (MOU), attached to this Protective Order, agreeing to comply with the terms of this Protective Order; and

(3) a need-to-know for the classified information at issue, as determined by the Original Classification Authority (OCA) for that information.

b. In order to be provided access to classified information in connection with this case, each member of the Defense shall execute the attached MOU, file the executed originals of the MOU with the Chief Security Manager, Office of Military Commissions, and submit copies to the CSO and counsel for the Government. The execution and submission of the MOU is a condition precedent to the Defense having access to classified information for the purposes of these proceedings.

c. The substitution, departure, or removal of any member of the Defense, including defense witnesses, from this case for any reason shall not release that person from the provisions of this Protective Order or the MOU executed in connection with this Protective Order.

d. Once the Chief Security Manager, Office of Military Commissions verifies that counsel for the accused have executed and submitted the MOU, and are otherwise authorized to receive classified information in connection with this case, the Government may provide classified discovery to the Defense.

e. All classified documents or information provided or obtained in connection with this case remain classified at the level designated by the OCA, unless the documents bear a clear indication that they have been declassified. The person receiving the classified documents or information, together with all other members of the Defense or the Government, respectively, shall be responsible for protecting the classified information from disclosure and shall ensure

that access to and storage of the classified information is in accordance with applicable laws and regulations and the terms of this Protective Order.

f. No member of the Defense, including any defense witness, is authorized to disclose any classified information obtained during this case, outside the immediate parameters of these military commission proceedings. If any member of the Defense, any accused, or any defense witness receives any summons, subpoena, or court order, or the equivalent thereof, from any United States or foreign court or on behalf of any criminal or civil investigative entity within the United States or from any foreign entity, the Defense, including defense witnesses, shall immediately notify the Commission, the Chief Security Manager, Office of Military Commissions, and the Government so that appropriate consideration can be given to the matter by the Commission and the OCA of the materials concerned. Absent authority from the Commission or the Government, the Defense, an accused, and defense witnesses are not authorized to disseminate or disclose classified materials in response to such requests. The Defense, an accused, and defense witnesses and experts are not authorized to use or refer to any classified information obtained as a result of their participation in commission proceedings in any other forum, or in a military commission proceeding involving another detainee.

6. USE, STORAGE, AND HANDLING PROCEDURES

a. The Office of the Chief Defense Counsel, Office of Military Commissions, has approved secure areas in which the Defense may use, store, handle, and otherwise work with classified information. The Chief Security Manager, Office of Military Commissions, shall ensure that such secure areas are maintained and operated in a manner consistent with this Protective Order and as otherwise reasonably necessary to protect against the disclosure of classified information.

UNCLASSIFIED//FOR PUBLIC RELEASE

b. All classified information provided to the Defense, and otherwise possessed or maintained by the Defense, shall be stored, maintained, and used only in secure areas. Classified information may only be removed from secure areas in accordance with this Protective Order and applicable laws and regulations governing the handling and use of classified information.

c. Consistent with other provisions of this Protective Order, the Defense shall have access to the classified information made available to them and shall be allowed to take notes and prepare documents with respect to such classified information in secure areas.

d. The Defense shall not copy or reproduce any classified information in any form, except in secure areas and in accordance with this Protective Order and applicable laws and regulations governing the reproduction of classified information.

e. All documents prepared by the Defense that are known or believed to contain classified information—including, without limitation, notes taken or memoranda prepared by counsel and pleadings or other documents intended for filing with the Commission—shall be transcribed, recorded, typed, duplicated, copied, or otherwise prepared only by persons possessing an appropriate approval for access to such classified information. Such activities shall take place in secure areas, on approved word processing equipment, and in accordance with procedures approved by the Chief Security Manager, Office of Military Commissions. All such documents and any associated materials containing classified information—such as notes, memoranda, drafts, copies, typewriter ribbons, magnetic recordings, and exhibits—shall be maintained in secure areas unless and until the Chief Security Officer, Office of Military Commissions, advises that those documents or associated materials are unclassified in their entirety. None of these materials shall be disclosed to the Government unless authorized by the Commission, by counsel for an accused, or as otherwise provided in this Protective Order.

UNCLASSIFIED//FOR PUBLIC RELEASE

f. The Defense may discuss classified information only within secure areas and shall not discuss, disclose, or disseminate classified information over any non-secure communication system, such as standard commercial telephones, office intercommunication systems, or non-secure electronic mail.

g. The Defense shall not disclose any classified documents or information to any person, including counsel in related cases of Guantanamo Bay detainees in military commissions or other courts (including, but not limited to, habeas proceedings), except those persons authorized by this Protective Order, the Commission, and counsel for the Government with the appropriate clearances and the need-to-know that information. The Commission recognizes that the presentation of a joint defense may necessitate disclosure on a need to know basis to counsel for co-accused.

h. To the extent the Defense is not certain of the classification of information it wishes to disclose, the Defense shall follow procedures established by the Office of Military Commissions for a determination as to its classification. In any instance in which there is any doubt as to whether information is classified, the Defense must consider the information classified unless and until it receives notice from the Chief Security Manager, Office of Military Commissions such information is not classified.

i. Until further order of this Commission, the Defense shall not disclose to an accused any classified information not previously provided by an accused to the Defense, except where such information has been approved for release to an accused and marked accordingly.

j. Except as otherwise stated in this paragraph, and to ensure the national security of the United States, at no time, including any period subsequent to the conclusion of these proceedings, shall the Defense make any public or private statements disclosing any classified

information accessed pursuant to this Protective Order, or otherwise obtained in connection with this case, including the fact that any such information or documents are classified. In the event classified information enters the public domain without first being properly declassified by the United States Government, counsel are reminded they may not make public or private statements about the information if the information is classified. (See paragraph 2 of this Protective Order for specific examples of information which remains classified even if it is in the public domain). In an abundance of caution and to help ensure clarity on this matter, the Commission emphasizes that counsel shall not be the source of any classified information entering the public domain, nor should counsel comment on information which has entered the public domain but which remains classified.

7. PROCEDURES FOR FILING DOCUMENTS

- a. See Rule 3, Motion Practice, Military Commissions Trial Judiciary Rules of Court.
- b. For all filings, other than those filed pursuant to M.C.R E. 505, in which counsel know, reasonably should know, or are uncertain as to whether the filing contains classified information or other information covered by Chapter 19-3(b), DoD Regulation for Trial By Military Commission, counsel shall submit the filing by secure means under seal with the Chief Clerk of the Trial Judiciary.
- c. Documents containing classified information or information the defense counsel believes to be classified shall be filed pursuant to the procedures specified for classified information.
- d. Classified filings must be marked with the appropriate classification markings on each page, including classification markings for each paragraph. If a party is uncertain as to the appropriate classification markings for a document, the party shall seek guidance from the Chief

Security Officer, Office of Military Commissions, who will consult with the OCA of the information or other appropriate agency, as necessary, regarding the appropriate classification.

e All original filings will be maintained by the Director, Office of Court Administration, as part of the Record of Trial. The Office of Court Administration shall ensure any classified information contained in such filings is maintained under seal and stored in an appropriate secure area consistent with the highest level of classified information contained in the filing.

f. Under no circumstances may classified information be filed in an otherwise unclassified filing except as a separate classified attachment. In the event a party believes an unsealed filing contains classified information, the party shall immediately notify the Chief Security Manager, Office of Military Commissions, and CSO/ACSO, who shall take appropriate action to retrieve the documents or information at issue. The filing will then be treated as containing classified information unless and until determined otherwise. Nothing herein limits the Government's authority to take other remedial action as necessary to ensure the protection of the classified information.

g. Nothing herein requires the Government to disclose classified information. Additionally, nothing herein prevents the Government or Defense from submitting classified information to the Commission *in camera* or *ex parte* in these proceedings or accessing such submissions or information filed by the other party. Except as otherwise authorized by the Military Judge, the filing party shall provide the other party with notice on the date of the filing.

8. PROCEDURES FOR MILITARY COMMISSION PROCEEDINGS

a. Except as provided herein, and in accordance with M.C.R.E. 505, no party shall disclose or cause to be disclosed any information known or believed to be classified in connection with any hearing or proceeding in this case.

(1) Notice Requirements

(a) The parties must comply with all notice requirements under M.C.R.E. 505 prior to disclosing or introducing any classified information in this case.

(b) Because statements of an accused may contain information classified as TOP SECRET/SCI, the Defense must provide notice in accordance with this Protective Order and M.C.R.E. 505(g) if an accused intends to make statements or offer testimony at any proceeding.

(2) Closed Proceedings

(a) While proceedings shall generally be publicly held, the Commission may exclude the public from any proceeding, *sua sponte* or upon motion by either party, in order to protect information, the disclosure of which could reasonably be expected to damage national security. If the Commission closes the courtroom during any proceeding in order to protect classified information from disclosure, no person may remain who is not authorized to access classified information in accordance with this Protective Order, which the CSO shall verify prior to the proceeding.

(b) No participant in any proceeding, including the Government, Defense, accused, witnesses, and courtroom personnel, may disclose classified information, or any information that tends to reveal classified information, to any person not authorized to access such classified information in connection with this case.

(3) Delayed Broadcast of Open Proceedings

(a) Due to the nature and classification level of the classified information in this case, the Commission finds that to protect against the unauthorized disclosure of classified information during proceedings open to the public, it will be necessary to employ a forty-second delay in the broadcast of the proceedings from the courtroom to the public gallery. This is the least disruptive method of both insuring the continued protection of classified information while providing the maximum in public transparency.

(b) Should classified information be disclosed during any open proceeding, this delay will allow the Military Judge, CSO, or Government to take action to suspend the broadcast—including any broadcast of the proceedings to locations other than the public gallery of the courtroom (e.g., any closed-circuit broadcast of the proceedings to a remote location)—so that the classified information will not be disclosed to members of the public.

(c) The broadcast may be suspended whenever it is reasonably believed that any person in the courtroom has made or is about to make a statement or offer testimony disclosing classified information.

(d) The Commission shall be notified immediately if the broadcast is suspended. In that event, and otherwise if necessary, the Commission may stop the proceedings to evaluate whether the information disclosed, or about to be disclosed, is classified information as defined in this Protective Order. The Commission may also conduct an *in camera* hearing to address any such disclosure of classified information.

(4) Other Protections

(a) During the examination of any witness, the Government may object to any question or line of inquiry that may require the witness to disclose classified information not found previously to be admissible by the Commission. Following such an objection, the

Commission will determine whether the witness's response is admissible and, if so, may take steps as necessary to protect against the public disclosure of any classified information contained therein.

(b) Classified information offered or admitted into evidence will remain classified at the level designated by the OCA and will be handled accordingly. All classified evidence offered or accepted during trial will be kept under seal, even if such evidence was inadvertently disclosed during a proceeding. Exhibits containing classified information may also be sealed after trial as necessary to prevent disclosure of such classified information.

(5) Record of Trial

(a) It is the responsibility of the Government, IAW 10 U.S.C § 9481(c) to control and prepare the Record of Trial. What is included in the Record of Trial is set out by R.M.C. 1103. The Director, Office of Court Administration, shall ensure that the Record of Trial is reviewed and redacted as necessary to protect any classified information from public disclosure.

(b) The Director, Office of Court Administration, shall ensure portions of the Record of Trial containing classified information remain under seal and are properly segregated from the unclassified portion of the transcripts, properly marked with the appropriate security markings, stored in a secure area, and handled in accordance with this Protective Order.

9. UNAUTHORIZED DISCLOSURE

a. Any unauthorized disclosure of classified information may constitute a violation of United States criminal laws. Additionally, any violation of the terms of this Protective Order shall immediately be brought to the attention of the Commission and may result in disciplinary action or other sanctions, including a charge of contempt of the Commission and possible

referral for criminal prosecution. Any breach of this Protective Order may also result in the termination of access to classified information. Persons subject to this Protective Order are advised that unauthorized disclosure, retention, or negligent handling of classified documents or information could cause damage to the national security of the United States or may be used to the advantage of an adversary of the United States or against the interests of the United States. The purpose of this Protective Order is to ensure those authorized to receive classified information in connection with this case will never divulge that information to anyone not authorized to receive it, without prior written authorization from the OCA and in conformity with this Order.


b. The Defense shall promptly notify the Chief Security Officer, Office of Military Commissions, upon becoming aware of any unauthorized access to or loss, theft, or other disclosure of classified information, and shall take all reasonably necessary steps to retrieve such classified information and protect it from further unauthorized disclosure or dissemination.

10. SURVIVAL OF ORDER

a. The terms of this Protective Order and any signed MOU shall survive and remain in effect after the termination of this case unless otherwise determined by a court of competent jurisdiction.

b. This Protective Order is entered without prejudice to the right of the parties to seek such additional protections or exceptions to those stated herein as they deem necessary.

So ORDERED this 6th day of December, 2012.



JAMES L. POHL
COL, JA, USA
Military Judge

MILITARY COMMISSIONS TRIAL JUDICIARY
GUANTANAMO BAY, CUBA

UNITED STATES OF AMERICA)	
)	
v.)	Memorandum of Understanding
)	Regarding the Receipt of Classified
)	Information
KHALID SHAIKH MOHAMMAD;)	
WALID MUHAMMAD SALIH)	
MUBARAK BIN ATTASH;)	
RAMZI BINALSHIBH;)	
ALI ABDUL AZIZ ALI;)	
MUSTAFA AHMED ADAM AL)	
HAWSAWI)	

I, _____, [print or type full name], have been provided a copy of and have read Protective Order #1 relating to the protection of classified information in the above-captioned case, and agree to be bound by the terms of that order. I understand that in connection with this case I will receive classified documents and information that are protected pursuant to both the terms of the Protective Order and the applicable laws and regulations governing the use, storage, and handling of classified information. I also understand that the classified documents and information are the property of the United States and refer or relate to the national security of the United States.

I agree that I will not use or disclose any classified documents or information, except in strict compliance with the provisions of the Protective Order and the applicable laws and regulations governing the use, storage, and handling of classified information. I have further familiarized myself with the statutes, regulations, and orders relating to the unauthorized disclosure of classified information, espionage, and other related criminal offenses, including but

UNCLASSIFIED//FOR PUBLIC RELEASE

not limited to 50 U.S.C. § 421; 18 U.S.C. § 641; 18 U.S.C. § 793; 50 U.S.C. § 783; and Executive Order 13526.

I agree to take all reasonable precautions to prevent any unauthorized use or disclosure of any classified documents or information in my possession or control. I understand that failure to comply with this Memorandum of Understanding Regarding the Receipt of Classified Information (MOU) or any protective order entered in this case could result in sanctions or other consequences, including criminal consequences. I understand that the terms of this MOU shall survive and remain in effect after the termination of this case, and that any termination of my involvement in this case prior to its conclusion will not relieve me from the terms of this MOU or any protective order entered in the case.

I make the above statements under penalty of perjury.

Signature

Date

Witness

Date

Witness

Date

Tab 11

**MILITARY COMMISSIONS TRIAL JUDICIARY
GUANTANAMO BAY, CUBA**

UNITED STATES OF AMERICA v. KHALID SHAIKH MOHAMMAD, WALID MUHAMMAD SALIH MUBARAK BIN ATTASH, RAMZI BINALSHIBH, ALI ABDUL-AZIZ ALI, MUSTAFA AHMED ADAM AL HAWSAWI	AE 013Z SUPPLEMENTAL RULING Government Motion To Protect Against Disclosure of National Security Information 9 February 2013
--	---

1. This Commission issued Protective Order #1 on 6 December 2013 (AE 013P) regulating the use and safeguarding of classified information during the pendency of *United States v. Khalid Shaikh Mohammad, Walid Muhammad Salih Mubarak BinAttash, Ramzi Binalshibh, Ali Abdul Aziz Ali, and Mustafa Ahmed Adam al Hawsawi*.

2. Subsequently, and at the invitation of the Commission, the Defense filed four motions to amend Protective Order #1.

a. A Motion to Reconsider Definition of “Unauthorized Disclosure” in AE013P Protective Order #1 (AE013R) in which they ask the Commission to reconsider the definition of “unauthorized disclosure of classified information” in paragraph 2 (k) of the Order to eliminate the phrase “including its very existence.”

b. A Motion to Reconsider Need-to-Know Provision in Protective Order #1 (AE013S) in which they ask the Commission to reconsider the need-to-know provision in Paragraph 5(a)(3) of the Order to eliminate the requirement for determination by Original Classification Authority.

c. A Motion to Amend Protective Order #1 Memorandum of Understanding and Related Language (AE013T) in which they ask the Commission to change paragraph 5(a)(2) by

substituting “acknowledging a duty” for the word “agreeing,” as well as making a comparable change to the requisite Memorandum of Understanding, and, in the Memorandum changing recognition of the possible penalties for failure to comply with “any protective order” to specify “Protective Order #1

d. A Motion to Strike The Testimonial Notice Requirement of Protective Order #1 (AE013U) in which they ask the Commission to delete the language of Paragraph 8 (1)(b) of the Order requiring the Accused to provide notice of all statements or testimony at any proceeding, regardless of classification.

3. The Government filed a response to each of the Defense motions for amendment of Protective Order #1:

a. As to the motion to redefine “Unauthorized Disclosure” (AE013R) the Government took the stance (AE013R-1) that current language of paragraph 2(k) is proper as a matter of law and security policy and correctly describes the definition of “unauthorized disclosure of classified information.” Their rationale is that if the existence of a fact is classified, then acknowledging its very existence would constitute an unauthorized disclosure.

b. As to the motion (AE 013S) to reconsider the need-to-know provision in Paragraph 5(a)(3) of the Order to eliminate the requirement for determination by Original Classification Authority the Government’s response (AE 013S-1) requested the Commission to deny the motion asserting paragraph 5(a)(3) is proper as a matter of law and security policy in that members of the defense team are not in a position to make a “need-to-know” determination regarding classified information and further Defense does not have a "need-to-know" for classified information and is not authorized to receive such classified information unless the information is discoverable.

c. As to the motion to amend Protective Order #1 (AE013T) the Government took the position (AE013T-1) that by agreeing to comply with the terms of the Order does not mean that Defense acquiesces in its propriety and that agreeing to comply with or be bound by any

protective orders in this case does not constitute waiver when Defense has made timely objections to the Memorandum of Understanding and Related Language.

d. As to the motion to delete the notice requirement of the Protective Order #1 (AE013U) the Government response (AE013U-1), requesting denial, asserts the notice provision in paragraph 8(a)(1)(b) of the Order is consistent with the notice requirement found in Military Commissions Rule of Evidence (M.C.R.E.) 505(g), which is modeled after Section 5 of the Classified Information Procedures Act 18 U.S.C. App. 3(CIPA).

FINDINGS

1. The Defense motion (AE 013 R) to amend paragraph 2(k) of the Order is granted in part with the agreement of the Government; the language to be substituted is from the Government Response (AE 013R-1). Unofficial/Unauthenticated Transcript of the Khalid Shaikh Mohammad, et al. (2) Hearing Dated 1/28/2013 from 10:49 AM to 11:51 AM, p 1383.
2. The Defense motion (AE 013S) to amend paragraph 5 (a) (3) of the Order is denied predicated upon the representations of the Government that the provisions of the cited paragraph are an “overarching” caveat pertaining to individuals outside the defense team and do not address the sharing of information between members of a Defense “team” or, in the instance of a joint defense, among the Defense “teams.” Unofficial/Unauthenticated Transcript of the Khalid Shaikh Mohammad, et al. (2) Hearing Dated 1/28/2013 from 10:49 AM to 11:51 AM, pp 1405-1406.
3. The Defense motion (AE013T) to amend both the Order and the accompanying Memorandum of Understanding is granted in part. The Memorandum will be changed to reflect that is’

provision pertains only to the terms of Protective Order #1 thereby affording the Defense opportunity to offer comment for the record on any additional protective orders. As to changing the language of the Order the motion is denied; the Defense has noted for the record, through both oral argument and written response, their disagreement with the language of the Order. That being said the Defense must agree to the terms of the Order to facilitate discovery of classified materials.

4. The Defense motion (AE 013 U) to amend the language of paragraph 8(a)(1)(b) of the Order is granted . The notice provisions of paragraph 505(g), Manual for Military Commissions and the 40 second delay authorized by the Protective Order, used to buffer the unauthorized disclosure of classified information, provide necessary protections for the Government in that regard.

Unofficial/Unauthenticated Transcript of the Khalid Shaikh Mohammad et al. (2) Hearing Dated 1/29/2013 from 9:09 AM to 10:08 AM, pp 1499-1531.

An Amended Protective Order and Memorandum of Agreement will be issued forthwith.

So ORDERED this 9th day of February, 2013.

//original signed//
JAMES L. POHL
COL, JA, USA
Military Judge

Tab 12

**MILITARY COMMISSIONS TRIAL JUDICIARY
GUANTANAMO BAY, CUBA**

<p>UNITED STATES OF AMERICA</p> <p>v.</p> <p>KHALID SHAIKH MOHAMMAD, WALID MUHAMMAD SALIH MUBARAK BIN ATTASH, RAMZI BINALSHIBH, ALI ABDUL AZIZ ALI, MUSTAFA AHMED ADAM AL HAWSAWI</p>	<p>AE 013AA</p> <p><i>Amended</i></p> <p>PROTECTIVE ORDER #1</p> <p>To Protect Against Disclosure of National Security Information</p> <p>9 February 2013</p>
---	--

Upon consideration of the submissions regarding the Government's motion for a protective order to protect classified information in this case, the Commission finds this case involves classified national security information, including TOP SECRET / SENSITIVE COMPARTMENTED INFORMATION (SCI), the disclosure of which would be detrimental to national security, the storage, handling, and control of which requires special security precautions, and the access to which requires a security clearance and a need-to-know. Accordingly, pursuant to authority granted under 10 U.S.C. § 949p-1 to p-7, Rules for Military Commissions (R.M.C.) 701 and 806, Military Commissions Rule of Evidence (M.C.R.E.) 505, Department of Defense Regulation for Trial by Military Commissions (2011) ¶ 17-3, and the general judicial authority of the Commission, in order to protect the national security, and for good cause shown, the following Protective Order is entered.

1. SCOPE

a. This Protective Order establishes procedures applicable to all persons who have access to or come into possession of classified documents or information in connection with this case,

regardless of the means by which the persons obtained the classified information. These procedures apply to all aspects of pre-trial, trial, and post-trial stages in this case, including any appeals, subject to modification by further order of the Commission or orders issued by a court of competent jurisdiction.

b. This Protective Order applies to all information, documents, testimony, and material associated with this case that contain classified information, including but not limited to any classified pleadings, written discovery, expert reports, transcripts, notes, summaries, or any other material that contains, describes, or reflects classified information.

c. Counsel are responsible for advising their clients, translators, witnesses, experts, consultants, support staff, and all others involved with the defense or prosecution of this case, respectively, of the contents of this Protective Order.

2. DEFINITIONS

a. As used in this Protective Order, the term "Court Security Officer (CSO)" and "Assistant Court Security Officer (ACSO)" refer to security officers, appointed by the Military Judge, to serve as the security advisor to the judge, to oversee security provisions pertaining to the filing of motions, responses, replies, and other documents with the Commission, and to manage security during sessions of the Commission. The CSO and ACSO will be administered an oath IAW Rule 10, Military Commissions Rules of Court.

b. The term "Chief Security Manager, Office of Military Commissions" refers to the official within the Office of Military Commission responsible for all security requirements and missions of the Office of Military Commissions.

c. The term “Defense” includes any counsel for an accused in this case and any employees, contractors, investigators, paralegals, experts, translators, support staff, or other persons working on the behalf of an accused or his counsel in this case.

d. The term “Defense Security Officer” (DSO) refers to a security officer, serving as security advisor to the Defense, who oversees security provisions pertaining to the filing of motions, response, replies, and other documents with the Commission.

e. The term “Government” includes any counsel for the United States in this case and any employees, contractors, investigators, paralegals, experts, translators, support staff or other persons working on the behalf of the United States or its counsel in this case.

f. The words “documents” and “information” include, but are not limited to, all written or printed matter of any kind, formal or informal, including originals, conforming and non-conforming copies, whether different from the original by reason of notation made on such copies or otherwise, and further include, but are not limited to:

(1) papers, correspondence, memoranda, notes, letters, cables, reports, summaries, photographs, maps, charts, graphs, inter-office and intra-office communications, notations of any sort concerning conversations, meetings, or other communications, bulletins, teletypes, telegrams, facsimiles, invoices, worksheets, and drafts, alterations, modifications, changes, and amendments of any kind to the foregoing;

(2) graphic or oral records or representations of any kind, including, but not limited to: photographs, maps, charts, graphs, microfiche, microfilm, videotapes, and sound or motion picture recordings of any kind;

(3) electronic, mechanical, or electric records of any kind, including, but not limited to: tapes, cassettes, disks, recordings, electronic mail, instant messages, films, typewriter

ribbons, word processing or other computer tapes, disks or portable storage devices, and all manner of electronic data processing storage; and

(4) information acquired orally.

g. The terms “classified national security information and/or documents,” “classified information,” and “classified documents” include:

(1) any classified document or information that was classified by any Executive Branch agency in the interests of national security or pursuant to Executive Order, including Executive Order 13526, as amended, or its predecessor Orders, as “CONFIDENTIAL,” “SECRET,” “TOP SECRET,” or additionally controlled as “SENSITIVE COMPARTMENTED INFORMATION (SCI);”

(2) any document or information, regardless of its physical form or characteristics, now or formerly in the possession of a private party that was derived from United States Government information that was classified, regardless of whether such document or information has subsequently been classified by the Government pursuant to Executive Order, including Executive Order 13526, as amended, or its predecessor Orders, as “CONFIDENTIAL,” “SECRET,” “TOP SECRET,” or additionally controlled as “SENSITIVE COMPARTMENTED INFORMATION (SCI);”

(3) verbal or non-documentary classified information known to an accused or the Defense;

(4) any document or information as to which the Defense has been notified orally or in writing that such document or information contains classified information, including, but not limited to the following:

UNCLASSIFIED//FOR PUBLIC RELEASE

(a) Information that would reveal or tend to reveal details surrounding the capture of an accused other than the location and date;

(b) Information that would reveal or tend to reveal the foreign countries in which: Khalid Shaikh Mohammad and Mustafa Ahmed Adam al Hawsawi were detained from the time of their capture on or about 1 March 2003 through 6 September 2006; Walid Muhammad Salih Bin Attash and Ali Abdul Aziz Ali were detained from the time of their capture on or about 29 April 2003 through 6 September 2006; and Ramzi Binalshibh was detained from the time of his capture on or around 11 September 2002 through 6 September 2006.

(c) The names, identities, and physical descriptions of any persons involved with the capture, transfer, detention, or interrogation of an accused or specific dates regarding the same, from on or around the aforementioned capture dates through 6 September 2006;

(d) The enhanced interrogation techniques that were applied to an accused from on or around the aforementioned capture dates through 6 September 2006, including descriptions of the techniques as applied, the duration, frequency, sequencing, and limitations of those techniques; and

(e) Descriptions of the conditions of confinement of any of the accused from on or around the aforementioned capture dates through 6 September 2006;

(5) In addition, the term “information” shall include, without limitation, observations and experiences of an accused with respect to the matters set forth in subparagraphs 2g(4)(a)-(e), above.

(6) any document or information obtained from or related to a foreign government or dealing with matters of U.S. foreign policy, intelligence, or military operations, which is known to be closely held and potentially damaging to the national security of the United States or its allies.

h. “National Security” means the national defense and foreign relations of the United States.

i. “Access to classified information” means having authorized access to review, read, learn, or otherwise come to know classified information.

j. “Secure area” means a physical facility accredited or approved for the storage, handling, and control of classified information.

k. “Unauthorized disclosure of classified information” means any knowing, willful, or negligent action that could reasonably be expected to result in a communication or physical transfer of classified information to an unauthorized recipient. Confirming or denying information, *where the very existence of the information is classified*, constitutes disclosing that information.

3. COURT SECURITY OFFICER

a. A Court Security Officer (CSO) and Assistant Court Security Officer(s) (ACSO) for this case have been designated by the Military Judge.

b. The CSO and any ACSO are officers of the court. *Ex parte* communication by a party in a case, to include the Office of Military Commissions, DoD General Counsel or any intelligence or law enforcement agency, with the CSO/ASCO is prohibited except as authorized by the M.C.A. or the M.M.C. This is to preclude any actual or perceived attempt to improperly influence the Commission in violation of 10 U.S.C. § 949b. This does not include administrative

matters necessary for the management of the security responsibilities of the Office of Trial Judiciary.

c. The CSO/ACSO shall ensure that all classified or protected evidence and information is appropriately safeguarded at all times during Commission proceedings and that only personnel with the appropriate clearances and authorizations are present when classified or protected evidence is presented before Military Commissions.

d. The CSO shall consult with the original classification authority (OCA) of classified documents or information, as necessary, to address classification decisions or other related issues.

4. DEFENSE SECURITY OFFICER

a. Upon request of defense counsel for an accused, the Convening Authority shall provide a Defense Security Officer for the defendant

b. The Defense Security Officer is, for limited purposes associated with this case, a member of the defense team, and therefore shall not disclose to any person any information provided by the defense, other than information provided in a filing with the court. In accordance with MCRE 502, the Defense Security Officer shall not reveal to any person the content of any conversations he hears by or among the defense, nor reveal the nature of documents being reviewed by them or the work generated by them, except as necessary to report violations of classified handling or dissemination regulations or any Protective Order issued in this case, to the Military Judge. Additionally, the presence of the Defense Security Officer, who

has been appointed as a member of the defense team, shall not be construed to waive, limit, or otherwise render inapplicable the attorney-client privilege or work product protections.

c. The Defense Security Officer shall perform the following duties:

(1) Assist the defense with applying classification guides, including reviewing pleadings and other papers prepared by the defense to ensure they are unclassified or properly marked as classified.

(2) Assist the defense in performing their duty to apply derivative classification markings pursuant to E.O. 13526 § 2.1(b).

(3) Ensure compliance with the provisions of any Protective Order.

d. Any CSO or other security entity shall not disclose to any other entity any information provided by a Defense Security Officer, including any component of the Office of Military Commissions, except that the entity may inform the military judge of any information that presents a current threat to loss of life or presents an immediate safety issue in the detention facility. This does not include administrative matters necessary for the management of the security responsibilities of the Office of Military Commissions.

5. ACCESS TO CLASSIFIED INFORMATION

a. Without authorization from the Government, no member of the Defense, including defense witnesses, shall have access to classified information in connection with this case unless that person has:

(1) received the necessary security clearance from the appropriate Department of Defense (DoD) authorities and signed an appropriate non-disclosure agreement, as verified by the Chief Security Manager, Office of Military Commissions;

(2) signed the Memorandum of Understanding Regarding Receipt of Classified Information (MOU), attached to this Protective Order, agreeing to comply with the terms of this Protective Order; and

(3) a need-to-know for the classified information at issue, as determined by the Original Classification Authority (OCA) for that information.

b. In order to be provided access to classified information in connection with this case, each member of the Defense shall execute the attached MOU, file the executed originals of the MOU with the Chief Security Manager, Office of Military Commissions, and submit copies to the CSO and counsel for the Government. The execution and submission of the MOU is a condition precedent to the Defense having access to classified information for the purposes of these proceedings.

c. The substitution, departure, or removal of any member of the Defense, including defense witnesses, from this case for any reason shall not release that person from the provisions of this Protective Order or the MOU executed in connection with this Protective Order.

d. Once the Chief Security Manager, Office of Military Commissions verifies that counsel for the accused have executed and submitted the MOU, and are otherwise authorized to receive classified information in connection with this case, the Government may provide classified discovery to the Defense.

e. All classified documents or information provided or obtained in connection with this case remain classified at the level designated by the OCA, unless the documents bear a clear indication that they have been declassified. The person receiving the classified documents or information, together with all other members of the Defense or the Government, respectively, shall be responsible for protecting the classified information from disclosure and shall ensure

that access to and storage of the classified information is in accordance with applicable laws and regulations and the terms of this Protective Order.

f. No member of the Defense, including any defense witness, is authorized to disclose any classified information obtained during this case, outside the immediate parameters of these military commission proceedings. If any member of the Defense, any accused, or any defense witness receives any summons, subpoena, or court order, or the equivalent thereof, from any United States or foreign court or on behalf of any criminal or civil investigative entity within the United States or from any foreign entity, the Defense, including defense witnesses, shall immediately notify the Commission, the Chief Security Manager, Office of Military Commissions, and the Government so that appropriate consideration can be given to the matter by the Commission and the OCA of the materials concerned. Absent authority from the Commission or the Government, the Defense, an accused, and defense witnesses are not authorized to disseminate or disclose classified materials in response to such requests. The Defense, an accused, and defense witnesses and experts are not authorized to use or refer to any classified information obtained as a result of their participation in commission proceedings in any other forum, or in a military commission proceeding involving another detainee.

6. USE, STORAGE, AND HANDLING PROCEDURES

a. The Office of the Chief Defense Counsel, Office of Military Commissions, has approved secure areas in which the Defense may use, store, handle, and otherwise work with classified information. The Chief Security Manager, Office of Military Commissions, shall ensure that such secure areas are maintained and operated in a manner consistent with this Protective Order and as otherwise reasonably necessary to protect against the disclosure of classified information.

b. All classified information provided to the Defense, and otherwise possessed or maintained by the Defense, shall be stored, maintained, and used only in secure areas. Classified information may only be removed from secure areas in accordance with this Protective Order and applicable laws and regulations governing the handling and use of classified information.

c. Consistent with other provisions of this Protective Order, the Defense shall have access to the classified information made available to them and shall be allowed to take notes and prepare documents with respect to such classified information in secure areas.

d. The Defense shall not copy or reproduce any classified information in any form, except in secure areas and in accordance with this Protective Order and applicable laws and regulations governing the reproduction of classified information.

e. All documents prepared by the Defense that are known or believed to contain classified information—including, without limitation, notes taken or memoranda prepared by counsel and pleadings or other documents intended for filing with the Commission—shall be transcribed, recorded, typed, duplicated, copied, or otherwise prepared only by persons possessing an appropriate approval for access to such classified information. Such activities shall take place in secure areas, on approved word processing equipment, and in accordance with procedures approved by the Chief Security Manager, Office of Military Commissions. All such documents and any associated materials containing classified information—such as notes, memoranda, drafts, copies, typewriter ribbons, magnetic recordings, and exhibits—shall be maintained in secure areas unless and until the Chief Security Officer, Office of Military Commissions, advises that those documents or associated materials are unclassified in their entirety. None of these materials shall be disclosed to the Government unless authorized by the Commission, by counsel for an accused, or as otherwise provided in this Protective Order.

f. The Defense may discuss classified information only within secure areas and shall not discuss, disclose, or disseminate classified information over any non-secure communication system, such as standard commercial telephones, office intercommunication systems, or non-secure electronic mail.

g. The Defense shall not disclose any classified documents or information to any person, including counsel in related cases of Guantanamo Bay detainees in military commissions or other courts (including, but not limited to, habeas proceedings), except those persons authorized by this Protective Order, the Commission, and counsel for the Government with the appropriate clearances and the need-to-know that information. The Commission recognizes that the presentation of a joint defense may necessitate disclosure on a need to know basis to counsel for co-accused.

h. To the extent the Defense is not certain of the classification of information it wishes to disclose, the Defense shall follow procedures established by the Office of Military Commissions for a determination as to its classification. In any instance in which there is any doubt as to whether information is classified, the Defense must consider the information classified unless and until it receives notice from the Chief Security Manager, Office of Military Commissions such information is not classified.

i. Until further order of this Commission, the Defense shall not disclose to an accused any classified information not previously provided by an accused to the Defense, except where such information has been approved for release to an accused and marked accordingly.

j. Except as otherwise stated in this paragraph, and to ensure the national security of the United States, at no time, including any period subsequent to the conclusion of these proceedings, shall the Defense make any public or private statements disclosing any classified

information accessed pursuant to this Protective Order, or otherwise obtained in connection with this case, including the fact that any such information or documents are classified. In the event classified information enters the public domain without first being properly declassified by the United States Government, counsel are reminded they may not make public or private statements about the information if the information is classified. (See paragraph 2 of this Protective Order for specific examples of information which remains classified even if it is in the public domain). In an abundance of caution and to help ensure clarity on this matter, the Commission emphasizes that counsel shall not be the source of any classified information entering the public domain, nor should counsel comment on information which has entered the public domain but which remains classified.

7. PROCEDURES FOR FILING DOCUMENTS

- a. See Rule 3, Motion Practice, Military Commissions Trial Judiciary Rules of Court.
- b. For all filings, other than those filed pursuant to M.C.R E. 505, in which counsel know, reasonably should know, or are uncertain as to whether the filing contains classified information or other information covered by Chapter 19-3(b), DoD Regulation for Trial By Military Commission, counsel shall submit the filing by secure means under seal with the Chief Clerk of the Trial Judiciary.
- c. Documents containing classified information or information the defense counsel believes to be classified shall be filed pursuant to the procedures specified for classified information.
- d. Classified filings must be marked with the appropriate classification markings on each page, including classification markings for each paragraph. If a party is uncertain as to the appropriate classification markings for a document, the party shall seek guidance from the Chief

Security Officer, Office of Military Commissions, who will consult with the OCA of the information or other appropriate agency, as necessary, regarding the appropriate classification.

e All original filings will be maintained by the Director, Office of Court Administration, as part of the Record of Trial. The Office of Court Administration shall ensure any classified information contained in such filings is maintained under seal and stored in an appropriate secure area consistent with the highest level of classified information contained in the filing.

f. Under no circumstances may classified information be filed in an otherwise unclassified filing except as a separate classified attachment. In the event a party believes an unsealed filing contains classified information, the party shall immediately notify the Chief Security Manager, Office of Military Commissions, and CSO/ACSO, who shall take appropriate action to retrieve the documents or information at issue. The filing will then be treated as containing classified information unless and until determined otherwise. Nothing herein limits the Government's authority to take other remedial action as necessary to ensure the protection of the classified information.

g. Nothing herein requires the Government to disclose classified information. Additionally, nothing herein prevents the Government or Defense from submitting classified information to the Commission *in camera* or *ex parte* in these proceedings or accessing such submissions or information filed by the other party. Except as otherwise authorized by the Military Judge, the filing party shall provide the other party with notice on the date of the filing.

8. PROCEDURES FOR MILITARY COMMISSION PROCEEDINGS

a. Except as provided herein, and in accordance with M.C.R.E. 505, no party shall disclose or cause to be disclosed any information known or believed to be classified in connection with any hearing or proceeding in this case.

(1) Notice Requirements: The parties must comply with all notice requirements under M.C.R.E. 505 prior to disclosing or introducing any classified information in this case *including testimony offered by an Accused*.

(2) Closed Proceedings

(a) While proceedings shall generally be publicly held, the Commission may exclude the public from any proceeding, *sua sponte* or upon motion by either party, in order to protect information, the disclosure of which could reasonably be expected to damage national security. If the Commission closes the courtroom during any proceeding in order to protect classified information from disclosure, no person may remain who is not authorized to access classified information in accordance with this Protective Order, which the CSO shall verify prior to the proceeding.

(b) No participant in any proceeding, including the Government, Defense, accused, witnesses, and courtroom personnel, may disclose classified information, or any information that tends to reveal classified information, to any person not authorized to access such classified information in connection with this case.

(3) Delayed Broadcast of Open Proceedings

(a) Due to the nature and classification level of the classified information in this case, the Commission finds that to protect against the unauthorized disclosure of classified information during proceedings open to the public, it will be necessary to employ a forty-second delay in the broadcast of the proceedings from the courtroom to the public gallery. This is the

least disruptive method of both insuring the continued protection of classified information while providing the maximum in public transparency.

(b) Should classified information be disclosed during any open proceeding, this delay will allow the Military Judge, CSO, or Government to take action to suspend the broadcast—including any broadcast of the proceedings to locations other than the public gallery of the courtroom (e.g., any closed-circuit broadcast of the proceedings to a remote location)—so that the classified information will not be disclosed to members of the public.

(c) The broadcast may be suspended whenever it is reasonably believed that any person in the courtroom has made or is about to make a statement or offer testimony disclosing classified information.

(d) The Commission shall be notified immediately if the broadcast is suspended. In that event, and otherwise if necessary, the Commission may stop the proceedings to evaluate whether the information disclosed, or about to be disclosed, is classified information as defined in this Protective Order. The Commission may also conduct an *in camera* hearing to address any such disclosure of classified information.

(4) Other Protections

(a) During the examination of any witness, the Government may object to any question or line of inquiry that may require the witness to disclose classified information not found previously to be admissible by the Commission. Following such an objection, the Commission will determine whether the witness's response is admissible and, if so, may take steps as necessary to protect against the public disclosure of any classified information contained therein.

(b) Classified information offered or admitted into evidence will remain classified at the level designated by the OCA and will be handled accordingly. All classified evidence offered or accepted during trial will be kept under seal, even if such evidence was inadvertently disclosed during a proceeding. Exhibits containing classified information may also be sealed after trial as necessary to prevent disclosure of such classified information.

(5) Record of Trial

(a) It is the responsibility of the Government, IAW 10 U.S.C § 948I(c) to control and prepare the Record of Trial. What is included in the Record of Trial is set out by R.M.C. 1103. The Director, Office of Court Administration, shall ensure that the Record of Trial is reviewed and redacted as necessary to protect any classified information from public disclosure.

(b) The Director, Office of Court Administration, shall ensure portions of the Record of Trial containing classified information remain under seal and are properly segregated from the unclassified portion of the transcripts, properly marked with the appropriate security markings, stored in a secure area, and handled in accordance with this Protective Order.

9. UNAUTHORIZED DISCLOSURE

a. Any unauthorized disclosure of classified information may constitute a violation of United States criminal laws. Additionally, any violation of the terms of this Protective Order shall immediately be brought to the attention of the Commission and may result in disciplinary action or other sanctions, including a charge of contempt of the Commission and possible referral for criminal prosecution. Any breach of this Protective Order may also result in the termination of access to classified information. Persons subject to this Protective Order are advised that unauthorized disclosure, retention, or negligent handling of classified documents or

information could cause damage to the national security of the United States or may be used to the advantage of an adversary of the United States or against the interests of the United States. The purpose of this Protective Order is to ensure those authorized to receive classified information in connection with this case will never divulge that information to anyone not authorized to receive it, without prior written authorization from the OCA and in conformity with this Order.

b. The Defense shall promptly notify the Chief Security Officer, Office of Military Commissions, upon becoming aware of any unauthorized access to or loss, theft, or other disclosure of classified information, and shall take all reasonably necessary steps to retrieve such classified information and protect it from further unauthorized disclosure or dissemination.

10. SURVIVAL OF ORDER

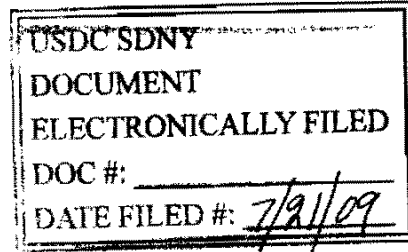
a. The terms of this Protective Order and any signed MOU shall survive and remain in effect after the termination of this case unless otherwise determined by a court of competent jurisdiction.

b. This Protective Order is entered without prejudice to the right of the parties to seek such additional protections or exceptions to those stated herein as they deem necessary.

So ORDERED this 9th day of February, 2013.

//original signed//
JAMES L. POHL
COL, JA, USA
Military Judge

Tab 13



UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
----- x

UNITED STATES OF AMERICA :

- v. - :

AHMED KHALFAN GHAILANI, :

Defendant. :

----- x

(S10) 98 Cr. 1023 (LAK)

**MODIFIED PROTECTIVE ORDER
PERTAINING TO CLASSIFIED INFORMATION**

This matter comes before the Court upon the Government's Motion for a Modified Protective Order pursuant to Section 3 of the Classified Information Procedures Act ("CIPA"), 18 U.S.C. App. 3 § 3, to protect against the disclosure in this case of any classified information disclosed by the Government to, or otherwise in the possession of, the Defendant or the Defense.

Pursuant to the authority granted under Sections 3 and 9 of CIPA, the Security Procedures Established Pursuant to Pub. L. No. 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information (reprinted following CIPA § 9), Rules 16(d) and 57 of the Federal Rules of Criminal Procedure, and the general supervisory authority of the Court, and to protect the national security, the following Modified Protective Order is entered.

General Provisions

1. The Court finds that this case will involve information that has been currently in the interest of national security of

the United States pursuant to Executive Order 12958, as amended.¹ The storage, handling and control of this information will require special security precautions mandated by statute, executive order, and regulation, and access to which requires the appropriate security clearances, and a "need to know" determination pursuant to Executive Order 12958.

2. The purpose of this Order is to establish procedures that must be followed by the Defense and the Government, and any other person who comes into possession of classified information as a result of their participation in this case. These procedures will apply to all pretrial, trial, post-trial, and appellate matters concerning classified information, and may be modified from time to time by further order of the Court acting under its inherent supervisory authority to ensure a fair and expeditious trial.

Definitions

3. The following definitions shall apply to this Order:
- a. The term "Defense" shall mean any counsel for the defendant, employees or contractors of counsel for the Defendant (including, without limitation, investigators, paralegals,

¹Executive Order 12958 was amended by Executive Order 13292. See E.O. No. 13292, 68 Fed. Reg. 15315 (Mar., 28, 2003). All citations to E.O. 12958 are to that Executive Order as amended by E.O. 13292. See E.O. 12958, 3 C.F.R. 333 (1995), reprinted as amended in 50 U.S.C.A. § 435, note at 180 (Supp. 2007).

experts and translators), and any witnesses for the Defendant so authorized by the Court.

b. The term "classified information" shall include:

(i) Any document or information contained therein, which has been classified by any executive agency in the interests of national security pursuant to Executive Order 12958, as amended, or its predecessor orders, as "CONFIDENTIAL," "SECRET," "TOP SECRET," or additionally controlled as "SENSITIVE COMPARTMENTED INFORMATION" ("SCI");

(ii) Any document or information that is currently properly classified, as set forth in (i), and that has been approved by the Government or the Court for release to the Defendant. All classified information that is approved for release to the Defendant will contain an appropriate classification marking and will be marked "Releasable to Ghailani";

(iii) Any document or information now or formerly in the possession of a private party which (A) has been derived from information from the United States Government that was classified, and (B) has subsequently been classified by the United States pursuant to executive order as "CONFIDENTIAL," "SECRET," "TOP SECRET," or additionally controlled as SCI;

(iv) Any document or information that the Defense knows or reasonably should know contains classified information,

including information acquired or conveyed orally;

(v) Any information, regardless of place of origin, to include "foreign government information" as that term is defined in Executive Order 12958, that could reasonably be believed to contain classified information, or that refers or relates to national security or intelligence matters; and

(vi) Any document or information as to which the Defense has been notified orally or in writing contains classified information, including but not limited to the following four areas of classified information, which may be at issue in this case, and for which the Defense has received notice of its classified nature:

(a) Information that would reveal or tend to reveal the foreign countries in which the Defendant was held from on or about July 25, 2004 through September 6, 2006;

(b) The names, identities, and physical descriptions of any officers responsible for the capture, transfer, detention, or interrogation of the Defendant from on or about July 25, 2004 through June 9, 2009;

(c) The Enhanced Interrogation Techniques that were applied to the Defendant from on or about July 25, 2004 through September 6, 2006, including descriptions of the techniques as applied, the duration, frequency, sequencing, and limitations of those techniques; and

(d) Descriptions of the Defendant's conditions of confinement from on or about July 25, 2004 through June 9, 2009.

c. The terms "document" and "information" shall include, but are not limited to, all written, printed, visual or audible matter of any kind, formal or informal, including originals, conforming copies, and non-conforming copies (whether different from the original by reason of notation made on such copies or otherwise). The terms "document" and "information" shall also include without limitation, notes (handwritten, oral, or electronic); letters; correspondence; memoranda; reports; summaries; photographs; maps; charts; graphs; inter-office communications; notations of any sort concerning conversations, meetings or other communications; bulletins; teletypes; telecopies; telegrams; telexes; cables; facsimiles; invoices; worksheets and drafts; microfiche; microfilm; videotapes; sound recordings of any kind; motion pictures; electronic, mechanical or electric records of any kind, including but not limited to tapes, cassettes, disks, recordings, films, typewriter ribbons, word processing or other computer tapes, disks, or thumb drives and all manner of electronic data processing storage; and alterations, modifications, changes and amendments of any kind to the foregoing. In addition, the term "information" shall include without limitation observations and experiences of the Defendant

with respect to matters set forth in subparagraphs (3)(b)(vi)(a)-(d), above.

d. The term "access to classified information" shall mean having access to, reviewing, reading, learning, or otherwise coming to know in any manner classified information.

e. The term "Secure Area" shall mean a sensitive compartmented information facility ("SCIF") accredited by a Court Security Officer for the storage, handling, and control of classified information.

Classified Information, General Provisions

4. All classified documents, and information contained therein, shall remain classified unless the documents bear a clear indication that they have been "declassified" by the agency or department that originated the document or information contained therein ("originating agency").

5. Any classified information provided to the Defense by the Government is to be used solely by the Defense and solely for the purpose of preparing the defense. The Defense may not disclose or cause to be disclosed in connection with this case any information known or reasonably believed to be classified information except as otherwise provided herein.

a. The Defense may not disclose classified information to the Defendant unless that same information has been previously provided to the Defense by the Defendant. The

Defense may not confirm or deny to the Defendant the assertions made by the Defendant based on knowledge the Defense may have obtained from classified information, except where that classified information has been provided to the Defendant.

b. The Defense shall not disclose classified information to any person, except to the Court, Government personnel who hold appropriate security clearances and have been determined to have a need to know that information, and those authorized pursuant to this Order.

c. Information that is classified that also appears in the public domain is not thereby automatically declassified unless it appears in the public domain as the result of an official statement by a U.S. Government Executive Branch official who is authorized to declassify the information. Individuals who by virtue of this Order or any other court order are granted access to classified information may not confirm or deny classified information that appears in the public domain. Prior to any attempt by the Defense to have such information confirmed or denied at trial or in any public proceeding in this case, the Defense must comply with the notification requirements of Section 5 of CIPA and all provisions of this Order.

d. In the event that classified information enters the public domain, the Defense is precluded from making private or public statements where the statements would reveal personal

knowledge from non-public sources regarding the classified status of the information, or would disclose that the Defense had personal access to classified information confirming, contradicting, or otherwise relating to the information already in the public domain. The Defense is not precluded from citing or repeating information in the public domain that counsel does not know or have reason to believe to be classified information, or derived from classified information.

Security Procedures

6. In accordance with the provisions of CIPA and the security procedures promulgated by the Chief Justice of the United States pursuant to that Act, this Court designates Michael P. Macisso as Court Security Officer ("CSO") and Joan B. Kennedy, Christine E. Gunning, James P. Londergan, Barbara J. Russell, Nathaniel Johnson, Miguel Ferrer, Jennifer H. Campbell, Daniel O. Hartenstine, Charline Dasilva, and Erin Hogarty as alternate CSOs for this case, for the purpose of providing security arrangements necessary to protect against unauthorized disclosure any classified information that has been made available to the Defense in connection with this case. The Defense shall seek guidance from the CSO with regard to appropriate storage, handling, transmittal, and use of classified information.

7. The Court has been advised, through the CSO, that the Assistant United States Attorneys David Raskin, Leslie C. Brown,

and Nicholas J. Lewin (collectively, "Counsel for the Government"), as well as certain other Department of Justice employees, have the requisite security clearances allowing them to have access to the classified information that relates to this case.

8. No Defendant or representative of the Defense shall have access to classified information at issue in this case unless the person shall first have:

a. Received from the CSO the appropriate security clearance for the level of the classified information involved in this case;

b. A "need to know" the classified information at issue in this proceeding; and

c. Signed the Memorandum of Understanding in the form attached hereto agreeing to comply with the terms of this Order. The signed Memorandum of Understanding shall be filed with the Court. The substitution, departure, or removal for any reason from this case, of counsel for the Defendant or any other member of the Defense, shall not release that individual from the provisions of this Order or the Memorandum of Understanding executed in connection with this Order.²

² The sole exception to the requirements set forth in this paragraph is that, pending receipt of the necessary security clearances, defense counsel Gregory E. Cooper, Esq., Peter Enrique Quijano, Esq., and Michael K. Bachrach, Esq., shall be permitted access to classified information known to the Defendant

9. Pursuant to Section 4 of the security procedures promulgated pursuant to CIPA, no court personnel (except for the Judge) required by this Court for its assistance shall have access to classified information involved in this case unless that person shall first has received the necessary security clearance as determined by the CSO.

10. Standard Form 86, "Questionnaire for National Security Positions," attached releases, and full fingerprints shall be completed and submitted to the CSO forthwith by all defense counsel not otherwise already cleared, all persons whose assistance the defense reasonably requires, and by such courtroom personnel as the Court requires for its assistance. The CSO shall undertake all reasonable steps to process all security clearance applications in accordance with applicable regulations.

11. Prior security clearance and a "need to know" as determined by any government entity as applying to one person does not automatically give that person the authority to disclose any classified information to any other individual, even if that individual also has a security clearance. By way of example, but not limitation, defense counsel with appropriate clearances and a

by virtue of his observations and experiences, as described in subparagraphs (3) (b) (vi) (a) - (d). The Government agrees to this exception based on counsel's commitment to abide by the Special Administrative Measures; the Government's expectation that counsel will soon receive security clearances; and to promote effective representation of the Defendant.

need to know, as determined by the government, are not authorized to discuss or otherwise disclose such classified information with an uncleared defendant absent approval of the Court or written permission of the Government.

12. *Secure Area for the Defense.* The CSO shall arrange for an approved Secure Area for use by the Defense. The CSO shall establish procedures to assure that the Secure Area is accessible during business hours to the Defense, and at other times upon reasonable request as approved by the CSO. The Secure Area shall contain a separate working area for the Defense and will be outfitted with any secure office equipment requested by the Defense that is reasonable and necessary to the preparation of the defense. The CSO, in consultation with counsel for the Defendant, shall establish procedures to assure that the Secure Area may be maintained and operated in the most efficient manner consistent with the protection of classified information. No classified documents may be removed from the Secure Area unless so authorized by the CSO with notice provided to the Court. The CSO shall not reveal to the Government the content of any conversations he may hear among the Defense, nor reveal the nature of the documents being reviewed, or the work being generated. The presence of the CSO shall not operate to render inapplicable the attorney-client privilege.

13. *Filing of Papers by the Defense.* Any pleading or other

document filed by the Defense that counsel for the Defendant knows or reasonably should know contains classified information as defined in paragraph 3(b), shall be filed under seal with the Court Security Officer or a designee and shall be marked, "Filed in Camera and Under Seal with the Court Security Officer." The time of physical submission to the CSO (or alternate CSO designated by the CSO) shall be considered the date and time of filing. The CSO shall promptly examine the pleading or document and, in consultation with representatives of the appropriate departments or agencies, determine whether the pleading or document contains classified information. If it is determined that the pleading or document contains classified information, the CSO shall ensure that the relevant portion of the document, and only that portion, is marked with the appropriate classification marking and remains under seal. All portions of all paper filed by the Defense that do not contain classified information shall be immediately unsealed by the CSO and placed in the public record. The CSO shall immediately deliver under seal to the Court and Counsel for the Government any pleading or document to be filed by the Defense that contains classified information, unless the pleading or document is an ex parte filing. The Court shall then direct the clerk to enter on the docket sheet the title of the pleading or document, if the title itself would not tend to reveal classified information, the date

it was filed, and the fact that it has been filed under seal with the CSO.

14. *Filing of Papers by the Government.* Only the portions of pleadings or documents filed by the Government that contain classified information shall be filed under seal with the Court through the CSO. Such pleadings and documents shall be marked, "Filed In Camera and Under Seal with the Court Security Officer." The time of physical submission to the CSO (or designee) shall be considered the date and time of filing. The CSO shall immediately deliver under seal to the Court and counsel for the Defendant any pleading or document to be filed by the Government that contains classified information, unless the pleading or document is an ex parte filing. The Court shall then direct the clerk to enter on the docket sheet the title of the pleading or document, if the title itself would not tend to reveal classified information, the date it was filed, and the fact that it has been filed under seal with the CSO.

15. *Record and Maintenance of Classified Filings.* The CSO shall maintain a separate sealed record for those materials which are classified. The CSO shall be responsible for the maintaining of the secured records for purposes of later proceedings or appeal.

16. *The Classified Information Procedures Act.* Procedures for public disclosure of classified information in this case

shall be those established by CIPA. The Defense shall comply with the requirements of CIPA Section 5 prior to any disclosure of classified information during any proceeding in this case. As set forth in Section 5, the Defense shall not disclose any information known or believed to be classified in connection with any proceeding until notice has been given to Counsel for the Government and until the Government has been afforded a reasonable opportunity to seek a determination pursuant to the procedures set forth in CIPA Section 6, and until the time for the Government to appeal such determination under CIPA Section 7 has expired or any appeal under Section 7 by the Government is decided. Pretrial conferences involving classified information shall be conducted in camera in the interest of national security, be attended only by persons with access to classified information and a need to know, and the transcripts of such proceedings shall be maintained under seal.

17. *Access to Classified Information.* In the interest of the national security, representatives of the Defense granted access to classified information shall have access to classified information only as follows:

a. All classified information produced by the Government to counsel for the Defendant in discovery or otherwise, and all classified information possessed, created or maintained by the Defense, including notes and any other work

product, shall be stored, maintained and used only in the Secure Area established by the CSO.

b. The Defense shall have free access to the classified information made available to them in the Secure Area established by the CSO and shall be allowed to take notes and prepare documents with respect to those materials.

c. No representative of the Defense (including, but not limited to, counsel, investigators, paralegals, translators, experts and witnesses) shall copy or reproduce any classified information in any manner or form, except with the approval of the CSO or in accordance with the procedures established by the CSO for the operation of the Secure Area.

d. All documents prepared by the Defense (including, without limitation, pleadings or other documents intended for filing with the Court) that do or may contain classified information must be prepared in the Secure Area on word processing equipment approved by the CSO. All such documents and any associated materials (such as notes, drafts, copies, typewriter ribbons, magnetic recordings, exhibits) containing classified information shall be maintained in the Secure Area unless and until the CSO determines that those documents or associated materials are unclassified in their entirety. None of these materials shall be disclosed to counsel for the Government or any other party.

e. The Defense shall discuss classified information only within the Secure Area or in an area authorized by the CSO.

f. The Defense shall not disclose, without prior approval of the Court, classified information to any person not named in this Order except the Court, Court personnel, and Government personnel identified by the CSO as having the appropriate clearances and the need to know. Counsel for the Government shall be given an opportunity to be heard in response to any Defense request for disclosure to a person not identified in this Order. Any person approved by the Court for access to classified information under this paragraph shall be required to obtain the appropriate security clearance, to sign and submit to the Court the Memorandum of Understanding appended to the Order, and to comply with all the terms and conditions of the Order. If preparation of the defense requires that classified information be disclosed to persons not identified in this Order, the Department of Justice shall promptly seek to obtain security clearances for them at the request of counsel for the Defendant.

g. The Defense shall not discuss classified information over any standard commercial telephone instrument or office intercommunication systems, including but not limited to the Internet, or in the presence of any person who has not been granted access to classified information by the Court.

h. Any documents written by the Defense that do or

may contain classified information shall be transcribed, recorded, typed, duplicated, copied, or otherwise prepared only by persons who have received an appropriate approval for access to classified information.

i. The Defense shall not disclose classified information to the Defendant -- other than materials marked "Releasable to Ghailani" -- absent leave of this Court or written permission of the Government. Counsel for the Government shall be given an opportunity to be heard in response to any Defense request for disclosure to the Defendant of such classified information.

18. Any unauthorized disclosure of classified information may constitute violations of United States criminal laws. In addition, any violation of the terms of this Order shall be brought immediately to the attention of the Court and may result in a charge of contempt of Court and possible referral for criminal prosecution. Any breach of this Order may also result in termination of an individual's access to classified information. Persons subject to this Order are advised that direct or indirect unauthorized disclosure, retention or negligent handling of classified documents or information could cause serious damage, and in some cases exceptionally grave damage to the national security of the United States or may be used to the advantage of a foreign nation against the interests

of the United States. The purpose of this Order is to ensure that those authorized to receive classified information in connection with this case will never divulge that information to anyone not authorized to receive it, without prior written authorization from the originating agency and in conformance with this Order.

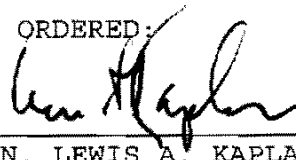
19. All classified documents and information to which the Defense has access in this case are now and will remain the property of the United States. Upon demand of the CSO, these persons shall return to the CSO all classified information in their possession obtained through discovery from the Government in this case, or for which they are responsible because of access to classified information. The notes, summaries and other documents prepared by the Defense that do or may contain classified information shall remain at all times in the custody of the CSO for the duration of the case. At the conclusion of this case, all such notes, summaries, and other documents are to be destroyed by the CSO in the presence of counsel for the Defendant.

20. Nothing contained in this Order shall be construed as a waiver of any right of the Defendant. No admission made by the Defendant or his counsel during pretrial conferences may be used against the Defendant unless it is in writing and signed by the Defendant. See CIPA § 2.

21. A copy of this Order shall be issued forthwith to counsel for the Defendant who shall be responsible for advising the Defendant and representatives of the Defense of this Order. Counsel for the Defendant, and any other representatives of the Defense who will be provided access to the classified information, shall execute the Memorandum of Understanding described in paragraph 8 of this Order, and counsel for the Defendant shall file executed originals of such documents with the Court and the CSO and serve an executed original upon the Government. The execution and filing of the Memorandum of Understanding is a condition precedent for counsel for the Defendant and any other representative of the Defense to have access to classified information.

Dated: New York, New York
July 21, 2009

SO ORDERED:



HON. LEWIS A. KAPLAN
United States District Judge
Southern District of New York

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- - - - - x

UNITED STATES OF AMERICA :

- v. - :

(S10) 98 Cr. 1023 (LAK)

AHMED KHALFAN GHAILANI, :

Defendant. :

- - - - - x

**MEMORANDUM OF UNDERSTANDING REGARDING RECEIPT OF
CLASSIFIED INFORMATION**

Having familiarized myself with the applicable statutes, regulations, and orders, related to, but not limited to, Title 18 United States Code, including unauthorized disclosure of classified information, espionage and related offenses; The Intelligence Agents Identities Protection Act, Title 50 U.S.C. Section 421;; Title 18 U.S.C. Section 641; Title 50 U.S.C. Section 783; 28 C.F.R. 17 et seq., and Executive Order 12356; I understand that I may be the recipient of information and documents that concern the present and future security of the United States and belong to the United States, and that such documents and information together with the methods and sources of collecting it are classified by the United States Government. In consideration for the disclosure of classified information and documents:

- (1) I agree that I shall never divulge, publish, or reveal either by word, conduct or any other means, such classified documents and information unless specifically

authorized in writing to do so by an authorized representative of the United States Government; or as expressly authorized by the Court pursuant to the Classified Information Procedures Act and the Protective Order entered in the case of United States v. Ahmed Khalfan Ghailani, (S10) 98 Cr. 1023 (LAK), Southern District of New York.

(2) I agree that this Memorandum and any other non-disclosure agreement signed by me will remain forever binding on me.

(3) I have received, read, and understand the Protective Order entered by the United States District Court for the Southern District of New York on _____, 2009, in the case of United States v. Ahmed Khalfan Ghailani, (S10) 98 Cr. 1023 (LAK), relating to classified information, and I agree to comply with the provisions thereof.

Court Security Officer

Date

Gregory E. Cooper, Esq.
Counsel for Ahmed Khalfan Ghailani

Date

Peter Enrique Quijano, Esq.
Counsel for Ahmed Khalfan Ghailani

Date

Tab 14



Federal Register

Tuesday,
January 5, 2010

Part VII

The President

**Executive Order 13526—Classified
National Security Information
Memorandum of December 29, 2009—
Implementation of the Executive Order
“Classified National Security Information”
Order of December 29, 2009—Original
Classification Authority**

Presidential Documents

Title 3—

Executive Order 13526 of December 29, 2009

The President

Classified National Security Information

This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information both within the Government and to the American people. Nevertheless, throughout our history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information critical to our Nation's security and demonstrating our commitment to open Government through accurate and accountable application of classification standards and routine, secure, and effective declassification are equally important priorities.

NOW, THEREFORE, I, BARACK OBAMA, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

PART 1—ORIGINAL CLASSIFICATION

Section 1.1. *Classification Standards.* (a) Information may be originally classified under the terms of this order only if all of the following conditions are met:

- (1) an original classification authority is classifying the information;
- (2) the information is owned by, produced by or for, or is under the control of the United States Government;
- (3) the information falls within one or more of the categories of information listed in section 1.4 of this order; and
- (4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.

(b) If there is significant doubt about the need to classify information, it shall not be classified. This provision does not:

- (1) amplify or modify the substantive criteria or procedures for classification; or
- (2) create any substantive or procedural rights subject to judicial review.

(c) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

(d) The unauthorized disclosure of foreign government information is presumed to cause damage to the national security.

Sec. 1.2. *Classification Levels.* (a) Information may be classified at one of the following three levels:

- (1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
- (2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the

national security that the original classification authority is able to identify or describe.

(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.

(c) If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

Sec. 1.3. Classification Authority. (a) The authority to classify information originally may be exercised only by:

(1) the President and the Vice President;

(2) agency heads and officials designated by the President; and

(3) United States Government officials delegated this authority pursuant to paragraph (c) of this section.

(b) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.

(c) Delegation of original classification authority.

(1) Delegations of original classification authority shall be limited to the minimum required to administer this order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) "Top Secret" original classification authority may be delegated only by the President, the Vice President, or an agency head or official designated pursuant to paragraph (a)(2) of this section.

(3) "Secret" or "Confidential" original classification authority may be delegated only by the President, the Vice President, an agency head or official designated pursuant to paragraph (a)(2) of this section, or the senior agency official designated under section 5.4(d) of this order, provided that official has been delegated "Top Secret" original classification authority by the agency head.

(4) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this order. Each delegation shall identify the official by name or position.

(5) Delegations of original classification authority shall be reported or made available by name or position to the Director of the Information Security Oversight Office.

(d) All original classification authorities must receive training in proper classification (including the avoidance of over-classification) and declassification as provided in this order and its implementing directives at least once a calendar year. Such training must include instruction on the proper safeguarding of classified information and on the sanctions in section 5.5 of this order that may be brought against an individual who fails to classify information properly or protect classified information from unauthorized disclosure. Original classification authorities who do not receive such mandatory training at least once within a calendar year shall have their classification authority suspended by the agency head or the senior agency official designated under section 5.4(d) of this order until such training has taken place. A waiver may be granted by the agency head, the deputy agency head, or the senior agency official if an individual is unable to receive such training due to unavoidable circumstances. Whenever a waiver is granted, the individual shall receive such training as soon as practicable.

(e) Exceptional cases. When an employee, government contractor, licensee, certificate holder, or grantee of an agency who does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent

with this order and its implementing directives. The information shall be transmitted promptly as provided under this order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within 30 days whether to classify this information.

Sec. 1.4. Classification Categories. Information shall not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security in accordance with section 1.2 of this order, and it pertains to one or more of the following:

- (a) military plans, weapons systems, or operations;
- (b) foreign government information;
- (c) intelligence activities (including covert action), intelligence sources or methods, or cryptology;
- (d) foreign relations or foreign activities of the United States, including confidential sources;
- (e) scientific, technological, or economic matters relating to the national security;
- (f) United States Government programs for safeguarding nuclear materials or facilities;
- (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or
- (h) the development, production, or use of weapons of mass destruction.

Sec. 1.5. Duration of Classification. (a) At the time of original classification, the original classification authority shall establish a specific date or event for declassification based on the duration of the national security sensitivity of the information. Upon reaching the date or event, the information shall be automatically declassified. Except for information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, the date or event shall not exceed the time frame established in paragraph (b) of this section.

(b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, unless the original classification authority otherwise determines that the sensitivity of the information requires that it be marked for declassification for up to 25 years from the date of the original decision.

(c) An original classification authority may extend the duration of classification up to 25 years from the date of origin of the document, change the level of classification, or reclassify specific information only when the standards and procedures for classifying information under this order are followed.

(d) No information may remain classified indefinitely. Information marked for an indefinite duration of classification under predecessor orders, for example, marked as "Originating Agency's Determination Required," or classified information that contains incomplete declassification instructions or lacks declassification instructions shall be declassified in accordance with part 3 of this order.

Sec. 1.6. Identification and Markings. (a) At the time of original classification, the following shall be indicated in a manner that is immediately apparent:

- (1) one of the three classification levels defined in section 1.2 of this order;
- (2) the identity, by name and position, or by personal identifier, of the original classification authority;
- (3) the agency and office of origin, if not otherwise evident;
- (4) declassification instructions, which shall indicate one of the following:

(A) the date or event for declassification, as prescribed in section 1.5(a);
(B) the date that is 10 years from the date of original classification, as prescribed in section 1.5(b);

(C) the date that is up to 25 years from the date of original classification, as prescribed in section 1.5(b); or

(D) in the case of information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, the marking prescribed in implementing directives issued pursuant to this order; and

(5) a concise reason for classification that, at a minimum, cites the applicable classification categories in section 1.4 of this order.

(b) Specific information required in paragraph (a) of this section may be excluded if it would reveal additional classified information.

(c) With respect to each classified document, the agency originating the document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are unclassified. In accordance with standards prescribed in directives issued under this order, the Director of the Information Security Oversight Office may grant and revoke temporary waivers of this requirement. The Director shall revoke any waiver upon a finding of abuse.

(d) Markings or other indicia implementing the provisions of this order, including abbreviations and requirements to safeguard classified working papers, shall conform to the standards prescribed in implementing directives issued pursuant to this order.

(e) Foreign government information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information. Foreign government information retaining its original classification markings need not be assigned a U.S. classification marking provided that the responsible agency determines that the foreign government markings are adequate to meet the purposes served by U.S. classification markings.

(f) Information assigned a level of classification under this or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Whenever such information is used in the derivative classification process or is reviewed for possible declassification, holders of such information shall coordinate with an appropriate classification authority for the application of omitted markings.

(g) The classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document or prepare a product to allow for dissemination at the lowest level of classification possible or in unclassified form.

(h) Prior to public release, all declassified records shall be appropriately marked to reflect their declassification.

Sec. 1.7. Classification Prohibitions and Limitations. (a) In no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to:

(1) conceal violations of law, inefficiency, or administrative error;

(2) prevent embarrassment to a person, organization, or agency;

(3) restrain competition; or

(4) prevent or delay the release of information that does not require protection in the interest of the national security.

(b) Basic scientific research information not clearly related to the national security shall not be classified.

(c) Information may not be reclassified after declassification and release to the public under proper authority unless:

(1) the reclassification is personally approved in writing by the agency head based on a document-by-document determination by the agency that reclassification is required to prevent significant and demonstrable damage to the national security;

(2) the information may be reasonably recovered without bringing undue attention to the information;

(3) the reclassification action is reported promptly to the Assistant to the President for National Security Affairs (National Security Advisor) and the Director of the Information Security Oversight Office; and

(4) for documents in the physical and legal custody of the National Archives and Records Administration (National Archives) that have been available for public use, the agency head has, after making the determinations required by this paragraph, notified the Archivist of the United States (Archivist), who shall suspend public access pending approval of the reclassification action by the Director of the Information Security Oversight Office. Any such decision by the Director may be appealed by the agency head to the President through the National Security Advisor. Public access shall remain suspended pending a prompt decision on the appeal.

(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552), the Presidential Records Act, 44 U.S.C. 2204(c)(1), the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section 3.5 of this order only if such classification meets the requirements of this order and is accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official designated under section 5.4 of this order. The requirements in this paragraph also apply to those situations in which information has been declassified in accordance with a specific date or event determined by an original classification authority in accordance with section 1.5 of this order.

(e) Compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that:

(1) meets the standards for classification under this order; and

(2) is not otherwise revealed in the individual items of information.

Sec. 1.8. Classification Challenges. (a) Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established under paragraph (b) of this section.

(b) In accordance with implementing directives issued pursuant to this order, an agency head or senior agency official shall establish procedures under which authorized holders of information, including authorized holders outside the classifying agency, are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall ensure that:

(1) individuals are not subject to retribution for bringing such actions;

(2) an opportunity is provided for review by an impartial official or panel; and

(3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel (Panel) established by section 5.3 of this order.

(c) Documents required to be submitted for prepublication review or other administrative process pursuant to an approved nondisclosure agreement are not covered by this section.

Sec. 1.9. *Fundamental Classification Guidance Review.* (a) Agency heads shall complete on a periodic basis a comprehensive review of the agency's classification guidance, particularly classification guides, to ensure the guidance reflects current circumstances and to identify classified information that no longer requires protection and can be declassified. The initial fundamental classification guidance review shall be completed within 2 years of the effective date of this order.

(b) The classification guidance review shall include an evaluation of classified information to determine if it meets the standards for classification under section 1.4 of this order, taking into account an up-to-date assessment of likely damage as described under section 1.2 of this order.

(c) The classification guidance review shall include original classification authorities and agency subject matter experts to ensure a broad range of perspectives.

(d) Agency heads shall provide a report summarizing the results of the classification guidance review to the Director of the Information Security Oversight Office and shall release an unclassified version of this report to the public.

PART 2—DERIVATIVE CLASSIFICATION

Sec. 2.1. *Use of Derivative Classification.* (a) Persons who reproduce, extract, or summarize classified information, or who apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

(1) be identified by name and position, or by personal identifier, in a manner that is immediately apparent for each derivative classification action;

(2) observe and respect original classification decisions; and

(3) carry forward to any newly created documents the pertinent classification markings. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward:

(A) the date or event for declassification that corresponds to the longest period of classification among the sources, or the marking established pursuant to section 1.6(a)(4)(D) of this order; and

(B) a listing of the source materials.

(c) Derivative classifiers shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document or prepare a product to allow for dissemination at the lowest level of classification possible or in unclassified form.

(d) Persons who apply derivative classification markings shall receive training in the proper application of the derivative classification principles of the order, with an emphasis on avoiding over-classification, at least once every 2 years. Derivative classifiers who do not receive such training at least once every 2 years shall have their authority to apply derivative classification markings suspended until they have received such training. A waiver may be granted by the agency head, the deputy agency head, or the senior agency official if an individual is unable to receive such training due to unavoidable circumstances. Whenever a waiver is granted, the individual shall receive such training as soon as practicable.

Sec. 2.2. *Classification Guides.* (a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides shall conform to standards contained in directives issued under this order.

(b) Each guide shall be approved personally and in writing by an official who:

(1) has program or supervisory responsibility over the information or is the senior agency official; and

(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Agencies shall establish procedures to ensure that classification guides are reviewed and updated as provided in directives issued under this order.

(d) Agencies shall incorporate original classification decisions into classification guides on a timely basis and in accordance with directives issued under this order.

(e) Agencies may incorporate exemptions from automatic declassification approved pursuant to section 3.3(j) of this order into classification guides, provided that the Panel is notified of the intent to take such action for specific information in advance of approval and the information remains in active use.

(f) The duration of classification of a document classified by a derivative classifier using a classification guide shall not exceed 25 years from the date of the origin of the document, except for:

(1) information that should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction; and

(2) specific information incorporated into classification guides in accordance with section 2.2(e) of this order.

PART 3—DECLASSIFICATION AND DOWNGRADING

Sec. 3.1. Authority for Declassification. (a) Information shall be declassified as soon as it no longer meets the standards for classification under this order.

(b) Information shall be declassified or downgraded by:

(1) the official who authorized the original classification, if that official is still serving in the same position and has original classification authority;

(2) the originator's current successor in function, if that individual has original classification authority;

(3) a supervisory official of either the originator or his or her successor in function, if the supervisory official has original classification authority; or (4) officials delegated declassification authority in writing by the agency head or the senior agency official of the originating agency.

(c) The Director of National Intelligence (or, if delegated by the Director of National Intelligence, the Principal Deputy Director of National Intelligence) may, with respect to the Intelligence Community, after consultation with the head of the originating Intelligence Community element or department, declassify, downgrade, or direct the declassification or downgrading of information or intelligence relating to intelligence sources, methods, or activities.

(d) It is presumed that information that continues to meet the classification requirements under this order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or the senior agency official. That official will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to the national security that might reasonably be expected from disclosure. This provision does not:

(1) amplify or modify the substantive criteria or procedures for classification; or

(2) create any substantive or procedural rights subject to judicial review.

(e) If the Director of the Information Security Oversight Office determines that information is classified in violation of this order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the President through the National Security Advisor. The information shall remain classified pending a prompt decision on the appeal.

(f) The provisions of this section shall also apply to agencies that, under the terms of this order, do not have original classification authority, but had such authority under predecessor orders.

(g) No information may be excluded from declassification under section 3.3 of this order based solely on the type of document or record in which it is found. Rather, the classified information must be considered on the basis of its content.

(h) Classified nonrecord materials, including artifacts, shall be declassified as soon as they no longer meet the standards for classification under this order.

(i) When making decisions under sections 3.3, 3.4, and 3.5 of this order, agencies shall consider the final decisions of the Panel.

Sec. 3.2. *Transferred Records.*

(a) In the case of classified records transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this order.

(b) In the case of classified records that are not officially transferred as described in paragraph (a) of this section, but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such records shall be deemed to be the originating agency for purposes of this order. Such records may be declassified or downgraded by the agency in possession of the records after consultation with any other agency that has an interest in the subject matter of the records.

(c) Classified records accessioned into the National Archives shall be declassified or downgraded by the Archivist in accordance with this order, the directives issued pursuant to this order, agency declassification guides, and any existing procedural agreement between the Archivist and the relevant agency head.

(d) The originating agency shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National Archives. However, the Archivist may require that classified records be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to records transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or records for which the National Archives serves as the custodian of the records of an agency or organization that has gone out of existence.

(e) To the extent practicable, agencies shall adopt a system of records management that will facilitate the public release of documents at the time such documents are declassified pursuant to the provisions for automatic declassification in section 3.3 of this order.

Sec. 3.3 *Automatic Declassification.*

(a) Subject to paragraphs (b)–(d) and (g)–(j) of this section, all classified records that (1) are more than 25 years old and (2) have been determined to have permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. All classified records shall be automatically declassified on December 31 of the year that is 25 years from the date of origin, except as provided in paragraphs (b)–(d) and (g)–(j) of this section. If the date of origin of an individual record cannot be readily determined, the date of original classification shall be used instead.

(b) An agency head may exempt from automatic declassification under paragraph (a) of this section specific information, the release of which should clearly and demonstrably be expected to:

- (1) reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign

government or international organization, or a nonhuman intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development;

(2) reveal information that would assist in the development, production, or use of weapons of mass destruction;

(3) reveal information that would impair U.S. cryptologic systems or activities;

(4) reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system;

(5) reveal formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans;

(6) reveal information, including foreign government information, that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States;

(7) reveal information that would impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized;

(8) reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security; or

(9) violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.

(c)(1) An agency head shall notify the Panel of any specific file series of records for which a review or assessment has determined that the information within that file series almost invariably falls within one or more of the exemption categories listed in paragraph (b) of this section and that the agency proposes to exempt from automatic declassification at 25 years.

(2) The notification shall include:

(A) a description of the file series;

(B) an explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time; and

(C) except when the information within the file series almost invariably identifies a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction, a specific date or event for declassification of the information, not to exceed December 31 of the year that is 50 years from the date of origin of the records.

(3) The Panel may direct the agency not to exempt a designated file series or to declassify the information within that series at an earlier date than recommended. The agency head may appeal such a decision to the President through the National Security Advisor.

(4) File series exemptions approved by the President prior to December 31, 2008, shall remain valid without any additional agency action pending Panel review by the later of December 31, 2010, or December 31 of the year that is 10 years from the date of previous approval.

(d) The following provisions shall apply to the onset of automatic declassification:

(1) Classified records within an integral file block, as defined in this order, that are otherwise subject to automatic declassification under this section shall not be automatically declassified until December 31 of the year that is 25 years from the date of the most recent record within the file block.

(2) After consultation with the Director of the National Declassification Center (the Center) established by section 3.7 of this order and before the records are subject to automatic declassification, an agency head or senior agency official may delay automatic declassification for up to five additional years for classified information contained in media that make a review for possible declassification exemptions more difficult or costly.

(3) Other than for records that are properly exempted from automatic declassification, records containing classified information that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies with respect to the classified information and could reasonably be expected to fall under one or more of the exemptions in paragraph (b) of this section shall be identified prior to the onset of automatic declassification for later referral to those agencies.

(A) The information of concern shall be referred by the Center established by section 3.7 of this order, or by the centralized facilities referred to in section 3.7(e) of this order, in a prioritized and scheduled manner determined by the Center.

(B) If an agency fails to provide a final determination on a referral made by the Center within 1 year of referral, or by the centralized facilities referred to in section 3.7(e) of this order within 3 years of referral, its equities in the referred records shall be automatically declassified.

(C) If any disagreement arises between affected agencies and the Center regarding the referral review period, the Director of the Information Security Oversight Office shall determine the appropriate period of review of referred records.

(D) Referrals identified prior to the establishment of the Center by section 3.7 of this order shall be subject to automatic declassification only in accordance with subparagraphs (d)(3)(A)–(C) of this section.

(4) After consultation with the Director of the Information Security Oversight Office, an agency head may delay automatic declassification for up to 3 years from the date of discovery of classified records that were inadvertently not reviewed prior to the effective date of automatic declassification.

(e) Information exempted from automatic declassification under this section shall remain subject to the mandatory and systematic declassification review provisions of this order.

(f) The Secretary of State shall determine when the United States should commence negotiations with the appropriate officials of a foreign government or international organization of governments to modify any treaty or international agreement that requires the classification of information contained in records affected by this section for a period longer than 25 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this section.

(g) The Secretary of Energy shall determine when information concerning foreign nuclear programs that was removed from the Restricted Data category in order to carry out provisions of the National Security Act of 1947, as amended, may be declassified. Unless otherwise determined, such information shall be declassified when comparable information concerning the United States nuclear program is declassified.

(h) Not later than 3 years from the effective date of this order, all records exempted from automatic declassification under paragraphs (b) and (c) of this section shall be automatically declassified on December 31 of a year that is no more than 50 years from the date of origin, subject to the following:

(1) Records that contain information the release of which should clearly and demonstrably be expected to reveal the following are exempt from automatic declassification at 50 years:

(A) the identity of a confidential human source or a human intelligence source; or

(B) key design concepts of weapons of mass destruction.

(2) In extraordinary cases, agency heads may, within 5 years of the onset of automatic declassification, propose to exempt additional specific information from declassification at 50 years.

(3) Records exempted from automatic declassification under this paragraph shall be automatically declassified on December 31 of a year that is no more than 75 years from the date of origin unless an agency head, within 5 years of that date, proposes to exempt specific information from declassification at 75 years and the proposal is formally approved by the Panel.

(i) Specific records exempted from automatic declassification prior to the establishment of the Center described in section 3.7 of this order shall be subject to the provisions of paragraph (h) of this section in a scheduled and prioritized manner determined by the Center.

(j) At least 1 year before information is subject to automatic declassification under this section, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office, serving as Executive Secretary of the Panel, of any specific information that the agency proposes to exempt from automatic declassification under paragraphs (b) and (h) of this section.

(1) The notification shall include:

(A) a detailed description of the information, either by reference to information in specific records or in the form of a declassification guide;

(B) an explanation of why the information should be exempt from automatic declassification and must remain classified for a longer period of time; and

(C) a specific date or a specific and independently verifiable event for automatic declassification of specific records that contain the information proposed for exemption.

(2) The Panel may direct the agency not to exempt the information or to declassify it at an earlier date than recommended. An agency head may appeal such a decision to the President through the National Security Advisor. The information will remain classified while such an appeal is pending.

(k) For information in a file series of records determined not to have permanent historical value, the duration of classification beyond 25 years shall be the same as the disposition (destruction) date of those records in each Agency Records Control Schedule or General Records Schedule, although the duration of classification shall be extended if the record has been retained for business reasons beyond the scheduled disposition date.

Sec. 3.4. Systematic Declassification Review.

(a) Each agency that has originated classified information under this order or its predecessors shall establish and conduct a program for systematic declassification review for records of permanent historical value exempted from automatic declassification under section 3.3 of this order. Agencies shall prioritize their review of such records in accordance with priorities established by the Center.

(b) The Archivist shall conduct a systematic declassification review program for classified records:

(1) accessioned into the National Archives; (2) transferred to the Archivist pursuant to 44 U.S.C. 2203; and (3) for which the National Archives serves as the custodian for an agency or organization that has gone out of existence.

Sec. 3.5. Mandatory Declassification Review.

(a) Except as provided in paragraph (b) of this section, all information classified under this order or predecessor orders shall be subject to a review for declassification by the originating agency if:

(1) the request for a review describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort;

(2) the document or material containing the information responsive to the request is not contained within an operational file exempted from search and review, publication, and disclosure under 5 U.S.C. 552 in accordance with law; and

(3) the information is not the subject of pending litigation.

(b) Information originated by the incumbent President or the incumbent Vice President; the incumbent President's White House Staff or the incumbent Vice President's Staff; committees, commissions, or boards appointed by the incumbent President; or other entities within the Executive Office of the President that solely advise and assist the incumbent President is exempted from the provisions of paragraph (a) of this section. However, the Archivist shall have the authority to review, downgrade, and declassify papers or records of former Presidents and Vice Presidents under the control of the Archivist pursuant to 44 U.S.C. 2107, 2111, 2111 note, or 2203. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective Presidential papers or records. Agencies with primary subject matter interest shall be notified promptly of the Archivist's decision. Any final decision by the Archivist may be appealed by the requester or an agency to the Panel. The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information that no longer meets the standards for classification under this order. They shall release this information unless withholding is otherwise authorized and warranted under applicable law.

(d) If an agency has reviewed the requested information for declassification within the past 2 years, the agency need not conduct another review and may instead inform the requester of this fact and the prior review decision and advise the requester of appeal rights provided under subsection (e) of this section.

(e) In accordance with directives issued pursuant to this order, agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They also shall provide a means for administratively appealing a denial of a mandatory review request, and for notifying the requester of the right to appeal a final agency decision to the Panel.

(f) After consultation with affected agencies, the Secretary of Defense shall develop special procedures for the review of cryptologic information; the Director of National Intelligence shall develop special procedures for the review of information pertaining to intelligence sources, methods, and activities; and the Archivist shall develop special procedures for the review of information accessioned into the National Archives.

(g) Documents required to be submitted for prepublication review or other administrative process pursuant to an approved nondisclosure agreement are not covered by this section.

(h) This section shall not apply to any request for a review made to an element of the Intelligence Community that is made by a person other than an individual as that term is defined by 5 U.S.C. 552a(a)(2), or by a foreign government entity or any representative thereof.

Sec. 3.6. *Processing Requests and Reviews.* Notwithstanding section 4.1(i) of this order, in response to a request for information under the Freedom of Information Act, the Presidential Records Act, the Privacy Act of 1974, or the mandatory review provisions of this order:

(a) An agency may refuse to confirm or deny the existence or nonexistence of requested records whenever the fact of their existence or nonexistence is itself classified under this order or its predecessors.

(b) When an agency receives any request for documents in its custody that contain classified information that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies with respect to the classified information, or identifies such documents in the process of implementing sections 3.3 or 3.4 of this order, it shall refer copies of any request and the pertinent documents to the originating agency for processing and may, after consultation with the originating agency, inform any requester of the referral unless such association is itself classified under this order or its predecessors. In cases in which the originating agency determines in writing that a response under paragraph (a) of this section is required, the referring agency shall respond to the requester in accordance with that paragraph.

(c) Agencies may extend the classification of information in records determined not to have permanent historical value or nonrecord materials, including artifacts, beyond the time frames established in sections 1.5(b) and 2.2(f) of this order, provided:

- (1) the specific information has been approved pursuant to section 3.3(j) of this order for exemption from automatic declassification; and
- (2) the extension does not exceed the date established in section 3.3(j) of this order.

Sec. 3.7. National Declassification Center. (a) There is established within the National Archives a National Declassification Center to streamline declassification processes, facilitate quality-assurance measures, and implement standardized training regarding the declassification of records determined to have permanent historical value. There shall be a Director of the Center who shall be appointed or removed by the Archivist in consultation with the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, and the Director of National Intelligence.

(b) Under the administration of the Director, the Center shall coordinate:

- (1) timely and appropriate processing of referrals in accordance with section 3.3(d)(3) of this order for accessioned Federal records and transferred presidential records.

- (2) general interagency declassification activities necessary to fulfill the requirements of sections 3.3 and 3.4 of this order;

- (3) the exchange among agencies of detailed declassification guidance to enable the referral of records in accordance with section 3.3(d)(3) of this order;

- (4) the development of effective, transparent, and standard declassification work processes, training, and quality assurance measures;

- (5) the development of solutions to declassification challenges posed by electronic records, special media, and emerging technologies;

- (6) the linkage and effective utilization of existing agency databases and the use of new technologies to document and make public declassification review decisions and support declassification activities under the purview of the Center; and

- (7) storage and related services, on a reimbursable basis, for Federal records containing classified national security information.

(c) Agency heads shall fully cooperate with the Archivist in the activities of the Center and shall:

- (1) provide the Director with adequate and current declassification guidance to enable the referral of records in accordance with section 3.3(d)(3) of this order; and

- (2) upon request of the Archivist, assign agency personnel to the Center who shall be delegated authority by the agency head to review and exempt

or declassify information originated by their agency contained in records accessioned into the National Archives, after consultation with subject-matter experts as necessary.

(d) The Archivist, in consultation with representatives of the participants in the Center and after input from the general public, shall develop priorities for declassification activities under the purview of the Center that take into account the degree of researcher interest and the likelihood of declassification.

(e) Agency heads may establish such centralized facilities and internal operations to conduct internal declassification reviews as appropriate to achieve optimized records management and declassification business processes. Once established, all referral processing of accessioned records shall take place at the Center, and such agency facilities and operations shall be coordinated with the Center to ensure the maximum degree of consistency in policies and procedures that relate to records determined to have permanent historical value.

(f) Agency heads may exempt from automatic declassification or continue the classification of their own originally classified information under section 3.3(a) of this order except that in the case of the Director of National Intelligence, the Director shall also retain such authority with respect to the Intelligence Community.

(g) The Archivist shall, in consultation with the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, the Director of National Intelligence, the Director of the Central Intelligence Agency, and the Director of the Information Security Oversight Office, provide the National Security Advisor with a detailed concept of operations for the Center and a proposed implementing directive under section 5.1 of this order that reflects the coordinated views of the aforementioned agencies.

PART 4—SAFEGUARDING

Sec. 4.1. General Restrictions on Access.

(a) A person may have access to classified information provided that:

- (1) a favorable determination of eligibility for access has been made by an agency head or the agency head's designee;
- (2) the person has signed an approved nondisclosure agreement; and
- (3) the person has a need-to-know the information.

(b) Every person who has met the standards for access to classified information in paragraph (a) of this section shall receive contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

(c) An official or employee leaving agency service may not remove classified information from the agency's control or direct that information be declassified in order to remove it from agency control.

(d) Classified information may not be removed from official premises without proper authorization.

(e) Persons authorized to disseminate classified information outside the executive branch shall ensure the protection of the information in a manner equivalent to that provided within the executive branch.

(f) Consistent with law, executive orders, directives, and regulations, an agency head or senior agency official or, with respect to the Intelligence Community, the Director of National Intelligence, shall establish uniform procedures to ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information:

- (1) prevent access by unauthorized persons;
- (2) ensure the integrity of the information; and

(3) to the maximum extent practicable, use:

(A) common information technology standards, protocols, and interfaces that maximize the availability of, and access to, the information in a form and manner that facilitates its authorized use; and

(B) standardized electronic formats to maximize the accessibility of information to persons who meet the criteria set forth in section 4.1(a) of this order.

(g) Consistent with law, executive orders, directives, and regulations, each agency head or senior agency official, or with respect to the Intelligence Community, the Director of National Intelligence, shall establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

(h) Consistent with directives issued pursuant to this order, an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. "Confidential" information, including modified handling and transmission and allowing access to individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed an approved non-disclosure agreement.

(i)(1) Classified information originating in one agency may be disseminated to another agency or U.S. entity by any agency to which it has been made available without the consent of the originating agency, as long as the criteria for access under section 4.1(a) of this order are met, unless the originating agency has determined that prior authorization is required for such dissemination and has marked or indicated such requirement on the medium containing the classified information in accordance with implementing directives issued pursuant to this order.

(2) Classified information originating in one agency may be disseminated by any other agency to which it has been made available to a foreign government in accordance with statute, this order, directives implementing this order, direction of the President, or with the consent of the originating agency. For the purposes of this section, "foreign government" includes any element of a foreign government, or an international organization of governments, or any element thereof.

(3) Documents created prior to the effective date of this order shall not be disseminated outside any other agency to which they have been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information that originated within that agency.

(4) For purposes of this section, the Department of Defense shall be considered one agency, except that any dissemination of information regarding intelligence sources, methods, or activities shall be consistent with directives issued pursuant to section 6.2(b) of this order.

(5) Prior consent of the originating agency is not required when referring records for declassification review that contain information originating in more than one agency.

Sec. 4.2 Distribution Controls.

(a) The head of each agency shall establish procedures in accordance with applicable law and consistent with directives issued pursuant to this order to ensure that classified information is accessible to the maximum extent possible by individuals who meet the criteria set forth in section 4.1(a) of this order.

(b) In an emergency, when necessary to respond to an imminent threat to life or in defense of the homeland, the agency head or any designee

may authorize the disclosure of classified information (including information marked pursuant to section 4.1(i)(1) of this order) to an individual or individuals who are otherwise not eligible for access. Such actions shall be taken only in accordance with directives implementing this order and any procedure issued by agencies governing the classified information, which shall be designed to minimize the classified information that is disclosed under these circumstances and the number of individuals who receive it. Information disclosed under this provision or implementing directives and procedures shall not be deemed declassified as a result of such disclosure or subsequent use by a recipient. Such disclosures shall be reported promptly to the originator of the classified information. For purposes of this section, the Director of National Intelligence may issue an implementing directive governing the emergency disclosure of classified intelligence information.

(c) Each agency shall update, at least annually, the automatic, routine, or recurring distribution mechanism for classified information that it distributes. Recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in status occurs.

Sec. 4.3. *Special Access Programs.* (a) Establishment of special access programs. Unless otherwise authorized by the President, only the Secretaries of State, Defense, Energy, and Homeland Security, the Attorney General, and the Director of National Intelligence, or the principal deputy of each, may create a special access program. For special access programs pertaining to intelligence sources, methods, and activities (but not including military operational, strategic, and tactical programs), this function shall be exercised by the Director of National Intelligence. These officials shall keep the number of these programs at an absolute minimum, and shall establish them only when the program is required by statute or upon a specific finding that:

(1) the vulnerability of, or threat to, specific information is exceptional; and

(2) the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure.

(b) Requirements and limitations.

(1) Special access programs shall be limited to programs in which the number of persons who ordinarily will have access will be reasonably small and commensurate with the objective of providing enhanced protection for the information involved.

(2) Each agency head shall establish and maintain a system of accounting for special access programs consistent with directives issued pursuant to this order.

(3) Special access programs shall be subject to the oversight program established under section 5.4(d) of this order. In addition, the Director of the Information Security Oversight Office shall be afforded access to these programs, in accordance with the security requirements of each program, in order to perform the functions assigned to the Information Security Oversight Office under this order. An agency head may limit access to a special access program to the Director of the Information Security Oversight Office and no more than one other employee of the Information Security Oversight Office or, for special access programs that are extraordinarily sensitive and vulnerable, to the Director only.

(4) The agency head or principal deputy shall review annually each special access program to determine whether it continues to meet the requirements of this order.

(5) Upon request, an agency head shall brief the National Security Advisor, or a designee, on any or all of the agency's special access programs.

(6) For the purposes of this section, the term "agency head" refers only to the Secretaries of State, Defense, Energy, and Homeland Security, the

Attorney General, and the Director of National Intelligence, or the principal deputy of each.

(c) Nothing in this order shall supersede any requirement made by or under 10 U.S.C. 119.

Sec. 4.4. Access by Historical Researchers and Certain Former Government Personnel.

(a) The requirement in section 4.1(a)(3) of this order that access to classified information may be granted only to individuals who have a need-to-know the information may be waived for persons who:

- (1) are engaged in historical research projects;
- (2) previously have occupied senior policy-making positions to which they were appointed or designated by the President or the Vice President; or
- (3) served as President or Vice President.

(b) Waivers under this section may be granted only if the agency head or senior agency official of the originating agency:

- (1) determines in writing that access is consistent with the interest of the national security;
- (2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this order; and
- (3) limits the access granted to former Presidential appointees or designees and Vice Presidential appointees or designees to items that the person originated, reviewed, signed, or received while serving as a Presidential or Vice Presidential appointee or designee.

PART 5—IMPLEMENTATION AND REVIEW

Sec. 5.1. Program Direction. (a) The Director of the Information Security Oversight Office, under the direction of the Archivist and in consultation with the National Security Advisor, shall issue such directives as are necessary to implement this order. These directives shall be binding on the agencies. Directives issued by the Director of the Information Security Oversight Office shall establish standards for:

- (1) classification, declassification, and marking principles;
- (2) safeguarding classified information, which shall pertain to the handling, storage, distribution, transmittal, and destruction of and accounting for classified information;
- (3) agency security education and training programs;
- (4) agency self-inspection programs; and
- (5) classification and declassification guides.

(b) The Archivist shall delegate the implementation and monitoring functions of this program to the Director of the Information Security Oversight Office.

(c) The Director of National Intelligence, after consultation with the heads of affected agencies and the Director of the Information Security Oversight Office, may issue directives to implement this order with respect to the protection of intelligence sources, methods, and activities. Such directives shall be consistent with this order and directives issued under paragraph (a) of this section.

Sec. 5.2. Information Security Oversight Office. (a) There is established within the National Archives an Information Security Oversight Office. The Archivist shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

(b) Under the direction of the Archivist, acting in consultation with the National Security Advisor, the Director of the Information Security Oversight Office shall:

- (1) develop directives for the implementation of this order;

- (2) oversee agency actions to ensure compliance with this order and its implementing directives;
- (3) review and approve agency implementing regulations prior to their issuance to ensure their consistency with this order and directives issued under section 5.1(a) of this order;
- (4) have the authority to conduct on-site reviews of each agency's program established under this order, and to require of each agency those reports and information and other cooperation that may be necessary to fulfill its responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the President through the National Security Advisor within 60 days of the request for access. Access shall be denied pending the response;
- (5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend Presidential approval through the National Security Advisor;
- (6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the program established under this order;
- (7) have the authority to prescribe, after consultation with affected agencies, standardization of forms or procedures that will promote the implementation of the program established under this order;
- (8) report at least annually to the President on the implementation of this order; and
- (9) convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

Sec. 5.3. *Interagency Security Classification Appeals Panel.*

(a) Establishment and administration.

- (1) There is established an Interagency Security Classification Appeals Panel. The Departments of State, Defense, and Justice, the National Archives, the Office of the Director of National Intelligence, and the National Security Advisor shall each be represented by a senior-level representative who is a full-time or permanent part-time Federal officer or employee designated to serve as a member of the Panel by the respective agency head. The President shall designate a Chair from among the members of the Panel.
- (2) Additionally, the Director of the Central Intelligence Agency may appoint a temporary representative who meets the criteria in paragraph (a)(1) of this section to participate as a voting member in all Panel deliberations and associated support activities concerning classified information originated by the Central Intelligence Agency.
- (3) A vacancy on the Panel shall be filled as quickly as possible as provided in paragraph (a)(1) of this section.
- (4) The Director of the Information Security Oversight Office shall serve as the Executive Secretary of the Panel. The staff of the Information Security Oversight Office shall provide program and administrative support for the Panel.
- (5) The members and staff of the Panel shall be required to meet eligibility for access standards in order to fulfill the Panel's functions.
- (6) The Panel shall meet at the call of the Chair. The Chair shall schedule meetings as may be necessary for the Panel to fulfill its functions in a timely manner.
- (7) The Information Security Oversight Office shall include in its reports to the President a summary of the Panel's activities.

(b) Functions. The Panel shall:

- (1) decide on appeals by persons who have filed classification challenges under section 1.8 of this order;
- (2) approve, deny, or amend agency exemptions from automatic declassification as provided in section 3.3 of this order;
- (3) decide on appeals by persons or entities who have filed requests for mandatory declassification review under section 3.5 of this order; and
- (4) appropriately inform senior agency officials and the public of final Panel decisions on appeals under sections 1.8 and 3.5 of this order.

(c) Rules and procedures. The Panel shall issue bylaws, which shall be published in the *Federal Register*. The bylaws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel shall provide that the Panel will consider appeals only on actions in which:

- (1) the appellant has exhausted his or her administrative remedies within the responsible agency;
- (2) there is no current action pending on the issue within the Federal courts; and
- (3) the information has not been the subject of review by the Federal courts or the Panel within the past 2 years.

(d) Agency heads shall cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner. The Panel shall report to the President through the National Security Advisor any instance in which it believes that an agency head is not cooperating fully with the Panel.

(e) The Panel is established for the sole purpose of advising and assisting the President in the discharge of his constitutional and discretionary authority to protect the national security of the United States. Panel decisions are committed to the discretion of the Panel, unless changed by the President.

(f) An agency head may appeal a decision of the Panel to the President through the National Security Advisor. The information shall remain classified pending a decision on the appeal.

Sec. 5.4. General Responsibilities. Heads of agencies that originate or handle classified information shall:

(a) demonstrate personal commitment and commit senior management to the successful implementation of the program established under this order;

(b) commit necessary resources to the effective implementation of the program established under this order;

(c) ensure that agency records systems are designed and maintained to optimize the appropriate sharing and safeguarding of classified information, and to facilitate its declassification under the terms of this order when it no longer meets the standards for continued classification; and

(d) designate a senior agency official to direct and administer the program, whose responsibilities shall include:

- (1) overseeing the agency's program established under this order, provided an agency head may designate a separate official to oversee special access programs authorized under this order. This official shall provide a full accounting of the agency's special access programs at least annually;
- (2) promulgating implementing regulations, which shall be published in the *Federal Register* to the extent that they affect members of the public;
- (3) establishing and maintaining security education and training programs;
- (4) establishing and maintaining an ongoing self-inspection program, which shall include the regular reviews of representative samples of the agency's

original and derivative classification actions, and shall authorize appropriate agency officials to correct misclassification actions not covered by sections 1.7(c) and 1.7(d) of this order; and reporting annually to the Director of the Information Security Oversight Office on the agency's self-inspection program;

(5) establishing procedures consistent with directives issued pursuant to this order to prevent unnecessary access to classified information, including procedures that:

(A) require that a need for access to classified information be established before initiating administrative clearance procedures; and

(B) ensure that the number of persons granted access to classified information meets the mission needs of the agency while also satisfying operational and security requirements and needs;

(6) developing special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;

(7) ensuring that the performance contract or other system used to rate civilian or military personnel performance includes the designation and management of classified information as a critical element or item to be evaluated in the rating of:

(A) original classification authorities;

(B) security managers or security specialists; and

(C) all other personnel whose duties significantly involve the creation or handling of classified information, including personnel who regularly apply derivative classification markings;

(8) accounting for the costs associated with the implementation of this order, which shall be reported to the Director of the Information Security Oversight Office for publication;

(9) assigning in a prompt manner agency personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of this order that pertains to classified information that originated in a component of the agency that no longer exists and for which there is no clear successor in function; and

(10) establishing a secure capability to receive information, allegations, or complaints regarding over-classification or incorrect classification within the agency and to provide guidance to personnel on proper classification as needed.

Sec. 5.5. Sanctions. (a) If the Director of the Information Security Oversight Office finds that a violation of this order or its implementing directives has occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and its contractors, licensees, certificate holders, and grantees shall be subject to appropriate sanctions if they knowingly, willfully, or negligently:

(1) disclose to unauthorized persons information properly classified under this order or predecessor orders;

(2) classify or continue the classification of information in violation of this order or any implementing directive;

(3) create or continue a special access program contrary to the requirements of this order; or

(4) contravene any other provision of this order or its implementing directives.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this order.

(e) The agency head or senior agency official shall:

(1) take appropriate and prompt corrective action when a violation or infraction under paragraph (b) of this section occurs; and

(2) notify the Director of the Information Security Oversight Office when a violation under paragraph (b)(1), (2), or (3) of this section occurs.

PART 6—GENERAL PROVISIONS

Sec. 6.1. Definitions. For purposes of this order:

(a) “Access” means the ability or opportunity to gain knowledge of classified information.

(b) “Agency” means any “Executive agency,” as defined in 5 U.S.C. 105; any “Military department” as defined in 5 U.S.C. 102; and any other entity within the executive branch that comes into the possession of classified information.

(c) “Authorized holder” of classified information means anyone who satisfies the conditions for access stated in section 4.1(a) of this order.

(d) “Automated information system” means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

(e) “Automatic declassification” means the declassification of information based solely upon:

(1) the occurrence of a specific date or event as determined by the original classification authority; or

(2) the expiration of a maximum time frame for duration of classification established under this order.

(f) “Classification” means the act or process by which information is determined to be classified information.

(g) “Classification guidance” means any instruction or source that prescribes the classification of specific information.

(h) “Classification guide” means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

(i) “Classified national security information” or “classified information” means information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

(j) “Compilation” means an aggregation of preexisting unclassified items of information.

(k) “Confidential source” means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

(l) “Damage to the national security” means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

(m) “Declassification” means the authorized change in the status of information from classified information to unclassified information.

(n) “Declassification guide” means written instructions issued by a declassification authority that describes the elements of information regarding

a specific subject that may be declassified and the elements that must remain classified.

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

(p) "Document" means any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

(q) "Downgrading" means a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

(r) "File series" means file units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access or use.

(s) "Foreign government information" means:

(1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

(2) information produced by the United States Government pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or

(3) information received and treated as "foreign government information" under the terms of a predecessor order.

(t) "Information" means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, is produced by or for, or is under the control of the United States Government.

(u) "Infraction" means any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not constitute a "violation," as defined below.

(v) "Integral file block" means a distinct component of a file series, as defined in this section, that should be maintained as a separate unit in order to ensure the integrity of the records. An integral file block may consist of a set of records covering either a specific topic or a range of time, such as a Presidential administration or a 5-year retirement schedule within a specific file series that is retired from active use as a group. For purposes of automatic declassification, integral file blocks shall contain only records dated within 10 years of the oldest record in the file block.

(w) "Integrity" means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

(x) "Intelligence" includes foreign intelligence and counterintelligence as defined by Executive Order 12333 of December 4, 1981, as amended, or by a successor order.

(y) "Intelligence activities" means all activities that elements of the Intelligence Community are authorized to conduct pursuant to law or Executive Order 12333, as amended, or a successor order.

(z) "Intelligence Community" means an element or agency of the U.S. Government identified in or designated pursuant to section 3(4) of the National Security Act of 1947, as amended, or section 3.5(h) of Executive Order 12333, as amended.

(aa) "Mandatory declassification review" means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.5 of this order.

(bb) "Multiple sources" means two or more source documents, classification guides, or a combination of both.

(cc) "National security" means the national defense or foreign relations of the United States.

(dd) "Need-to-know" means a determination within the executive branch in accordance with directives issued pursuant to this order that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(ee) "Network" means a system of two or more computers that can exchange data or information.

(ff) "Original classification" means an initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure.

(gg) "Original classification authority" means an individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to classify information in the first instance.

(hh) "Records" means the records of an agency and Presidential papers or Presidential records, as those terms are defined in title 44, United States Code, including those created or maintained by a government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant.

(ii) "Records having permanent historical value" means Presidential papers or Presidential records and the records of an agency that the Archivist has determined should be maintained permanently in accordance with title 44, United States Code.

(jj) "Records management" means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations.

(kk) "Safeguarding" means measures and controls that are prescribed to protect classified information.

(ll) "Self-inspection" means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this order and its implementing directives.

(mm) "Senior agency official" means the official designated by the agency head under section 5.4(d) of this order to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

(nn) "Source document" means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

(oo) "Special access program" means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

(pp) "Systematic declassification review" means the review for declassification of classified information contained in records that have been determined by the Archivist to have permanent historical value in accordance with title 44, United States Code.

(qq) "Telecommunications" means the preparation, transmission, or communication of information by electronic means.

(rr) "Unauthorized disclosure" means a communication or physical transfer of classified information to an unauthorized recipient.

(ss) "U.S. entity" includes:

(1) State, local, or tribal governments;

(2) State, local, and tribal law enforcement and firefighting entities;

(3) public health and medical entities;

(4) regional, state, local, and tribal emergency management entities, including State Adjutants General and other appropriate public safety entities; or

(5) private sector entities serving as part of the nation's Critical Infrastructure/Key Resources.

(tt) "Violation" means:

(1) any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;

(2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or

(3) any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of this order.

(uu) "Weapons of mass destruction" means any weapon of mass destruction as defined in 50 U.S.C. 1801(p).

Sec. 6.2. General Provisions. (a) Nothing in this order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947, as amended. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Director of National Intelligence may, with respect to the Intelligence Community and after consultation with the heads of affected departments and agencies, issue such policy directives and guidelines as the Director of National Intelligence deems necessary to implement this order with respect to the classification and declassification of all intelligence and intelligence-related information, and for access to and dissemination of all intelligence and intelligence-related information, both in its final form and in the form when initially gathered. Procedures or other guidance issued by Intelligence Community element heads shall be in accordance with such policy directives or guidelines issued by the Director of National Intelligence. Any such policy directives or guidelines issued by the Director of National Intelligence shall be in accordance with directives issued by the Director of the Information Security Oversight Office under section 5.1(a) of this order.

(c) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(d) Nothing in this order limits the protection afforded any information by other provisions of law, including the Constitution, Freedom of Information Act exemptions, the Privacy Act of 1974, and the National Security Act of 1947, as amended. This order is not intended to and does not create any right or benefit, substantive or procedural, enforceable at law

by a party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person. The foregoing is in addition to the specific provisos set forth in sections 1.1(b), 3.1(c) and 5.3(e) of this order.

(e) Nothing in this order shall be construed to obligate action or otherwise affect functions by the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(f) This order shall be implemented subject to the availability of appropriations.

(g) Executive Order 12958 of April 17, 1995, and amendments thereto, including Executive Order 13292 of March 25, 2003, are hereby revoked as of the effective date of this order.

Sec. 6.3. *Effective Date.* This order is effective 180 days from the date of this order, except for sections 1.7, 3.3, and 3.7, which are effective immediately.

Sec. 6.4. *Publication.* The Archivist of the United States shall publish this Executive Order in the *Federal Register*.

A handwritten signature in black ink, appearing to be Barack Obama's signature, consisting of a large 'B' followed by a circle and a horizontal line.

THE WHITE HOUSE,

December 29, 2009.

[FR Doc. E9-31418
Filed 1-4-10; 11:15 am]
Billing code 7515-01-P