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 356B (GOV) **Government Response** To Defense Motion to Compel Production of Discovery Regarding Revocation of Access to Classified Networks 20 April 2015

1. Timeliness

This Response is timely filed pursuant to Military Commissions Trial Judiciary Rule of Court (R.C.) 3.7.

2. Relief Sought

The Prosecution respectfully requests this Commission deny, without oral argument, AE 356 (AAA), the Defense Motion to Compel Production of Discovery Regarding Revocation of Access to Classified Networks.

3. Burden of proof

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

4. Facts

On 16 October 2012, Defense counsel for Mr. Ali acknowledged during an open-session of this Commission that the Defense held SIPRNet as well as JWICS accounts and, additionally, had "access to other streams of classified information that [does not] come from the prosecution." *See* Unofficial/ Unauthenticated Transcript (Tr.) at 573-574. Learned Counsel also represented to this Commission that "[i]n a federal proceeding, generally any classified information that a defendant -- that a defense counsel has comes from one of two sources. Most

comes from government discovery, and, if it is an insider case, some comes from their client." *See id.* at 573.

On 18 July 2013, the Secretary of Defense ("SECDEF") issued a memorandum to the Director, Washington Headquarters Services (WHS), directing that WHS "disable all JWICS and SIPR browsing capability, excepting Sharepoint and browser functionality that is required to access vaulted emails or required for file sharing capabilities, for all OMC personnel not approved for access per the individual justification process." AE 356 (AAA), Attachment B. The SECDEF also established the Director, WHS, as the approval authority for "access to JWICS and SIPRNet browser capability on an individualized basis for OMC individuals based on a written detailed need-to-know justification." *Id.*

On 8 November 2013, Defense counsel for Mr. Ali submitted a memorandum to the Director, WHS, requesting access to JWICS and SIPRNet browsing capability for [redacted] a Defense Security Officer (DSO). *See* AE 356 (AAA), Attachment D.

On 13 and 20 December 2013, the Director, WHS, disapproved the Defense request stating, "[m]y staff, in consultation with Office of the Secretary of Defense stakeholders, has determined that your request does not establish the need-to-know requirement, which is required to grant access." AE 356 (AAA), Attachment E.

On 6 April 2015, the Defense filed the instant motion requesting "that the military commission compel production of discovery relating to the Secretary of Defense's 18 July 2013 Memorandum revoking OMC access to SIPRNet and JWICS." AE 356 (AAA) at 1. The instant motion is premised on the assertions that, (1) the requested discovery is expected to provide evidence of unlawful influence over defense counsel; (2) the requested discovery is expected to show a violation of the principle of equality of arms; and, (3) the requested discovery directly addresses the issue raised in AE 350B (GOV), specifically, whether the defense has the capacity to vet interpreters and other consultants. *See id.* at 6-7.

5. Law and Argument

The Military Commissions Act of 2009 ("M.C.A.") affords the Defense a reasonable opportunity to obtain evidence through a process comparable to other United States criminal courts. *See* 10 U.S.C. § 949j. Pursuant to the M.C.A., the Rules for Military Commissions (R.M.C.) require that the government produce evidence that is material to the preparation of the defense. Specifically, R.M.C. 701(c)(1) requires the Prosecution to permit defense counsel to examine,

> [a]ny books, papers, documents, photographs, tangible objects, buildings, or places, or copies of portions thereof, which are within the possession, custody, or control of the Government, the existence of which is known or by the exercise of due diligence may become known to trial counsel, and which are material to the preparation of the defense or are intended for use by the trial counsel as evidence in the prosecution case-in-chief at trial.

See R.M.C. 701 (c)(1). However, notwithstanding this requirement, no authority grants defendants an unqualified right to receive, or compels the government to produce, discovery merely because the defendant has requested it. Rather, the government's discovery obligations are defined by the relevant rules and statutes. *See generally United States v. Agurs*, 427 U.S. 97, 106 (1976) (noting that "there is, of course, no duty to provide defense counsel with unlimited discovery of everything known by the prosecutor").

A criminal defendant has a right to discover certain materials, but the scope of this right and the government's attendant discovery obligations are not without limit. For example, upon request, the government must permit the defendant to inspect and copy documents in the government's possession, but only if the documents meet the requirements of R.M.C. 701. Military courts have adopted a standard by which "relevant evidence means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence." *United States v. Graner*, 69 M.J. 104, 107-108 (2010). In instances where the Defense did not present an adequate theory of relevance to justify the compelled production of evidence, C.A.A.F has

applied the relevance standard in upholding denials of compelled production. *See Graner*, 69 M.J. at 107-109. A defense theory that is too speculative, and too insubstantial, does not meet the threshold of relevance and necessity for the admission of evidence. *See United States v. Sanders*, 2008 WL 2852962 (A.F.Ct.Crim.App. 2008) (citing *United States v. Briggs,* 46 M.J. 699, 702 (A.F.Ct.Crim.App.1996)). A general description of the material sought or a conclusory argument as to its materiality is insufficient. *See Briggs*, 46 M.J. at 702 (citing *United States v. Branoff*, 34 M.J. 612, 620 (A.F.C.C.A. 1992) (remanded on other grounds) (citing *United States v. Cadet*, 727 F.2d 1453, 1468 (9th Cir. 1984))).

As this Commission lacks the authority to grant access to JWICS and SIPRNet browsing capabilities, *see* AE 232C at 1, it should deny the Defense request as it fails to adequately demonstrate the relevancy and materiality of the requested information to an issue before this Commission.

I. The Defense Cannot Challenge an Adverse "Need-to-Know" Determination Before This Commission

As this Commission is well-aware, the process of obtaining authorization to access classified information is multi-faceted. First, an individual must obtain the necessary security clearance, which grants that person permission to view classified material.[1] 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, 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

[1] A security clearance merely grants a person permission to view classified material; however, it does not entitle an individual to access all classified information. *See 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).

unnecessarily disseminated regardless of whether an individual holds the appropriate security clearance.). In this case, acting pursuant to their authority, both the SECDEF as well as the Director, WHS, made a determination that certain OMC personnel, [redacted], did not possess the requisite "need-to-know" with respect to the information resident on JWICS and SIPRNet. *See* AE 356 (AAA), Attachment B *and* E. While the Defense may disagree with that determination, this Military Commission is not the proper forum to seek reconsideration or redress, as it has previously found that it lacks the authority to determine who has a "need-to-know" classified information. *See* AE 232C at 1.

This Commission, as well as Defense counsel for Mr. Ali, have appropriately acknowledged that an Original Classification Authority (OCA) serves as the single-source authority to determine whether an individual has a "need-to-know" certain classified information.[2] This recognition is consistent with U.S. statutory and regulatory provisions, as well as U.S. Supreme Court precedent. *See* 10 U.S.C. § 949p-1(a) ("[c]lassified 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."); Exec. Order No. 13,526, 3 C.F.R. 1326 (2009) ("'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 a specific classified information in order to perform or assist in a lawful and authorized governmental function"); *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."); *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

[2] *See* Tr. at 769 ("MJ [COL POHL]: Who do you believe determines the need to know? LDC [MR. CONNELL]: An authorized holder of classified information."); *see also* AE 013DDD at 9 ("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: . . . (3) a need-to-know for the classified information at issue, as determined by the Original Classification Authority (OCA) for that information.").

disclosure). The Defense may now certainly disagree with the determination made by the SECDEF and Director, WHS, with regard to JWICS and SIPRNet access, but it cannot now request the Commission to intervene and order discovery on internal deliberations discussing the need-to-know determination, where it has cited no legal authority for the premise that they had some legal right to access to the databases in the first instance.

It is clear in filing the instant pleading that the Defense merely wishes to utilize the Commission as a forum and tool to dispute the "need-to-know" determination made by the OCA in this case. While the Defense claims that the requested information "is material to the preparation of the defense with respect to multiple issues," *see* AE 356 (AAA) at 6, their thinly proffered theories of materiality quickly fold under the most cursory scrutiny. Therefore, the Commission should deny the Defense request and should do so without entertaining oral argument.

II. An Adverse "Need-to-Know" Determination Does Not Give Rise to Unlawful Influence

Within their motion, Defense counsel for Mr. Ali assert that "the requested discovery is expected to provide evidence of unlawful influence over defense counsel." *Id.* Further, they contend that the SECDEF memorandum "certainly appears to target defense counsel; the communications which led to the revocation, and the implementation of the revocation and restorations, are expected to confirm this view." *Id.* However, even while they make such allegations, they fail to advance any legal or factual theory that substantively demonstrates a legal right to access the subject databases such that an adverse "need-to-know" determination by an OCA would represent "unlawful influence." Instead, they merely cite and state the statutory definition of unlawful influence as found in 10 U.S.C.§ 949b(a)(2), with the tenuous hope that the definition will somehow satisfy their burden. This Commission must and should demand a more specific showing from the Defense as to materiality and relevancy. *See Briggs*, 46 M.J. at 702 (citing *United States v. Branoff*, 34 M.J. 612, 620 (A.F.C.C.A. 1992) (remanded on other grounds)(citing *United States v. Cadet*, 727 F.2d 1453, 1468 (9th Cir. 1984))) ("[a] general

description of the material sought or a conclusory argument as to their materiality is insufficient."). Absent such a showing, the Commission should respectfully deny the Defense request.

However, even if Defense counsel for Mr. Ali could muster a more specific theory as to relevancy and/or materiality, it is unlikely that they will be able to meet their burden and demonstrate that an adverse "need-to-know" determination gives rise to unlawful influence. As previously stated in Section I, a "need-to-know" determination is a determination *made within the Executive Branch* that a prospective recipient requires access to a specific classified information in order to perform or assist in a lawful and authorized governmental function. *See* Exec. Order No. 13,526, 3 C.F.R. 1326 (2009) (emphasis added). Where Defense counsel have other authorized means to receive relevant and material classified information, *see* R.M.C. 701(f), M.C.R.E. 505(f), and may have been using SIPRNet and JWICS to circumvent those established procedures, the OCA acted appropriately in revoking all OMC personnel access to those two classified systems, absent an individual "need-to-know" justification. To deem the OCA's decision as unlawful influence would establish a dangerous precedent and interfere with the Executive Branch's duty to protect intelligence activities, sources and methods where no "need-to-know" exists. This Commission should not entertain such reasoning/logic and should reject it on its face.

III. The Military Commissions Act Provides the Defense With Access to Relevant and Material Evidence

Beyond their specious argument that the revocation of Defense access to JWICS and SIPRNet represents unlawful influence, the Defense also argues that "the requested discovery is expected to show a violation of equality of arms, one of the indispensable judicial guarantees under Common Article 3." *See* AE 356 (AAA) at 6.[3] The Defense further states that "some

[3] In AE 356 (AAA), the Defense cites to European Court of Human Rights case of *Bulut v. Austria*, 1996 Eur. Ct. no. 17358/90 (22 Feb 1996), in support of their argument that their lack of access to JWICS and SIPRNet does not provide the Defense with "equality of arms." It should be noted, however, that the European Court of Human Rights was not speaking of discovery issues when speaking of "equality of arms," but rather "considered that it is

person or organization has unreasonably impeded the access of the defense to evidence available to the prosecution on SIPRNet and JWICS." *Id.*

The Defense argument completely ignores the concept of the discovery process envisioned by the Military Commissions Act of 2009 and the Manual for Military Commissions (M.M.C.); specifically, that a criminal defendant will receive access to "[a]ny books, papers, documents, photographs, tangible objects, buildings, or places, or copies of portions thereof, which are within the possession, custody, or control of the Government, the existence of which is known or by the exercise of due diligence may become known to trial counsel, and which are material to the preparation of the Defense . . . ," *see* R.M.C. 701(c)(1), and that classified information shall be protected and is privileged from disclosure if disclosure would be detrimental to the national security. *See* M.C.R.E. 505(a)(1). Nothing within the Federal Rules of Criminal Procedure, *see* Rule 16, the Rules for Courts-Martial, *see* Rule 701, or the Rules for Military Commission, *see* Rule 701, allow for unconstrained and unrestricted access to official Government information systems, writ large, especially information which is classified in nature and may bear no relevancy to a case in litigation.

It was a mistake that someone had permitted Defense counsel, whose sole duty of loyalty lies with their clients (who, in this case, also happen to be Alien Unprivileged Enemy Belligerents in an on-going war against the United States), unfettered access to classified government information systems and databases in the first place. Such access is unheard of in federal court or courts-martial practice, and was an anomaly that was, and should have been, quickly corrected by the Original Classification Authority once that fact became publicly known following Mr. Connell's comments. Learned Counsel for Mr. Ali recognized such to the

---

inherently unfair for the prosecution to make submissions to a court without the knowledge of the defence and on which the defence has no opportunity to comment." *See id.* at para. 46. The Defense can cite to no national security case dealing with classified information where a judge determined that Defense counsel, under a theory of "equality of arms" must be given equal access to all classified information in the U.S. government's possession. Such a determination would be contrary to almost every single rule, regulation, or law protecting classified information. The Defense will have access to all classified information it is entitled to under the Military Commissions Act of 2009 and the Manual for Military Commissions.

Commission, when he stated, "[i]n a federal proceeding, generally any classified information that a defendant -- that a defense counsel has comes from one of two sources. Most comes from government discovery, and, if it is an insider case, some comes from their client." *See* Tr. at 573. As the process described by the Defense is how classified information is provided in every National Security case, the Defense argument that lack of access to SIPRNet and JWICS *unreasonably* impedes Defense access to relevant and material evidence should be rejected outright.

All government information the Defense seeks, whether classified or unclassified, should be provided by the Prosecution through the discovery process set forth in the M.C.A. and the M.M.C. Under that process, the Prosecution has an affirmative obligation to search for and provide certain materials regardless of whether the Defense requests the information, as well as a further obligation to review Defense requests for discovery and determine if the information they seek is required to be disclosed pursuant to the applicable discovery rules. *See generally* R.M.C. 701.

When it is classified information the Defense seeks, the Prosecution first must make a determination regarding whether the material is discoverable, and will convey its determination to an Original Classification Authority. Based on the Prosecution's determination, the Original Classification Authority can determine that the Defense has a "need-to-know," but is still not required to do so. Following that determination, if the OCA has found the Defense counsel have a "need-to-know," the Prosecution can avail itself of the protections and privileges afforded it under M.C.R.E. 505.

Should the Original Classification Authority decide, contrary to the determination made by the Prosecution, that the Defense still does not possess a "need-to-know," the Prosecution would have an obligation to so inform the Commission, and the Commission could craft an appropriate remedy; however, that does not change the fact that the Original Classification Authority ultimately makes an independent "need-to-know" determination, and is the only one who can authorize disclosure of classified information. Such a distinction is recognized under

the Manual for Military Commissions. *See* M.C.R.E. 505(a)(1) ("under no circumstances may a military judge order the release of classified information to any person not authorized to receive such information.").

While such an instance has not occurred in this case, it illustrates the fact that not only is the Original Classification Authority the only entity that can ultimately determine who has a "need-to-know," but also how granting Defense counsel of sworn enemies of the United States unfettered access to classified databases is contrary to nearly every safeguard and "need-to-know" principle that protects classified information, and also represents a complete end-run around the M.C.R.E 505 process (as well as the CIPA process it was modeled after). *See* M.C.R.E. 505(a)(4).

In National Security litigation, the Defense's "need-to-know" classified information is nearly always established only after the prosecution or, upon defense motion, a judge, determines that the Defense is entitled to the classified information under the discovery rules; a determination that clearly did not occur prior to Defense gaining access to the SIPRNet and JWICS databases in this instance. Even if some Original Classification Authority had, at one time, completely outside of the military commissions discovery process, made a determination that the Defense counsel had a "need-to-know" every classified document in SIPRNet and JWICS it had access to, nothing prevents an Original Classification Authority from revisiting that decision, as was apparently done here following the public revelations of access by Defense counsel. The Defense clearly cannot establish a legal right to such unfettered access to classified information; nor, therefore, can it carry its burden on this motion for discovery regarding he reason someone decided to take away access they were not entitled to from the beginning.

IV. There Is No Nexus Between The Requested Information and Those Issues Present in the AE 350 Series of Motions

Lastly, the Defense puts forth the argument that "the requested discovery directly addresses the issue raised in AE 350B; whether the defense has the capacity to vet interpreters and other consultants." *See* AE 356 (AAA) at 7. More specifically, they assert that "the

discovery is expected to show that the defense is the one element of OMC which lacks the capacity to vet interpreters and other consultants either for previous national security involvement or for national security risks." *Id.* While the fact that the Defense now lacks access to JWICS and SIPRNet may be probative to any Defense argument that they do not currently have the capability to thoroughly vet interpreters and other consultants to their satisfaction, there is actually no nexus between the issues contained within the AE 350 series of motions and the requested discovery. Any internal government deliberations or communications pertaining to the manner in which the subject "need-to-know" determination was made is not relevant to whether the Defense has or does not have the ability to vet certain defense personnel. Furthermore, there is no evidence to suggest that access to these databases could actually help perform a vetting function; it is all conjecture that said access could even serve that purpose at all, and specifically for the interpreter issue arising under AE 350. All that should be relevant in such an argument is whether in fact the Defense has access to the networks. To that extent, the Prosecution is willing to stipulate to Attachments B through G of the Defense filing and to the fact that the Defense no longer has access to these networks and databases. With that being the case, the Commission should once again decline to entertain the Defense's stated basis for relevancy and materiality for the requested discovery and deny the instant motion.

6. <u>Conclusion</u>

This Commission should deny AE 356 (AAA), the Defense Motion to Compel Production of Discovery Regarding Revocation of Access to Classified Networks, without entertaining oral argument. The Defense has failed to adequately demonstrate how the requested discovery is relevant and/or material to an issue now before this Commission as demonstrated above. While it is evident that the Defense disagrees with the determination made by the Original Classification Authority, this Commission does not represent the proper forum to request reconsideration or redress of that "need-to-know" determination. For that reason, as well

as the reasons stated above, the Prosecution respectfully requests the Commission deny the instant motion.

7. Oral Argument

The Prosecution does not request oral argument, and posits that this issue of law should be resolved by the Commission on the parties' submissions alone, and that no oral argument need be granted.

8. Witnesses and Evidence

The Prosecution will not rely on any witnesses or additional evidence in support of this motion.

9. Additional Information

The Prosecution has no additional information.

10. Attachments

A. Certificate of Service, dated 20 April 2015

Respectfully submitted,

_____//s//_____
Clay Trivett
Managing Deputy Trial Counsel

Mark Martins
Chief Prosecutor
Military Commissions

ATTACHMENT A

CERTIFICATE OF SERVICE

I certify that on the 20th day of April 2015, I filed AE 356B(GOV) the **Government Response** To Defense Motion to Compel Production of Discovery Regarding Revocation of Access to Classified Networks with the Office of Military Commissions Trial Judiciary and I served a copy on counsel of record.

_____//s//_____
Clay Trivett
Managing Deputy Trial Counsel
Office of the Chief Prosecutor
Office of Military Commissions