

**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 177A

Government Response

To Defense Motion to Compel Production
of Discovery of Information Related to
Government Intrusion Into Electronic or
Physical Spaces Containing Defense-
Related and/or Defense-Produced Materials

9 July 2013

1. Timeliness

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

2. Relief Sought

The Prosecution respectfully requests that the Commission deny the Defense motion to compel additional discovery on this topic.

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. Overview

The Defense is once again requesting that this Commission order the Prosecution to prove a negative. This time, counsel for the Accused asserts the baseless allegation that “[t]he government has exercised no diligence in determining what evidence of governmental intrusion into defense electronic and physical spaces.” AE 177 (WBA), at 10. However, the fact remains that there has been no governmental “intrusion” into privileged materials or spaces. As such, the Defense should not confuse the Prosecution’s failure to prove a negative with a lack of

reasonable due diligence. Quite the contrary, the Prosecution has been extremely proactive with regard to defense IT concerns in both practical measures and informational awareness. *See, e.g.* AE 154; *see also* Unofficial/Unauthenticated Transcript, *United States v. Nashiri*, at 2013-2085 (detailing technical measures to effectively isolate the defense network). The instant motion expounds demonstrably inaccurate or conflated assertions and depicts them as fact. This motion should be denied without argument.

5. Facts

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 9 April 2013, counsel for Mr. bin 'Attash filed AE 148A (WBA). That filing requested a continuance with respect to ten of the 19 docketed motions in this case. The sole basis for that request was the unsubstantiated assertion that the Defense lost data pertaining to the docketed motions.

On 10 April 2013, the Chief Defense Counsel issued an order to all OCDC personnel prohibiting the transmission of privileged materials over the Government network and instructing OCDC personnel to refrain from saving privileged materials on the networked "O" and "H" drives. *See* AE 155, Attachment C. However, the Chief Defense Counsel specifically authorized counsel in this case to access and use external hard drives to draft and file computer-generated motions and other documents. *Id.* The Defense was advised that the external hard

drives “allow you to create and store documents—especially those necessary to meet court imposed filing deadlines.” *Id.*

On 11 April 2013, the Prosecution responded, citing various facts demonstrating that the data loss was limited to brief periods of time—in one case the Defense experienced an information loss lasting about one day. *See* AE 148B. The Prosecution also advised the Commission that the computer problems experienced by various personnel were not the result of inherent problems with the network or targeted monitoring. *Id.* Rather, it was a problem limited to the now completed replication. The Prosecution incorporates by reference the facts and argument of AE 148B into this response.

On 12 April 2013, the Defense filed AE 155A. In that motion, the Chief Defense Counsel claims that seven gigabytes of information was never restored. AE 155A, at 7. The Chief Defense Counsel has not specified what files were lost, nor did she specify which Defense teams within her office lost information. In their filing, the five defense teams in this case did not indicate how, or to what extent, the remaining seven gigabytes pertained to this Military Commission or the scheduled hearings.

On 17 April 2013, this Commission denied the Defense request for abatement in these proceedings. *See* AE 155D. However, the Commission granted the Defense request for a continuance until 17 June 2013. *See* AE 155D; AE 155F. Later that day, the Commission denied a Prosecution motion to reconsider the previous order. *See* AE 155F.

On 2 May 2013, recognizing that AE 155 was resolved by the Commission, counsel for Mr. bin ‘Attash, in a supplement to a scheduling order, stated that counsel “intends to seek reconsideration of the relief sought in AE 155A.” *See* AE 155H (WBA), at 2. To date, counsel has not sought “reconsideration of the relief sought in AE 155A.”

On 15 May 2013, this Commission issued its Docketing Order for the June session. *See* AE 159. The Docketing Order did not include AE 148, AE 155, or AE 155I.

On 16 May 2013, the Prosecution filed AE 155I, requesting, in part, that this Commission order the Defense by 31 May 2013 to address, in writing, specific lost Defense files that would

impact the Defense's ability to proceed on any of the 23 motions docketed for the week of 17 June 2003.

On 30 May 2013, counsel for Mr. bin Attash filed AE 159A, "Mr. bin 'Attash's Response to Docketing Order for 17-21 June Motion Hearings." In its proposed amended docketing order, counsel for Mr. bin 'Attash did not request that AE 148, AE 155A, or AE 155I be argued during the June session.

On 30 May 2013, counsel for Mr. bin 'Attash responded to AE 155I, sharing the preference of the Prosecution that this Commission rule on AE 155I "based on the pleadings alone." AE 155L, at 13.

On 3 June 2013, counsel for Mr. bin 'Attash requested the production of witnesses relating to the IT issue. *See* AE 173 (WBA), Attachment B. On 10 June 2013, the Prosecution responded to the Defense request. *See* AE 173 (WBA), Attachment C.

On 11 June 2013, a prosecutor in another case addressed ongoing solutions to defense concerns over IT issues. The prosecutor noted that all parties, including the Chief Defense Counsel, are working to among other items; establish separate e-mail systems by 22 July 2013, implementation of a veritable stand-alone system as chosen by the Chief Defense Counsel, and administrative access is currently now set at the Chief Defense Counsel level. *See* Unofficial/Unauthenticated Transcript, *United States v. Nashiri*, at 1813-1817.

On 12 June 2013, Mr. Bryan Broyles, Principal Deputy Chief Defense Counsel, testified in another case on the IT issue as raised in the instant case. In his testimony, Mr. Broyles confirmed that his office was working with various entities within the Government to resolve the concerns. *See* Unofficial/Unauthenticated Transcript, *United States v. Nashiri*, at 2013-2085.

Between 17-21 June 2013, a scheduled session of this Commission took place. Counsel for the Accused did not request any sort of relief based on IT issues, nor did IT issues become part of the June docket or any subsequent dockets.

On 19 June 2013, the Defense filed the instant motion to compel discovery.

6. Law and Argument

The instant motion seeks the production of all records and identities “regarding any intrusion” into electronic or physical spaces. AE 177 (WBA), at 1. The Defense defines “intrusion” as “accessing electronic spaces where information is stored, and/or retrieving, browsing, observing, identifying, examining, or archiving electronic information contained there.” AE 177 (WBA), Attachment G. Even under that broad definition, there has been no “intrusion” into Defense spaces. No unauthorized person has accessed Defense information in this case. Nobody has browsed Defense work product. No one identified or examined privileged material apart from the very limited inadvertent instance described in AE 154 and its attachment. The Prosecution does not have access to any archived Defense information. Put plainly, there is no “intrusion.”

The Military Commissions Act of 2009 (M.C.A.) affords the defense a reasonable opportunity to obtain evidence through a process similar 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. *See* R.M.C. 701; *see also* 10 U.S.C. § 949(j)(a). However, 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 where “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, 107-08 (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 107-08. 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 their 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).

In this instance, the Defense continues to demand information that does not exist. As such, logic dictates that if information does not exist, then in this scenario it cannot possibly be material or helpful to the preparation of the defense. However, counsel appears to double down on its position by making incorrect and/or conflated statements and depicting them as fact.

First, the Defense incorrectly asserts that the Office of the Chief Prosecutor (OCP) conducted “3-4 other possible intrusions” in the form of Investigative Search Requests (ISR). AE 177 (WBA), at 9. This assertion is derived from an individual who merely “believes” he conducted such searches, but is specifically not the record keeper. *See AE 177 (WBA)*, at 6. Instead of consulting with the ISR record keeper, the Defense instead again attacks the Prosecution for “fail[ure] to use due diligence to provide any discovery regarding the intrusion into OCDC emails...” AE 177 (WBA), at 9. In response to this baseless accusation, the Prosecution consulted with the actual record keeper at EITSD. She confirmed that between January 2011 and the present, EITSD received one ISR request from OCP, but the request was

canceled prior to implementation.¹ There is nothing more the Prosecution can provide on this topic because in this instance, the Prosecution has indeed proven the negative.

Second, the Defense is conflating what appears to be a now-resolved “residual error” from 2009 into another baseless allegation of “intrusion.” *See* AE 177 (WBA), at 2-4, 9. In this instance, the Defense position that the “residual error” is somehow tantamount to “intrusion” is based on innocuous statements attributed to an IT professional who neither witnessed nor suggests that any government entity or prosecutor accessed privileged material. The fact again remains that no “intrusion” or monitoring of Defense material has taken place, and the Defense motion does not provide any semblance of evidence pointing to the contrary. Regardless, the concerns expressed on this particular issue have been rendered moot.

All parties, including the Chief Defense Counsel, are working to establish separate e-mail systems, conduct a comparison between the pre and post-replication to determine what files may have been lost (and to locate such files if necessary), and implementing a veritable stand-alone system as chosen by the Chief Defense Counsel. Moreover, administrative access is currently now set at the Chief Defense Counsel level to ensure that such issues do not reoccur. These IT issues are being addressed in a significant and collaborative manner. But for past issues, there is nothing more that can be provided in discovery that will be material or helpful to the preparation of the defense, particularly since no “intrusion” took place.

Finally, the Defense is requesting that this Commission compel the production of all JTF-GTMO orders, directives, “JQRs” and SOPs “governing the search and seizure of attorney-client communications...” AE 177 (WBA), at 8. The Prosecution has already agreed to produce four SOPs to the Defense. *See* AE 177 (WBA), Attachment H. Furthermore, the Prosecution has provided the Defense unprecedented, expedited access to witnesses and facilities as part of its investigation in AE 133. The Prosecution provided a detailed declaration from Mr. Maurice

¹ EITSD confirms that an additional ISR was submitted by Ms. Teresa Woodard of OMC as a result of a court order from the Court of Military Commissions Review (C.M.C.R.). Details of that ISR were produced to the Defense and this Commission in AE 154 and its attachment.

Elkins on the audio-visual technology in the court-room and the holding cells; a detailed declaration from COL John Bogdan on the audio-visual technology in the Echo II facility where the Accused meet their counsel; a detailed declaration from [REDACTED] on the “For the Record Gold” Courtroom Reporter Software; and a detailed declaration from CAPT Eric Schneider, the Director of the J-2, on the fact that JTF GTMO does not collect any intelligence whatsoever in Echo II on Attorney-Client Meetings. The Prosecution made all of these individuals available for defense interviews, and two of them testified extensively regarding their knowledge of the audio-visual capabilities.

The Prosecution also provided schematics of the court-room, photos of the audio and visual devices in Echo II, an inspection of the Echo II audio-visual control-room, an opportunity to listen to the Defense and Accused channels that were recorded for FTR Gold, emails between CAPT Thomas Welsh and COL Bogdan on audio capabilities in ECHO II, and emails CAPT Welsh found in his archives from predecessors regarding² attorney-client meetings. Every agency the Prosecution has asked has specifically denied that any such claimed “intrusions” as defined by the Defense are occurring, or have occurred, since counsel have represented the Accused.

7. Conclusion

The Prosecution has been exceptionally forthcoming with regard to IT issues. The reality is that collaborative measures are currently underway to help alleviate any lingering defense concerns. In the meantime, additional safeguards have been implemented to avoid any further inadvertent disclosures of attorney-client privileged information. However, at no point has there been any sort of “intrusion” as defined by the Defense. The Prosecution should not be compelled to once again prove a negative. No such discovery exists.

² Any documents that were responsive to this request indicated, either explicitly or by implication that no such audio-monitoring was occurring.

ATTACHMENT A

CERTIFICATE OF SERVICE

I certify that on the 9th day of July 2013, I filed AE 177A, the **Government Response To Defense Motion to Compel Production of Discovery of Information Related to Government Intrusion Into Electronic or Physical Spaces Containing Defense-Related and/or Defense-Produced Materials with the Office of Military Commissions Trial Judiciary** and I served a copy on counsel of record.

//s//

Michael J. Lebowitz
Captain, JA, USA
Trial Counsel
of the Chief Prosecutor
Office of Military Commissions

Assistant
Office
Off