

UNCLASSIFIED//FOR PUBLIC RELEASE
MILITARY COMMISSIONS TRIAL JUDICIARY
GUANTANAMO BAY

UNITED STATES OF AMERICA

v.

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

AE 356C(AAA)

Defense Reply
To Government Response
To Mr. al Baluchi's Motion to Compel
Production of Discovery Regarding Revocation
of Access to Classified Networks

4 May 2015

1. **Timeliness:** This reply is timely filed per AE356-2(RUL).

2. **Additional facts:**

a. On 20 August 2013, in open court, counsel for Mr. al Baluchi introduced AE013SS(AAA) to show that then-Assistant Trial Counsel Joanna Baltes had deleted an email containing the signed Memoranda of Understanding without reading it:

Your message

To: Baltes, Joanna CIV OSD OMC Prosecution
Subject: Signed MoUs
Sent: Tuesday, February 19, 2013 4:17:03 PM (UTC-05:00) Eastern Time (US & Canada)

was deleted without being read on Friday, August 02, 2013 7:57:08 PM (UTC-05:00) Eastern Time (US & Canada).

b. The same day, the government defended against the implication of AE013SS by explaining that the government had access to a dual information technology system:¹

ATC [LT KORCZYNSKI]: Your Honor, just briefly so we can clear up the facts on the ground. We receive two copies of every e-mail that comes in because of the different systems we work off of, so -- to assure the court that we maintain accountability through a couple of different e-mail addresses. So if one is deleted from one server, we maintain it through another, so we are aware of signed MOUs and we maintain accountability for them. Thank you, sir.

¹ Unofficial Transcript of 20 August 2013 at 4386.

provided to the defense. The SECDEF removed the access in a way that left access channels for the prosecution and Convening Authority. Relevant players concealed the affiliation of the former CIA interpreter utilized by defense teams in open source materials. The defense could not vet the former CIA interpreter utilized by defense teams using classified networks because they no longer had access. After the former CIA interpreter was utilized by Mr. bin al Shihb's team at a military commissions hearing, the prosecution accused the defense in public statements and a written motion of failing to properly vet the former CIA interpreter, a situation they had created by working to remove defense access to classified networks. Thus, in this scenario, the prosecution is exploiting its prior success in removing defense access to classified networks both by the "accident" of a former CIA interpreter appearing on a defense team and the failure of the defense to properly vet offered interpreters.

The scenario is admittedly not the only explanation of events. Without discovery, Mr. al Baluchi cannot prove the involvement of the prosecution in the revocation of defense access to classified networks. But the failure of the prosecution to deny Mr. al Baluchi's suggestion of its involvement,⁵ pled on information and belief, speaks volumes. In contrast to the government's absolute and italicized denial of placing the former CIA interpreter to gather information regarding defense activities,⁶ the government says nothing whatsoever about whether it was involved in the plan to revoke defense access to classified networks. Nor does the prosecution

⁵ "On information and belief, a member of the Office of the Chief Prosecutor (OCP) reported Mr. Connell's acknowledgement of access to SIPRNet and JWICS to the Office of the Director of National Intelligence." AE356 Motion to Compel Production of Discovery Regarding Revocation of Access to Classified Networks at 2. "Counsel for Mr. al Baluchi have reason to suspect that a member of OCP advocated for revocation of defense access to classified networks." *Id.* at 4.

⁶ See AE350B at 2 ("The Prosecution states affirmatively that the presence of a former CIA linguist on one of the defense teams is *absolutely* not due to any action by any agency of the Executive branch to gather any information regarding defense activities from any of the defense teams.").

deny that it and the Convening Authority still have access to classified networks through other channels.

The government's response argues that the defense does not have an absolute right to access to classified networks. This point is accurate, but misses the essence of what has apparently happened. If the defense sought access to classified networks it had never had, the defense would have to put forward an especially compelling case for access. Here, the Convening Authority provided access, but the SECDEF revoked it after referral. The inequity is not a failure to provide access, but rather a revocation of pre-existing access provided by the Convening Authority.

Despite the prosecution's efforts to cast access to classified networks as a discovery issue, the SECDEF's decision to revoke access to classified information has only a tenuous connection to discovery rules. The use of classified networks to vet potential defense experts inherently cannot be a discovery matter, because the prosecution is simply not involved. As an example, the defense sought an expert consultant to carry out certain defense activities.

[REDACTED]

[REDACTED]⁷ [REDACTED]

[REDACTED]⁸ and the defense is now in a position of uncertainty regarding future communications with the expert consultant. The discovery rules have nothing to say about this situation, as the defense cannot request and the government cannot provide discovery about *ex parte* expert consultants.

⁷ See AE282 Defense *Ex Parte* Under Seal Motion to Compel Convening Authority to Provide Expert Assistance; AE339 Defense *Ex Parte* Under Seal Motion to Compel Convening Authority to Provide Expert Assistance.

⁸ See AE282E/339E *Ex Parte* Under Seal Order.

The prosecution's need-to-know argument⁹ fails when compared to the actual language of the 18 July 2013 memorandum. The memorandum makes a general observation that the majority of personnel in OMC offices do not need to know information on classified networks.¹⁰ The SECDEF memorandum does not, however, determine whether any given individual has a need to know any particular classified information. In fact, one of the specific elements of Mr. al Baluchi's discovery request is information about any intelligence community determinations of defense personnel need-to-know. As far as defense counsel can determine, no person has ever determined their need to know classified information about the potential experts they interact with, the linguists to whom they confide attorney-client communications, or the other

⁹ Strangely, the government claims that, "Defense counsel for Mr. Ali [has] 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." AE356B at 5 (citing Transcript of 17 October 2012 at 769). This claim is not accurate, either in its substance or its attribution. As Mr. Connell explained in the argument the government cites, any authorized holder of classified information, not just an OCA, may make a need-to-know determination:

DC [MR. CONNELL]: It is -- the phrase "authorized holder" in the executive order is a term of art. That authorized holder is any person who is authorized to have access to particular classified information. For example, an authorized holder is allowed to make a need-to-know determination. An authorized holder of classified information has certain duties. So it is not simply the originating agency, if that's the distinction that the court is drawing, it is any authorized holder of classified information.

Transcript of 17 October 2012 at 725; *see also* Executive Order 13526, *Classified National Security Information*, 75 Fed. Reg. 707 (Jan. 5, 2010) § 6.1(dd); Department of Defense Manual No. 5200.01-V3, *DoD Information Security Program: Protection of Classified Information* Enclosure 2 § 4 (Change 1 Mar. 21, 2012).

¹⁰ AE356 Attachment B.

information routinely available on classified networks. Of course, discovery could show otherwise, but the prosecution has never even responded to Mr. al Baluchi's discovery request, much less addressed the existence of responsive discovery.

The law of discovery in this military commission requires that government to produce information when it is material to the preparation of the defense. The defense has a more-than-colorable claim of SECDEF unlawful influence, possibly with prosecution involvement, and a right to access to the facts to establish that claim before the military commission. The military commission should order the discovery requested in DR-083-AAA.¹¹

3. **Attachments:**

A. Certificate of Service

B. Summary for ptf.gov

Very respectfully,

//s//

JAMES G. CONNELL, III
Learned Counsel

Counsel for Mr. al Baluchi

//s//

STERLING R. THOMAS
Lt Col, USAF
Defense Counsel

¹¹ AE356 Attachment C.

Attachment A

CERTIFICATE OF SERVICE

I certify that on the 4th day of May, 2015, I electronically filed the foregoing document with the Clerk of the Court and served the foregoing on all counsel of record by email.

//s//

JAMES G. CONNELL, III

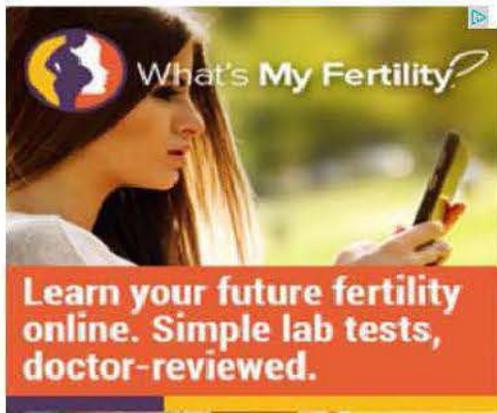
Learned Counsel

Attachment B

TCPIPUTILS.com [Members](#) [Premium](#) [Research](#) [Network Tools](#) [Email & DNS Tools](#) [SEO Tools](#) [Other sites](#)

Your ip: 134.152.252.249 (/browse/ip-address/134.152.252.249) (Provider DoD Network Information Center (/browse/as/6039)) - Arlington, Virginia, United States (US) 

Advertisements



[Home \(/\)](#) -> [browse domain \(/browse/domain\)](#) -> [gov \(/browse/domain/gov\)](#) -> ptf.gov

Summary for ptf.gov

Domain ptf.gov is **not** listed in the top million list of Alexa. ptf.gov is **not** listed in the top million list of Quantcast. It is **not** listed in the DMOZ directory. This domain is hosted by **Tinet SpA** (AS3257). The first DNS server is **a16-67.akam.net**. The current IPv4 address is **77.67.27.25**. The mail server with the highest priority is **mail1.cia.gov**.

Domain name information

Domain name	ptf.gov
Domain suffix	gov
Top-level domain (TLD)	gov (/browse/domain/gov)

Ranking

Current ranking Alexa	not in top million
Highest ranking Alexa	never ranked
Current ranking Quantcast	not in top million
Highest ranking Quantcast	never ranked
Google PageRank	6

DMOZ open directory

Domain in directory	No, domain not in open directory
---------------------	----------------------------------

WOT Reputation

Trustworthiness	Excellent (91/100)
Child safety	Excellent (92/100)

Advertisements

IT Service Desk Software

Prioritize & Manage Your Work Load. Learn How with a Free Trial Now!



Network information

DNS server (NS records)	a16-67.akam.net (23.211.132.67 (/browse/ip-address/23.211.132.67)) a3-64.akam.net (96.7.49.64 (/browse/ip-address/96.7.49.64)) a22-66.akam.net (23.211.61.66 (/browse/ip-address/23.211.61.66)) a1-22.akam.net (193.108.91.22 (/browse/ip-address/193.108.91.22)) a13-65.akam.net (2.22.230.65 (/browse/ip-address/2.22.230.65)) a12-65.akam.net (184.26.160.65 (/browse/ip-address/184.26.160.65))
Mail server (MX records)	mail1.cia.gov (198.81.129.68 (/browse/ip-address/198.81.129.68)) mail2.cia.gov (198.81.129.148 (/browse/ip-address/198.81.129.148))
IP address (IPv4)	77.67.27.25 (/browse/ip-address/77.67.27.25) 77.67.27.34 (/browse/ip-address/77.67.27.34)
IP address (IPv6)	2a01:4a0:1338:28::c38a:ff20 (/browse/ipv6-address/2a01:4a0:1338:28::c38a:ff20) 2a01:4a0:1338:28::c38a:ff2a (/browse/ipv6-address/2a01:4a0:1338:28::c38a:ff2a)
ASN number	3257 (/browse/as/3257)
ASN name (ISP)	Tinet SpA
IP-range/subnet	77.67.0.0/17 (/browse/ip-address/77.67.0.0-77.67.127.255) 77.67.0.0 - 77.67.127.255
Network tools (IPv4)	<input type="button" value="Ping 77.67.27.25"/> <input type="button" value="Traceroute 77.67.27.25"/>
Network tools (IPv6)	<input type="button" value="Ping 2a01:4a0:1338:28::c38a:ff20"/> <input type="button" value="Traceroute 2a01:4a0:1338:28::c38a:ff20"/>
Other tools	<input type="button" value="Testing info@ptf.gov"/>

[Login and create an alert for this domain. \(/members/alerts\)](#)

Alerts are fired when the IP, MX or NS records are changed and sent by email.

Network History

Number of IP history records	7
Number of DNS history records	4
Number of MX history records	0

[Premium \(/premium-access\)](#) members can view all details [here \(/ip-dns-history\)](#).

Sender Policy Framework (SPF)

No SPF records found.

Whois information

```
% DOTGOV WHOIS Server ready
Domain Name: PTF.GOV
Status: ACTIVE

>>> Last update of whois database: 2015-04-14T23:54:16Z <<<
Please be advised that this whois server only contains information pertaining
to the .GOV domain. For information for other domains please use the whois
server at RS.INTERNIC.NET.
```

Last updated on 2015-04-15

Update information

The information on this page is collected from many different sources on the internet. Below is the last update date given from each source.

Alexa and Quantcast ranking	2015-04-26
AS number information	2015-04-26
DMOZ open directory	2015-04-26
Network information	Realtime
PageRank	2015-01-10
WOT Reputation Scorecard	2015-04-07

[Contact Us \(/support\)](#) | [Privacy Policy \(/privacy-policy\)](#) | [Terms of Service \(/terms-of-service\)](#) | © 2015 webdevmedia