UNITED STATES OF AMERICA v. KHALID SHEIKH MOHAMMAD, WALID MUHAMMAD SALIH MUBARAK BIN 'ATTASH, RAMZI BIN AL SHIBH, ALI ABDUL-AZIZ ALI, MUSTAFA AHMED ADAM AL HAWSAWI	**AE356(AAA)** **Mr. al Baluchi's Motion to Compel** Production of Discovery Regarding Revocation of Access to Classified Networks 6 April 2015 *Amendment*[*] 7 August 2015

1. Timeliness: This motion is timely filed.

2. Relief Sought: Mr. al Baluchi respectfully requests 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.

3. Overview: On 18 July 2013, the Secretary of Defense issued a memorandum revoking browser access to the classified networks SIPRNet and JWICS based on concerns over defense access to these systems. Mr. al Baluchi immediately requested discovery regarding this decision, but the prosecution has not responded beyond acknowledging receipt of the request. The military commission should order the government to provide responsive discovery, as it is material to the preparation of the defense with respect to potential unlawful influence.

4. Burden and Standard of Proof: The burden of persuasion on this motion to compel discovery rests with the defense.

[*] Mr. al Baluchi's changes abandon his arguments relating to the use of classified systems to vet experts. Per Trial Judiciary instruction, the following description refers to the original version of this motion. In ¶ 3, ¶ 5(d), and the first, fourth, and fifth paragraphs of ¶ 6, Mr. al Baluchi modified the language to make clear that the SECDEF's action was the issuance of a memorandum. In ¶ 3, ¶ 5(d), and the first and seventh paragraphs of ¶ 6, Mr. al Baluchi deleted and modified language to eliminate references to the former CIA interpreter who is the subject of AE350 and equality of arms. Mr. al Baluchi deleted the sixth, ninth, and tenth paragraphs of ¶ 6 relating to vetting of experts and equality of arms. Mr. al Baluchi combined the seventh and eighth paragraphs of ¶ 6 and eliminated the topic sentence of the eighth paragraph.

5. Facts:

a. On 16 October 2012, Mr. James Connell argued in open court that the defense required classification guidance because, among other reasons, they hold ordinary SIPRNet and JWICS accounts which bring them into contact with classified information.[1]

b. On information and belief, a member of the Office of the Chief Prosecutor (OCP) reported Mr. Connell's acknowledgment of access to SIPRNet and JWICS to the Office of the Director of National Intelligence.

c. ~~(U//FOUO)~~ In 2013, the Office of the Director of National Intelligence "expressed concern" that defense counsel in this case have access to classified information through SIPRNet and JWICS accounts.[2]

d. ~~(U//FOUO)~~ On 18 July 2013, Secretary of Defense (SECDEF) Chuck Hagel issued a memorandum disabling Office of the Chief Defense Counsel browser access to SIPRNet and JWICS.[3] The memorandum delegated authority to the director of WHS to approve restoration of JWICS and SIPRNET access on a case-by-case basis.

e. On 25 July 2013, Mr. al Baluchi's defense team requested discovery from the prosecution regarding the SECDEF's decision to revoke defense access to SIPRNet and JWICS.[4] The government has not responded to this discovery request beyond acknowledging its receipt.

f. On 8 November 2013, defense counsel for Mr. al Baluchi requested access to specific sites on the JWICS and SIPRNet, with the specific justification that access would benefit the Defense Security Officer (DSO) in advising the defense team on protection of classified

[1] Unofficial/Unauthenticated Transcript of 16 October 2012 at 573-574.
[2] Attachment B, Memorandum from the Secretary of Defense to Director, Washington Headquarters Services et al, subject: Office of the Military Commissions Access to Classified Intelligence Information through Standard Web Browsers Available on the Joint Worldwide Intelligence Communications Systems and Secret Internet Protocol Router Network (18 July 2013).
[3] *Id.*
[4] Attachment C, DR-083-AAA (25 July 2013).

information, including classification decisions and determinations, historical classification justifications, and current guidance.[5]

g. In a pair of memoranda dated 13 December 2013 and 20 December 2013, WHS rejected the defense request for an exception to policy to allow for reactivation of JWICS and SIPRNet access.[6]

6. Law and Argument

~~(U)~~ In July 2013, the SECDEF issued a memorandum revoking browser access to classified networks for all Office of Military Commissions (OMC) personnel. Although facially equal, this revocation targeted defense litigation capabilities because the Office of the Chief Prosecutor (OCP) has access to classified information outside OMC information technology channels. The military commission should order the government to produce discovery on this issue.

~~(U//FOUO)~~ The 18 July 2013 SECDEF memorandum makes clear that the SECDEF's decision to revoke browser access to SIPRNet and JWICS was aimed at the defense. According to the SECDEF, "The Office of the Director of National Intelligence (ODNI) has expressed concern that defense counsel assigned to represent Guantanamo detainees in military commission cases have access to classified intelligence information outside of the established discovery process through web browsers resident on the Joint Worldwide Intelligence Communications System (JWICS) and the Secret Internet Protocol Router Network

[5] Memorandum from Defense Counsel for Mr. al Baluchi, OMC, to Director, WHS, Subject: Request for access to SIPRNet browser capability (8 November 2013) (Attachment D).
[6] Attachment E, Memorandum from Director, WHS to Defense Counsel, OMC (Attn: Lt Col Sterling Thomas), subject: Requests to Restore Access to Joint Worldwide Intelligence Communications System Browser Capability (13 December 2013); Attachment F, Memorandum from Director, WHS to Defense Counsel, OMC (Attn: Lt Col Sterling Thomas), subject: Request to Restore Access to Secret Internet Protocol Router Network (SIPRNet) Browser Capability (20 December 2013).

(SIPRNet)."[7] Neither the ODNI nor SECDEF expressed any concerns about access to classified networks by OCP.

~~(U//FOUO)~~ More insidiously, the SECDEF memorandum makes clear that the SECDEF revoked browser access to classified networks based on litigation concerns. The SECDEF wrote that the Military Commissions Act (MCA), Manual for Military Commissions (MMC), and a 21 August 2008 memorandum[8] "mandate that defense counsel obtain classified information only from the Office of the Chief Prosecutor."[9] Defense counsel access to classified information outside the discovery process, for example through the use of the JWICS and the SIPRNet web browsers, circumvents these established procedures."[10] This argument finds no actual support in the cited authorities: nothing in the MCA or the MMC prohibits defense access to classified networks. But the SECDEF's expressed misunderstanding of the MCA and MMC demonstrates that he acted with a government litigation advantage in mind.

Counsel for Mr. al Baluchi have reason to suspect that a member of OCP advocated for revocation of defense access to classified networks. On 16 October 2012, Mr. James Connell argued in open court that the defense required classification guidance because, among other reasons, defense counsel hold ordinary SIPRNet and JWICS accounts which bring them into contact with classified information.[11] Following this argument, a member of OCP repeatedly expressed off the record the view that defense counsel's access to classified networks was irregular. For more than five years prior to this statement in open court, personnel at the Office of Chief Defense Counsel had access to classified networks. Nine months later, SECDEF issued

[7] Attachment B at 1.
[8] Attachment G, Memorandum from Deputy Secretary of Defense, subject: Release of DoD Records to the Office of Military Commissions (21 August 2008).
[9] Attachment B at 1.
[10] *Id.*
[11] Unofficial/Unauthenticated Transcript of 16 October 2012 at 573-574.

the memorandum revoking browser access to SIPRNet and JWICS, citing concerns about defense counsel.

Although facially neutral, the memorandum revoking access to classified networks through OMC targets the defense disproportionately. The prosecution, as part of the High Value Detainee Prosecution Task Force, has access to classified networks through its dual computer network. The prosecution also has many non-DOD team members, including Department of Justice and Federal Bureau of Investigation personnel, who have access to classified networks through non-DoD channels. Further, the 21 August 2008 memorandum makes clear that other components of the Department of Defense shall produce "all responsive Records that Trial Counsel requests."[12] Although hardly necessary, Washington Headquarters Services may have restored browser access to members of OCP; without discovery, there is no way for the defense to know.

Discovery regarding the revocation of SIPRNet and JWICS browser access is material to the preparation of the defense with respect to potential unlawful influence. Title 10 U.S.C. § 949b(a)(2) provides that, "No person may attempt to coerce or, by any unauthorized means, influence . . . (C) the exercise of professional judgment by trial counsel or defense counsel." "While statutory in form, the prohibition can also raise due process concerns, where for example unlawful influence undermines a defendant's right to a fair trial or the opportunity to put on a defense."[13] The 18 July 2013 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.

7. <u>Request for Oral Argument</u>: The defense requests oral argument.

[12] Attachment G at 1.
[13] *United States v. Salyer*, 72 M.J. 415, 423 (C.A.A.F. 2003).

8. Certificate of Conference: The government opposes this motion.

9. Attachments:

A. Certificate of Service.

B. Memorandum from the Secretary of Defense to Director, Washington Headquarters Services et al, subject: Office of the Military Commissions Access to Classified Intelligence Information through Standard Web Browsers Available on the Joint Worldwide Intelligence Communications Systems and Secret Internet Protocol Router Network (18 July 2013).

C. DR-083-AAA (25 July 2013).

D. Memorandum from Defense Counsel for Mr. al Baluchi, OMC, to Director, WHS, Subject: Request for access to SIPRNet browser capability (8 November 2013).

E. Memorandum from Director, WHS to Defense Counsel, OMC (Attn: Lt Col Sterling Thomas), subject: Requests to Restore Access to Joint Worldwide Intelligence Communications System Browser Capability (13 December 2013).

F. Memorandum from Director, WHS to Defense Counsel, OMC (Attn: Lt Col Sterling Thomas), subject: Request to Restore Access to Secret Internet Protocol Router Network (SIPRNet) Browser Capability (20 December 2013).

G. Memorandum from Deputy Secretary of Defense, subject: Release of DoD Records to the Office of Military Commissions (21 August 2008).

Very respectfully,

//s//
JAMES G. CONNELL, III
Detailed Defense Counsel

//s//
STERLING R. THOMAS
Lt Col, USAF
Detailed Military Counsel

Counsel for Mr. al Baluchi

Attachment A

CERTIFICATE OF SERVICE

I certify that on the 7th day of August, 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

[redacted]

SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

JUL 18 2013

MEMORANDUM FOR DIRECTOR, WASHINGTON HEADQUARTERS SERVICES

SUBJECT: [redacted] Office of the Military Commissions Access to Classified Intelligence Information through Standard Web Browsers Available on the Joint Worldwide Intelligence Communications Systems and Secret Internet Protocol Router Network

[redacted] Access to classified information by the Office of the Military Commissions (OMC) must be consistent with law and policy. OMC includes the Office of the Convening Authority, the Office of Chief Prosecutor, the Office of the Chief Defense Counsel, the Military Commissions Trial Judiciary, and the U.S. Court of Military Commission Review.

[redacted] The Office of the Director of National Intelligence (ODNI) has expressed concern that defense counsel assigned to represent Guantanamo detainees in military commission cases have access to classified intelligence information outside of the established discovery process through web browsers resident on the Joint Worldwide Intelligence Communications System (JWICS) and the Secret Internet Protocol Router Network (SIPRNet). The ODNI is concerned that uncontrolled access to this information outside of the normal discovery process presents a risk of compromising intelligence sources and methods.

[redacted] The Military Commissions Act of 2009, Manual for Military Commissions, and the Deputy Secretary of Defense memorandum, "Release of DoD Records to the Office of Military Commissions," dated August 21, 2008, prescribe procedures for defense counsel access to classified information to support the discovery process in military commission cases. These discovery procedures were created to safeguard intelligence sources and methods while ensuring compliance with discovery obligations required by law. These procedures mandate that defense counsel obtain classified information only from the Office of the Chief Prosecutor. Defense counsel access to classified information outside the discovery process, for example through the use of the JWICS and the SIPRNet web browsers, circumvents these established procedures.

[redacted] In addition, section 4.1 of Executive Order 13526 prescribes that access to classified information is based on a need-to-know. The remainder of OMC personnel for whom discovery procedures do not apply should have access to classified information only upon meeting this standard. The majority of personnel working in OMC offices do not have the requisite "need-to-know" with respect to the information resident on JWICS and SIPRNet. Therefore, their web browser access should be disabled for this reason. This action will be subject to case-by-case exceptions when a need to have such access is demonstrated in writing.

[redacted] To ensure compliance with law and policy, I direct that:

- [redacted] The Director, Washington Headquarters Services (WHS), disable all JWICS and SIPR browsing capability, excepting Sharepoint and browser functionality that is required to access vaulted e-mails or required for file sharing

[redacted]

OSD071009-13

capabilities, for all OMC personnel not approved for access per the individual justification process detailed below.

- ~~(U//FOUO)~~ The implementation of this action must not impede OMC personnel from continued use of DoD classified information systems to process classified information for which they have appropriate lawful access either through the discovery or other processes established to facilitate the commissions litigation. In addition, this action must not disrupt the day-to-day work of OMC efforts to properly process and share classified information.

- ~~(U//FOUO)~~ This action shall be implemented in a manner that does not compromise or delete any information already in the lawful possession of any defense counsel and does not compromise any information protected by an attorney-client privilege.

- ~~(U//FOUO)~~ These restrictions must be implemented not later than five business days from the date of receipt of this memorandum.

- ~~(U//FOUO)~~ The Director, WHS, shall assign an information technology (IT) specialist from his staff to coordinate with the Office of the Chief Defense Counsel to ensure this action is implemented in the manner described above. This specialist shall assist the Office of the Chief Defense Counsel in identifying any unintended or unexpected IT problems. The IT specialist shall communicate only with the Office of the Director, WHS, and shall not communicate any defense information learned from this assignment to the Office of the Chief Prosecutor, the Office of the Convening Authority, or to any other person subject to the limited exception in the following sentence. Communication with the Office of the Director, WHS, regarding any defense information learned from this assignment shall occur only to remedy an identified problem and only when the Chief Defense Counsel is notified.

- ~~(U//FOUO)~~ If the Director, WHS, becomes aware that this implementation results in defense counsel being denied access to any critical applications, to include SharePoint or other databases that defense counsel has created to facilitate their Military Commissions legal work, the Director shall notify the Secretary of Defense within forty-eight hours and provide a remedy in a timely manner.

~~(U)~~ The Director, WHS, is delegated the authority to approve access to JWICS and SIPRNet browser capability on an individualized basis for OMC individuals based on a written detailed need-to-know justification. This authority may not be further delegated and will be exercised in consultation with the Under Secretary of Defense for Policy, Under Secretary of Defense for Intelligence, and the DoD General Counsel.

~~(U)~~ These restrictions are intended to ensure that OMC access to classified information conforms with law and policy, that OMC members continue to use accredited DoD classified information systems, and that risks of compromise to intelligence sources and methods are minimized.

(U) The Office of the Under Secretary of Defense for Intelligence point of contact is Ms. Theresa Ramsey at [redacted] or Theresa.Ramsey[redacted]. The WHS point of contact is Ms. Stephanie Flannery at [redacted] or Stephanie.Flannery[redacted]

cc:
USD(P)
USD(I)
DoDGC
ASD PA

Attachment C

25 July 2013

MEMORANDUM FOR Trial Counsel

FROM: James G. Connell, III, Defense Counsel for Mr. al Baluchi

SUBJECT: DEFENSE REQUEST FOR DISCOVERY (**DR-083-AAA**)

Defendant, by and through undersigned counsel pursuant to RMC 701, the Due Process Clause of the Fifth Amendment, the Confrontation Clause to the Sixth Amendment, and the Compulsory Process Clause of the Sixth Amendment to the United States Constitution, hereby requests that the government produce the document(s) and information listed below.

In this request, "Office of Military Commissions" (OMC) is defined to include, among other entities, the Office of the Chief Prosecutor (OCP) and the Office of the Chief Defense Counsel (OCDC). "Intelligence Community" (IC) shall have the meaning stated in Executive Order 12333 *United States Intelligence Activities* § 3.5(h).

Please produce all documents and information in the possession of the United States containing or referencing communications within and/or between the Department of Defense (DOD) and members of the IC regarding OMC access to classified information on the Joint Worldwide Intelligence Communications System (JWICS) and the Secret Internet Protocol Router Network (SIPRNet) from May 2011 to the date of production. This request includes, but is not limited to, the following:

(1) All documents and information containing or referencing Office of the Director of National Intelligence (ODNI) concern that defense counsel assigned to represent Guantanamo detainees in military commissions cases have access to classified intelligence information;
(2) All documents and information containing or referencing any IC need-to-know determination regarding OCDC personnel;
(3) All documents and information containing or referencing any communication between OCP personnel and members of the IC regarding OMC access to JWICS and SIPRNet;
(4) All documents and information referencing or memorializing any meetings between OMC personnel and other DOD personnel regarding OMC access to JWICS and SIPRNet.

Thank you for your attention in this matter. If you have any questions about this request or would like to discuss further, please feel free to contact me.

Respectfully submitted,
//s//
James G. Connell, III
Defense Counsel for Mr. al Baluchi

Attachment D

~~Unclassified/For Official Use Only~~

8 November 2013

MEMORANDUM FOR Director, Washington Headquarters Services
THROUGH: Director, Special Security Office

FROM: Detailed defense counsel for Ali Abdul Aziz Ali, Office of the Chief Defense Counsel

SUBJECT: Request for access to SIPRNet browser capability

1. We respectfully request that Mr. [redacted] be granted access to SIPRNet browser capability. We are detailed defense counsel for Mr. Ali Abdul Aziz Ali, one of the defendants in the military commission case of *United States v. Khalid Sheikh Mohammed, et al.* Pursuant to Secretary Hagel's 18 July 2013 Memorandum, the authority of members of the Office of the Chief Defense Counsel (OCDC) to conduct investigation and research on SIPR and JWICS systems was disabled.

2. We noted our objection to this policy change and requested reconsideration in our 2 August 2013 memorandum to Secretary Hagel. We have continued to attempt to zealously represent Mr. Ali under these conditions; however we have been severely hampered in many ways. To alleviate some of the problems created by Secretary Hagel's 18 July 2013 memo we respectfully request that our trial team Defense Security Officer (DSO) Mr. [redacted] be granted SIPRNet browser access.

3. Mr. [redacted] has been unable to fully perform his court-ordered responsibility to advise his defense counsel/trial team on how to protect classified information and avoid classified spills without access to SIPRNet browser capability. Mr. [redacted] requires access to the sites below in order to properly perform his role as DSO:

Site: Director of National Intelligence (DNI)
URL: SIPRNet: [redacted]
Position: Defense Security Officer (DSO)
Specific Justification: As a DSO, Mr. [redacted] has a court-ordered responsibility to advise his defense counsel/team on how to properly protect classified information and avoid classified data spills. Mr. [redacted] needs access to the DNI website in order to properly research historical information security classification decisions and determinations made by the Original Classification Authorities (OCA), as well as keep abreast of the most current IC and DoD security classification policy guidance.

Site: Office of the Under Secretary of Defense for Intelligence (OUSDI)
URL: SIPRNet: [redacted]
Position: Defense Security Officer (DSO)
Specific Justification: As a DSO, Mr. [redacted] has a court-ordered responsibility to advise his defense counsel/team on how to protect classified information and avoid classified data spills. Mr. [redacted] needs access to the OUSD(I) website in order to properly research historical information security classification decisions and determinations made by the Original Classification Authorities (OCA), as well as keep abreast of the most current IC and DoD security classification policy guidance.

Site: INTELINK
URL: SIPRNet: [redacted]
Position: Defense Security Officer (DSO)

~~Unclassified/For Official Use Only~~

~~Unclassified/For Official Use Only~~

Specific Justification: As a DSO, Mr. [redacted] has a court-ordered responsibility to advise his defense counsel/team on how to protect classified information and avoid classified data spills. Mr. [redacted] needs access to the Intelink website in order to properly research historical information security classification decisions and determinations made by the Original Classification Authorities (OCA), as well as keep abreast of the most current IC and DoD security classification policy guidance.

Site: Defense Intelligence Agency (DIA)
URL: SIPRNet: [redacted]
Position: Defense Security Officer (DSO)
Specific Justification: As a DSO, Mr. [redacted] has a court-ordered responsibility to advise his defense counsel/team on how to protect classified information and avoid classified data spills. Mr. [redacted] needs access to the DIA website in order to properly research historical information security classification decisions and determinations made by the Original Classification Authorities (OCA), as well as keep abreast of the most current IC and DoD security classification policy guidance.

Site: United States Southern Command (USSOUTHCOM)
URL: SIPRNet: [redacted]
Position: Defense Security Officer (DSO)
Specific Justification: As a DSO, Mr. [redacted] has a court-ordered responsibility to advise his defense counsel/team on how to protect classified information and avoid classified data spills. Mr. [redacted] needs access to the SOUTHCOM website in order to properly research historical information security classification decisions and determinations made by the Original Classification Authorities (OCA), as well as keep abreast of the most current IC and DoD security classification policy guidance.

Site: Joint Task Force - Guantanamo (JTF GTMO)
URL: SIPRNet: [redacted]
Position: Defense Security Officer (DSO)
Specific Justification: As a DSO, Mr [redacted] has a court-ordered responsibility to advise his defense counsel/team on how to protect classified information and avoid classified data spills. Mr. [redacted] needs access to the JTF GTMO website in order to properly research historical information security classification decisions and determinations made by the Original Classification Authorities (OCA), as well as keep abreast of the most current IC and DoD security classification policy guidance.

Site: Department of Justice (DOJ)
URL: SIPRNet: [redacted]
Position: Defense Security Officer (DSO)
Specific Justification: As a DSO, Mr. [redacted] has a court-ordered responsibility to advise his defense counsel/team on how to protect classified information and avoid classified data spills. Mr. [redacted] needs access to the DOJ/FBI website in order to properly research historical information security classification decisions and determinations made by the Original Classification Authorities (OCA), as well as keep abreast of the most current IC and DoD security classification policy guidance.

4. Thank you for your prompt attention to this matter. Please contact me at [redacted] or sterling.thomas[redacted] if there are any questions.

~~Unclassified/For Official Use Only~~

Attachment E

[redacted]

DEPARTMENT OF DEFENSE
WASHINGTON HEADQUARTERS SERVICES
1155 DEFENSE PENTAGON
WASHINGTON, DC 20301-1155

DEC 1 8 2013

MEMORANDUM FOR DEFENSE COUNSEL, OFFICE OF MILITARY COMMISSIONS
(ATTN: LT COL STERLING R. THOMAS)

SUBJECT: [redacted] Requests to Restore Access to Joint Worldwide Intelligence Communications System Browser Capability

[redacted] As you know, the Secretary of Defense memorandum, dated July 18, 2013, subject: [redacted] Office of the Military Commissions Access Joint Worldwide Intelligence Communications System (JWICS) and Secret Internet Protocol Router Network (SIPRnet) Browser Capability, directed the Director, Washington Headquarters Services (WHS), to disable all JWICS and SIPRnet browser capability, except SharePoint and browser functionality that is required to access vaulted e-mails or for file sharing capabilities for all Office of the Military Commissions (OMC) personnel. The memorandum also delegated authority to the Director, WHS, to approve restoring JWICS and SIPRnet browser capability for OMC personnel based on a compelling need-to-know justification in writing.

[redacted] We have received your request for exception to policy, endorsed by Mr. James Connell III, for Mr. [redacted] Defense Security Officer. My staff, in consultation with Office of the Secretary of Defense stakeholders, has determined that the request does not establish the need-to-know requirement, which is required to grant access. Accordingly, I deny your request for an exception to policy.

[redacted] I understand that Mr. [redacted] has been provided specific protection and classification guidance from the original classification authorities and has a variety of other resources available, including the DoD OMC/Habeas Corpus classification guide and several other classification guides on unclassified web browsers. If these resources are insufficient to make appropriate classification determinations, Mr. [redacted] may also work with Ms. Stephanie Flannery, WHS/Office of Special Security, to assist with classification determinations.

[redacted] If you have any questions, please let me know. My point of contact for this action is Jason Boykin, (703) 697-1542, or Jason.O.Boykin.civ[redacted].

William E. Brazis, Jr.
Director

[redacted]

Attachment F

[redacted]

DEPARTMENT OF DEFENSE
WASHINGTON HEADQUARTERS SERVICES
1155 DEFENSE PENTAGON
WASHINGTON, DC 20301-1155

DEC 20 2013

MEMORANDUM FOR DEFENSE COUNSEL, OFFICE OF MILITARY COMMISSIONS
(ATTN: LT COL STERLING R. THOMAS)

SUBJECT: [redacted] Request to Restore Access to Secret Internet Protocol Router Network (SIPRNet) Browser Capability

[redacted] This memorandum cancels and reissues my memorandum of December 13, 2013, subject: [redacted] Request to Restore Access to Joint Worldwide Intelligence Communications System Browser Capability, in order to provide better clarity and accuracy.

[redacted] We have received your request for exception to policy, endorsed by Mr. James Connell III, for Mr. [redacted] Defense Security Officer.

[redacted] As you know, the Secretary of Defense memorandum, dated July 18, 2013, directed the Director, Washington Headquarters Services (WHS), to disable all access to Joint Worldwide Intelligence Communications Systems (JWICS) and SIPRNet browser capability, except SharePoint and browser functionality that is required to access vaulted e-mails or for file sharing capabilities for all Office of the Military Commissions (OMC) personnel. The memorandum also delegated authority to the Director, WHS, to approve restoring JWICS and SIPRNet browser capability for OMC personnel based on a compelling need-to-know justification in writing.

[redacted] My 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. Accordingly, I deny your request for an exception to policy.

[redacted] I understand that Mr. [redacted] has been provided specific classification guidance from original classification authorities and has a variety of other resources available, including the DoD OMC/Habeas Corpus classification guide and several other classification guides on unclassified web browsers. If Mr. [redacted] believes that these resources are insufficient, he may also request assistance from Ms. Stephanie Flannery and her staff, WHS/Office of Special Security.

[redacted] If you have any questions, please let me know. My point of contact for this action is Jason Boykin, (703) 697-1542, or Jason.O.Boykin.civ[redacted]

William E. Brazis
Director

[redacted]

Attachment G

[redacted]

DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

AUG 21 2008

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANT SECRETARIES OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Release of DoD Records to the Office of Military Commissions

In order to achieve the purpose of the Military Commissions Act of 2006, the Office of the Chief Prosecutor for the Office of Military Commissions (OMC-P) requires records held by Department of Defense (DoD) Components and Agencies ("Components"). These DoD records ("Records") include, any item, collection, file, database, or grouping of information, whatever the storage medium (paper, electronic, audio or video, etc.), whether such item is in a current, back up, or archived system. These Records are required so OMC-P Trial Counsel can thoroughly investigate and prepare cases involving specified detainees and meet discovery obligations under the law. It is DoD's policy that all Components shall assist in locating these Records, and either produce or otherwise make available (including by inspection) all responsive Records that Trial Counsel requests.

To assist in this search, Trial Counsel will submit a detailed and specific request in the form of a Prudential Search Request ("PSR"). The requested search will include all applicable Records held by or under the control of the DoD Component and will be completed within the time period indicated by the Executive Secretary (generally not less than 14 days). Copies of requested Records will be delivered to the Trial Counsel in the manner in which such Records are ordinarily maintained or will otherwise be made available to the Trial Counsel. International Committee of the Red Cross (ICRC) Records will be sought or produced only in consultation with the Under Secretary of Defense for Policy (USD(P)). Videotapes of interviews by officials from a detainee's home country will be accessible to the Trial Counsel, but may not be used unless approved by USD(P). Medical Records shall be requested and provided in accordance with the Assistant Secretary of Defense for Global Security Affairs directive of May 2, 2008.

[redacted]

OSD 10522-08

[redacted]

Trial Counsel will submit PSRs to the Department of Defense Office of the General Counsel (DoD OGC), which will route the request through the Executive Secretary for tasking to the appropriate DoD Component. The Executive Services Directorate will develop supplemental instructions and procedural guidelines, as needed, to assist with and standardize procedures to effect this policy within the Department of Defense. Preparation of such guidelines will not slow the execution of this policy directive, and such policy guidelines will be completed within 30 days of this policy directive.

Upon receipt of a PSR, a Component will conduct a complete and timely search of its Records and either produce or make available the requested Records as directed. Requested Records will be supplied directly to the Trial Counsel, provided the counsel has the appropriate security clearances. As appropriate, OMC-P will keep DoD OGC or other appropriate authority informed of the status of pending discovery requests.

Once Trial Counsel obtains or gains access to and reviews all requested Records, Trial Counsel will identify for the originator those Records the Trial Counsel seeks to provide to the defense in discovery or use as evidence at trial. Pursuant to the Military Commissions Act §§ 949d(f) and 949j(c), Trial Counsel shall protect classified or otherwise sensitive information (e.g., information protected by executive, attorney-client, or other recognized privilege) consistent with Military Commission Rules of Evidence 505 (Classified Information privilege) and 506 (Government Information privilege) and related authorities. Trial Counsel will work with the originator to protect the originator's equities in any Record (including seeking declassification or appropriate protective orders), while fulfilling Trial Counsel's obligations arising under the law.

If a dispute arises over the use of certain Records the Chief Prosecutor for OMC and the originating DoD Component (at the Flag Officer level) will endeavor to resolve the dispute. If they are unable to resolve the matter, it will be forwarded for adjudication to the Special Detainee Follow-up Group (SDFG), co-chaired by the DoD OGC, which will include representatives from OMC and, as necessary, the originating Component. If the SDFG is unable to resolve the issue, it will be forwarded to the Senior Oversight Group of the SDFG for resolution. This dispute resolution mechanism does not apply to the initial production of Records to Trial Counsel as discussed elsewhere in this policy directive.

The Defense Intelligence Agency (DIA) will incorporate a declassification review operation in support of OMC into its ongoing declassification efforts related to Habeas Proceedings, as outlined in DEPSECDEF Memorandum dated July 18, 2008. DIA will identify additional resource requirements to OMC who will provide funding. The Under Secretary of Defense for Intelligence will provide security policy and oversight support, and will work closely with the DNI, CIA, and FBI to facilitate community cooperation. Involved agencies will expedite the review process.

[redacted]

[redacted]

All disclosures to the defense of controlled unclassified or classified information shall be made through Trial Counsel and shall be subject to appropriate security clearance and handling requirements.

cc:
Executive Secretary

[redacted]