

CIA program in 2006, and many of the program's operational details remain classified at the TS/SCI level because their disclosure could be expected to cause extremely grave damage to the national security and normal criteria for access and handling of even Top Secret information are insufficient to protect against unauthorized disclosure of such matters.

Respondents also demonstrated that because petitioner's case involves TS/SCI information, the standard *habeas* protective order first adopted in 2004 and applicable in many other Guantanamo cases is patently inadequate for cases involving high value detainees because it contemplates issues associated with the handling of information classified at no higher than the Secret level. It also allows habeas counsel in Guantanamo detainee cases to share classified based on a presumptive "need to know," which is at odds with the extremely limited and tightly controlled access permitted for TS/SCI information. Respondents, therefore, urged the Court to adopt their proposed TS/SCI protective order, which incorporates much of the current protective order regime, but is appropriately tailored to address the management and handling of TS/SCI information. Entry of the proposed protective order, respondents further demonstrated, would give due deference to the Executive Branch's authority, vested by the Constitution, to control access to classified information in order to safeguard the compelling government interest in national security. *See Dep't of Navy v. Egan*, 484 U.S. 518, 527-30 (1988); *Haig v. Agee*, 453 U.S. 280, 307 (1981). It would also be consistent with the Supreme Court's recent admonition in *Boumediene v. Bush*, 128 S. Ct. 2229, 2276 (2008), that the "District court . . . use[s] its discretion to accommodate" the government's interest in protecting the sources and methods of intelligence gathering "to the greatest extent possible."

Petitioner's opposition does not rebut respondents' showings. As discussed below,

petitioner's strained reading of the standard *habeas* protective order as being sufficient to protect TS/SCI information is simply wrong. Moreover, many of petitioner's arguments rest on his speculation that he would not be able to effectively challenge the legality of his detention if his counsel cannot freely share TS/SCI information with counsel for other high-value detainees. Such speculation does not warrant adopting a protective order regime whereby counsel are presumed to have a "need to know" the classified information. Rather, in the unique circumstance of this case which involves exceptionally sensitive national security information, a regime of case-by-case determination for the sharing of TS/SCI information, as proposed by the respondents, is needed to protect against the unauthorized disclosure of such information.

ARGUMENT

I. THE STANDARD *HABEAS* PROTECTIVE ORDER IS NOT SUFFICIENT TO PROTECT PRESUMPTIVELY TS/SCI INFORMATION

Petitioner argues that the standard *habeas* protective order entered in 2004² is fully capable of protecting presumptively TS/SCI information because the protective order defines the terms "classified national security information and/or documents," "classified information," and "classified documents" to include TS/SCI information. *See* Ex. 4 to Respondents' Mot. to Reconsider, at ¶ 9. Petitioner also cites certain Court orders in 2005 in which the Court

² The standard *habeas* protective order encompasses the following: (1) the Amended Protective Order and Procedures for Counsel Access to Detainees at the United States Naval Base in Guantanamo Bay, Cuba, first issued on November 8, 2004, 344 F. Supp. 2d 174 (D.D.C. 2004); (2) the Order Addressing Designation Procedures for Protected Information, first issued on November 10, 2004; and (3) the Order Supplementing and Amending Filing Procedures Contained in the November 8, 2004, Amended Protective Order, first issued on December 13, 2004. The Court recently entered a revised protective order incorporating these prior orders with only slight modifications primarily to document filing procedures. *See* 08-cv-442, dkt. no. 409 (September 11, 2008).

referenced classified information without qualification, and specifically allowed counsel access to classified information involving intelligence sources, information collected from those sources, and intelligence methods or activities. *See* Pet’s Opp’n at 23. Presumably attempting to show that the standard *habeas* protective order covers TS/SCI information, petitioner also argues that preservation orders issued by this Court required the government to preserve information relating to all detainees ever held by the Department of Defense at Guantanamo Bay. *See id.* at 25. These facts, however, do not establish that the standard *habeas* protective order contains the necessary mechanisms for the protection of TS/SCI information. To the contrary, as respondents have shown in their opening brief (at pp. 8-9), the standard *habeas* protective order requires counsel to hold only a Secret level security clearance, and contains procedures for the transmission, handling and management of classified information consistent with the Secret level classification. For example, it contemplates mailing of communications to counsel from a Guantanamo detainee (or of notes of a counsel’s meeting with a detainee at Guantanamo) to the secure workspace facility in Washington, D.C., a type of transmission appropriate for information classified at the Secret level, but not at the TS/SCI level. *See* Standard Access Procedures §§ IV.B.3; VI.B; Amended Protective Order ¶ 20.

Petitioner also argues that respondents’ request for a TS/SCI protective order is moot or unnecessary because the government currently already uses a courier to transport ordinary legal mail under the standard *habeas* protective order and at least one counsel for each of the three high-value detainees already possesses TS/SCI security clearance. *See* Pet. Opp’n at 19, 20 n.15. This argument completely misses the mark. Due to the extremely sensitive nature of the information at issue, an appropriate protective order must explicitly require that the transmission

and management of TS/SCI information strictly conform to procedures established for handling such information. *Id.*; 32 C.F.R. § 2001.45(c),(d). Contrary to petitioner’s argument (Pet. Opp’n at 20 n.15), that the standard *habeas* protective order does not preclude the handling of TS/SCI information in accordance with appropriate procedures is insufficient to protect against unauthorized disclosure of TS/SCI information – it is appropriate that a protective order address the proper handling of TS/SCI information in the context of this case, including with respect to counsel visits and other access to detainees, Privilege Team functions, and other matters unique to the Guantanamo litigation. Similarly, there must be specific mechanisms to ensure that all individuals who may have access to presumptively TS/SCI information, such as interpreters, translators, paralegals, investigators and all other personnel or support staff employed to engaged to assist in the litigation, possess the proper security clearance. *See* Declaration of Marilyn A. Dorn (Oct. 26, 2006) (“Dorn Decl.”) (Ex. 1 to Respondents’ Mot. to Reconsider), ¶ 15.

Petitioner further maintains that in *Zalita v. Bush*, No. 05-CV-1220 (RMU) (D.D.C.), a case involving another detainee who is not a high value detainee and who is represented by the same counsel, counsel received authorization from the government to file presumptively TS/SCI information with the Court under the standard *habeas* protective order “without incident.” Pet. Opp’n at 25. As petitioner puts it, “no harm resulted from presumptively TS//SCI filings in *Zalita*, and none would result if the standard *habeas* protective order were entered here.” *Id.* Again, petitioner’s argument misses the mark because, first, *Zalita* did not involve initial access by counsel to a TS/SCI detainee or TS/SCI information (or its transmission from Guantanamo to D.C.) under the standard *habeas* protective order regime. Rather, as respondents explained in their opening brief (at p. 11), in *Zalita* respondents authorized TS/SCI-cleared petitioner’s

counsel to share information with the District Court that counsel had previously learned through access to petitioner in the context of petitioner's Detainee Treatment Act ("DTA") case in the Court of Appeals, in which a TS/SCI specific protective order applied. In other words, the access to TS/SCI information had been permitted pursuant to and was governed by the special TS/SCI access procedures applicable in the DTA litigation context. Thus, any reliance on the *Zalita* situation is inapposite.

Second, petitioner is in no position to determine whether harm would result if this Court enters the standard *habeas* protective order in this case. That expertise belongs to the agency charged with the responsibility of protecting the national security. As explained in the Dorn declaration, which should be accorded "substantial weight," *Wolf v. C.I.A.*, 473 F.3d 370, 375 (D.C. Cir. 2007); *see also Frugone v. CIA*, 169 F.3d 772, 775 (D.C. Cir. 1999); *Krikorian v. Dep't of State*, 984 F.2d 461, 464 (D.C. Cir. 1993); *Fitzgibbon v. CIA*, 911 F.2d 755, 766 (D.C. Cir. 1990), improper disclosure of operational details about the CIA terrorist detention program, such as the locations of detention facilities abroad, would put United States' allies at risk of terrorist retaliation and betray relationships that are built on trust and are vital to efforts against terrorism. *See* Dorn Decl, ¶ 12; *see also* Declaration of Wendy M. Hilton (Mar. 28, 2006) ¶¶ 12-20 ("Hilton Decl.") (Ex. 3 to Respondents' Mot. to Reconsider). Improper disclosure of other operational details, such as interrogation methods, could also enable terrorist organizations and operatives to adapt their training to counter such methods, thereby obstructing the CIA's ability to obtain vital intelligence that could disrupt future planned terrorist attacks.³ *See* Dorn Decl.

³ As the President explained when he first revealed the existence of the program in 2006, the program is "one of the most vital tools in our war against terrorists." *See* Ex. 2 to Respondents' Mot. to Reconsider at 4. Information obtained through the program has helped

¶ 13; Hilton Decl. ¶¶ 19-21. Respondents' motion has explained why the proposed TS/SCI protective order is needed and appropriate in light of these interests. The national security interests at stake are significant, and petitioner's characterization of the respondents' efforts to protect such interests as merely part of a scheme to deprive petitioner of his constitutional habeas rights is simply wrong.

II. A PRESUMED "NEED TO KNOW" STANDARD IS INAPPROPRIATE IN THIS CASE WHICH INVOLVES TS/SCI INFORMATION

Petitioner argues that eliminating the presumption that habeas counsel have a presumptive "need to know" all classified information possessed by other habeas counsel would make it "impossible for petitioner to discover and present exculpatory evidence or show that his detention is unlawful" and "create[] an impenetrable barrier between petitioner Khan and other CIA prisoners." Pet. Opp'n at 14, 18. Because petitioner supposedly "already knows the information" possessed by other high-value detainees by virtue of his current and past direct contacts with those detainees and has shared such information with counsel, as likely is the case for other high-value detainees, petitioner speculates that the proposed TS/SCI protective order is really an attempt to prevent strategic discussions among counsel. Pet. Opp'n at 20-21. This alleged inability to coordinate their litigation, petitioner further argues, would deprive petitioners of their opportunities to present a joint defense or to conduct common discovery, and lead to inefficiency, redundant efforts, and waste of judicial resources.

These concerns are ill founded. None of petitioner's arguments justifies dispensing with

deterred threats to the national security, including identifying probable targets and likely methods for attacks on the United States, disrupting terrorist plots against the United States and its allies, and assisting in the capture and questioning of senior Al Qaeda operatives. *Id.*; Dorn Decl. ¶ 11.

the procedures necessary to protect against the unauthorized disclosure of highly classified national security information. As an initial matter, contrary to petitioner's portrayal of an impenetrable wall between counsel for high-value detainees, the TS/SCI protective order proposes a case-by-case determination, not a blanket prohibition, of whether sharing of any specific TS/SCI information between counsel in various cases is appropriate. The proposed TS/SCI protective order also does not prohibit counsel for high-value detainees from sharing or exchanging unclassified or protected information. It contains the same provisions governing the sharing of protected information that are contained in the standard *habeas* protective order. *See* Protective Order ¶ 38. Both regimes provide for classification review, at counsel's request, of presumptively classified materials (involving information provided by a detainee to counsel) by the DoD Privilege Team. *Compare* Standard Access Procedures §§ VII *with* TS/SCI Access Procedures ¶ 6. If the information is determined not go be classified, then counsel can share it with other counsel for Guantanamo detainees.

To be sure, inefficiencies may result from petitioner's having to request the Government's authorization to share TS/SCI information on a case-by-case basis and in attempting to craft such requests without disclosing privileged information or possibly litigation strategy. But such a situation is insufficient to trump the compelling government interest in protecting highly classified sensitive information, the disclosure of which reasonably could be expected to cause "exceptionally grave damage" to national security. *See* Dorn Decl. ¶ 9; *see also* Executive Order 12958, § 1.2(1) (the "Top Secret" classification applies to information, "the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security"). As respondents have explained before, beyond the Top Secret

classification, the operation of the CIA's terrorist detention program is placed in a sensitive compartmented program to further enhance protection from unauthorized disclosure. *See* Dorn Decl. ¶ 10. And, under Executive Order 12958 (Classified National Security Information), a compartment is created only upon "a specific finding" that "(1) the vulnerability of, or threat to, specific information is exceptional; and (2) the normal criteria for determining eligibility for access applicable to information classified at the same level [*i.e.*, Top Secret] are not deemed sufficient to protect the information from unauthorized disclosure." *See* Executive Order 12958, § 4.3(a). A person who has been granted a security approval simply does not become entitled to access to all information classified at the level of the clearance. And even a person cleared into a compartment may not be given access to all the information in that compartment; they are given access to information only as they have a legitimate need to know it. In other words, possessing the appropriate clearance is only one requirement for access to classified information. A security clearance is but one part of a much larger scheme established to protect classified information from unauthorized disclosure. A person who has been granted a security approval neither becomes entitled to, nor should have, access to all information classified at the level of the clearance. The fact that a person has been granted a security approval means only that a federal agency completed an appropriate personnel security background investigation of the person and, based upon the results of that investigation, determined that the individual could be entrusted with access to classified information at a given level.

Moreover, the most effective way to minimize the risk of unauthorized disclosure of classified information is to control the number of people who have access to the information. Accordingly, section 4.1(a)(3) of Executive Order 12958 requires that a determination be made

that the individual has a “need-to-know” the classified information, which means “a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized government function, ” *id.* § 6.1(z). Furthermore, section 5.4(d)(5)(B) of the Executive Order, which establishes the current program for classifying and safeguarding national security information, specifically charges agencies to “ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements.” Thus, it is apparent that a presumed need-to-know hinders, and in fact, prevents, the protection of especially sensitive information, as there is no way to know what information has been shared; thus, any hope of addressing protection of that information would only come after an inappropriate disclosure has been made and somehow discovered. Such a system thus risks exactly what a sensitive compartment seeks to avoid – the unauthorized disclosure of particularly sensitive information to individuals with no need to know that information.

Petitioner argues that the protective order entered in the September 11th conspirators’ case before the military commission does not prohibit counsel for the co-accused to share TS/SCI information. Pet. Opp’n at 26. However, to the extent that there is any sharing among counsel for high-value detainees who are charged by the military commission to be co-conspirators in a single conspiracy, that is a far cry from suggesting that a presumptive “need to know” is appropriate in the very different context of separate, civil habeas cases. In other words, even assuming that there is sharing of TS/SCI information in the military commission context, the fact that the government undertakes a greater accommodation in that context, with an

associated increase in risk to national security, does not suggest that it should also do so here and greatly expand the number of people having access to exceptionally sensitive classified information.

Although petitioner also argues that even in single-accused commission cases, the government likewise permits sharing of classified information among counsel, he is simply wrong. He cites paragraph 12 of the memorandum from the Convening Authority for Military Commission to detailed defense counsel in the case involving Abd al Rahim Hussen Muhammed Abdu al-Nashiri, which states that “any additional person whose assistance the Defense reasonably requires may only have access to Classified Information in this case after obtaining the appropriate level of classification and your approval for access on a need-to-know basis.” Ex. 8 to Pet. Opp’n, at ¶ 12. That language does not suggest that defense counsel therefore has broad discretion to share classified information either with any such person or with counsel in unrelated commissions cases. Far from it, the portion of paragraph 12 that petitioner conveniently omits explicitly states that it is subject to paragraph 11, which provides, in relevant part, that “no member of the Defense, nor witness for the Defense, shall have access to any Classified Information involved unless that person shall first have: . . . (c) been determined to “need to know” the Classified Information at issue *by the Original Classification Authority . . .*” *Id.* ¶ 11 (emphasis added).

In any event, petitioner’s concerns are speculative at this juncture, as is the catastrophic impact petitioner predicts a case-by-case determination regime would have on his ability to litigate his core constitutional habeas rights. Respondents have not filed a factual return in petitioner’s habeas case. Until the parties and the Court have a concrete factual record

explaining the basis for petitioner's detention, it is speculative whether petitioner may have any need for access to TS/SCI information within the possession of other high-value detainees.

In addition, the Court is currently considering the parties' competing submissions addressing procedural framework and discovery standards. Petitioner's concerns about his potential inability to conduct common discovery with other high-value detainees or to present a joint defense as if they were co-defendants are simply premature. And, as discussed above, when the need to share TS/SCI information arises, counsel can seek authorization on a case-by-case basis, as they have successfully done recently in order to share information regarding the medical condition of another high value detainee, Abu Zubaydah (*see* Pet. Opp'n at 23).

What is left of petitioner's argument then is that a presumptive "need to know" regime would be more efficient for habeas counsel. Petitioner complained about the fact that counsel for the three high-value detainees who have pending habeas cases were constrained in their ability to coordinate their response to respondents' proposed TS/SCI protective order. *See* Pet. Opp'n at 32. Even assuming some inefficiency in separately litigating the legality of each detainee's detention, that is not an appropriate basis for the Court to adopt a protective order regime that may expand the circle of individuals with access to highly classified information in a fashion that undermines the Executive's authority to safeguard that information. In the unique and especially sensitive circumstance of this case, which involves TS/SCI information, this Court should proceed in a "prudent and incremental" fashion, *Hamdi v. Rumsfeld*, 542 U.S. 507, 538-539 (2004) (plurality), and use its discretion to accommodate the government's interest in protecting national security information "to the greatest extent possible." *Boumediene*, 128 S.

Ct. at 2276. Respondents' proposed TS/SCI protective order presents a proper balance between accommodating petitioner's concerns and Executive Branch's constitutional responsibility to protect highly classified national security information. Accordingly, it should be adopted by this Court.

CONCLUSION

For the foregoing reasons, this Court should enter respondents' proposed TS/SCI protective order in this case.

Dated: September 26, 2008

Respectfully submitted,

GREGORY G. KATSAS
Assistant Attorney General

JOHN C. O'QUINN
Deputy Assistant Attorney General

/s/ Andrew I. Warden
JOSEPH H. HUNT
VINCENT M. GARVEY
JUDRY L. SUBAR
TERRY M. HENRY
ANDREW I. WARDEN (IN Bar No. 23840-49)
JEAN LIN
United States Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue N.W.
Washington, DC 20530
Tel: (202) 514-3716
Fax: (202) 616-8470

Attorneys for Respondent