

UNITED STATES DISTRICT COURT FOR  
THE DISTRICT OF COLUMBIA

MUSTAFA AHMED AL-HAWSAWI,

Petitioner,

v.

No. 21-cv-2907 (RJL)

JOSEPH R. BIDEN JR. et al.,

Respondents.

**AMENDED PROTECTIVE ORDER FOR HABEAS CASE INVOLVING TOP SECRET/  
SENSITIVE COMPARTMENTED INFORMATION**

**AND**

**PROCEDURES FOR COUNSEL ACCESS TO DETAINEES AT THE UNITED STATES  
NAVAL BASE IN GUANTANAMO BAY, CUBA, IN HABEAS CASES INVOLVING TOP  
SECRET/SENSITIVE COMPARTMENTED INFORMATION**

The Court finds that the above-captioned civil case involves national security information or documents, including up to TOP SECRET/SENSITIVE COMPARTMENTED INFORMATION (“TS/SCI”), the storage, handling, and control of which require special security precautions and access to which requires a security clearance and a “need to know.” This case might also involve other protected information or documents, the storage, handling, and control of which might require special precautions in order to protect the security of the United States and other significant interests. Accordingly, to protect the national security, and for good cause shown, the Court

**ORDERS** that the following Amended Protective Order for Habeas Case Involving TOP SECRET/SENSITIVE COMPARTMENTED INFORMATION (“TS/SCI Protective Order”) and Procedures for Counsel Access to Detainees at the United States Naval Base in Guantanamo Bay, Cuba, in Habeas Cases Involving TOP SECRET/SENSITIVE

COMPARTMENTED INFORMATION (“TS/SCI Procedures for Counsel Access”) applies in the above-captioned civil case:

**I. PROTECTIVE ORDER FOR HABEAS CASE INVOLVING TOP SECRET/SENSITIVE COMPARTMENTED INFORMATION**

**A. Overview and Applicability**

1. This TS/SCI Protective Order establishes procedures that must be followed by petitioner and his respective counsel, all other counsel involved in this matter, interpreters and translators for the parties, personnel or support staff employed or engaged to assist in this matter, and all other individuals who, in connection with this matter, receive access to classified national security information or documents or other protected information, including the Privilege Team as defined in the TS/SCI Procedures for Counsel Access, *see infra* Section II.B.6, and the Special Litigation Team as defined in the TS/SCI Procedures for Counsel Access, *see infra* Section II.B.7.
2. The procedures set forth in this TS/SCI Protective Order apply to all aspects of this matter and may be modified by further order of the Court upon its own motion or upon application by any party. The Court retains continuing jurisdiction to enforce or modify the terms of this TS/SCI Protective Order.
3. Nothing in this TS/SCI Protective Order precludes the government’s use of classified information as otherwise authorized by law outside of this matter.
4. As appropriate and needed, petitioner’s counsel are responsible for advising their employees, petitioner, and others of this TS/SCI Protective Order’s contents.
5. Petitioner’s counsel are bound by the terms and conditions set forth in the TS/SCI Procedures for Counsel Access, *see infra* Section II. To the extent such terms and conditions place limitations on petitioner’s counsel in their access to and interaction with petitioner or handling of information, this TS/SCI Protective Order specifically incorporates by reference all terms and conditions established in the procedures contained in the TS/SCI Procedures for Counsel Access. Any violation of those terms and conditions also will be deemed a violation of this TS/SCI Protective Order.
6. The Privilege Team shall not disclose to any person any information provided by petitioner’s counsel or petitioner, other than information provided in a filing with the Court, unless such information, if it were monitored information, could be disclosed under the TS/SCI Procedures for Counsel Access. Any such disclosure shall be consistent with the provisions of the TS/SCI Procedures for Counsel Access.

**B. Definitions**

7. As used in this TS/SCI Protective Order, the words “documents” and

“information” include, but are not limited to, all written or printed matter of any kind, formal or informal, including originals, conforming copies and non-conforming copies, whether different from the original by reason of notation made on such copies or otherwise, and further include, but are not limited to:

- a. papers, correspondence, memoranda, notes, letters, reports, summaries, photographs, maps, charts, graphs, interoffice and intra-office communications, notations of any sort concerning conversations, meetings, or other communications, bulletins, teletypes, telegrams, facsimiles, invoices, worksheets, and drafts, alterations, modifications, changes, and amendments of any kind to the foregoing;
  - b. graphic or oral records or representations of any kind, including, but not limited to, photographs, charts, graphs, microfiche, microfilm, videotapes, sound recordings of any kind, and motion pictures;
  - c. electronic, mechanical or electric records of any kind, including, but not limited to, tapes, cassettes, disks, recordings, electronic mail, films, typewriter ribbons, word processing or other computer tapes or disks, and all manner of electronic data processing storage; and
  - d. information acquired orally.
8. Unless otherwise stated, the terms “classified national security information and/or documents,” “classified information” and “classified documents” mean:
- a. any classified document or information that was classified by any Executive Branch agency in the interests of national security or pursuant to Executive Order, including Executive Order 13526, as amended, or its predecessor Orders, as “CONFIDENTIAL,” “SECRET,” or “TOP SECRET,” or additionally controlled as “SENSITIVE COMPARTMENTED INFORMATION (SCI),” or any classified information contained in such document;
  - b. any document or information, regardless of its physical form or characteristics, now or formerly in the possession of a private party that was derived from United States government information that was classified, regardless of whether such document or information has subsequently been classified by the government pursuant to Executive Order, including Executive Order 13526, as amended, or its predecessor Orders, as “CONFIDENTIAL,” “SECRET,” or “TOP SECRET,” or additionally controlled as “COMPARTMENTED INFORMATION (SCI)”;
  - c. verbal or non-documentary classified information known to petitioner or petitioner’s counsel; or
  - d. any document and information as to which petitioner or petitioner’s counsel were notified orally or in writing that such document or information contains classified information.
9. All classified documents, and information contained therein, shall remain classified unless the documents bear a clear indication that they were

declassified by the agency or department that is the original classification authority of the document or the information contained therein (hereinafter, "original classification authority").

10. The terms "protected information and/or documents," "protected information," and "protected documents" mean any document or information the Court deems, either *sua sponte* or upon designation pursuant to paragraph 35 of this TS/SCI Protective Order or paragraph 34 of the Protective Order first entered by Judge Hogan in 08-mc-442 on September 11, 2008, not suitable for public filing.
11. As used in this TS/SCI Protective Order, the term "petitioner's counsel" includes attorneys employed or retained by or on behalf of a petitioner for purposes of representing the petitioner in habeas corpus or other litigation in federal court in the United States, as well as co-counsel, interpreters/translators, paralegals, investigators and all other personnel or support staff employed or engaged to assist in the litigation. Access to classified information by all persons mentioned in the foregoing sentence is governed by Section I.D of this TS/SCI Protective Order, and access to protected information by all persons mentioned in the foregoing sentence is governed by Section I.E of this TS/SCI Protective Order.
12. "Access to classified information" or "access to protected information" means having access to, reviewing, reading, learning, or otherwise coming to know in any manner any classified information or protected information.
13. "Secure area" means a physical facility accredited or approved for the storage, handling, and control of classified information.
14. "Unauthorized disclosure of classified information" means any knowing, willful, or negligent action that could reasonably be expected to result in a communication or physical transfer of classified information to an unauthorized recipient.

#### **C. Designation of Court Security Officer**

15. The Court designates Harry J. Rucker, Litigation Security Group, U.S. Department of Justice, as Classified Information Security Officer for this case, along with Daniel O. Hartenstine, Daniella M. Medel, Matthew W. Mullery, Carli V. Rodriguez-Feo, and Winfield S. Slade as Alternate Classified Information Security Officers (collectively, "CISO") for the purpose of providing security arrangements necessary to protect against unauthorized disclosure of any classified documents or information to be made available in connection with this case. Petitioner's counsel shall seek guidance from the CISO with regard to appropriate storage, handling, transmittal, and use of classified documents or information.

#### **D. Access to Classified Information and Documents**

16. Without authorization from the government, no petitioner or petitioner's counsel shall have access to any classified information involved in this case unless that person has done the following:

- a. received the necessary security clearance as determined by the Department of Justice Security Officer; and
  - b. signed the Memorandum of Understanding ("MOU"), attached hereto as Exhibit A, agreeing to comply with the terms of this TS/SCI Protective Order.
17. Petitioner's counsel to be provided access to classified information shall execute the MOU appended to this TS/SCI Protective Order, and shall file executed originals of the MOU with the Court and submit copies to the CISO and government counsel. Such execution, filing, and submission of the MOU is a condition precedent to a petitioner's counsel having access to, or continued access to, classified information for the purposes of these proceedings.
18. The substitution, departure, or removal of any petitioner's counsel from these cases for any reason shall not release that person from the provisions of this TS/SCI Protective Order or the MOU executed in connection with this TS/SCI Protective Order.
19. The government has arranged for one appropriately approved secure area for petitioners' counsel's use in the Guantanamo *habeas* cases. The secure area shall contain a working area supplied with secure office equipment reasonably necessary for preparing petitioner's case. The government shall bear expenses for the secure area and its equipment.
20. The CISO shall establish procedures to ensure that the secure area is accessible to petitioner's counsel during normal business hours and at other times on reasonable request as approved by the CISO. The CISO shall establish procedures to ensure the secure area is maintained and operated in the most efficient manner consistent with the protection of classified information. The CISO or CISO designee may place reasonable and necessary restrictions on the schedule of use of the secure area in order to accommodate appropriate access to all petitioners' counsel in this and other Guantanamo habeas proceedings.
21. All classified information the government provides to petitioner's counsel, and all classified information petitioner's counsel otherwise possesses or maintains, shall be stored, maintained, and used only in the secure area.
22. No documents containing classified information may be removed from the secure area unless authorized by the CISO or CISO designee supervising the area.
23. Consistent with other provisions of this TS/SCI Protective Order, petitioner's counsel shall have access to the classified information made available to them in the secure area and shall be allowed to take notes and prepare documents with respect to those materials.
24. Petitioner's counsel shall not copy or reproduce any classified information in any form, except with the CISO's approval or in accordance with the procedures established by the CISO for the operation of the secure area.
25. All documents prepared by petitioner or petitioner's counsel that contain or may

contain classified information—including, without limitation, notes taken or memoranda prepared by counsel and pleadings or other documents intended for filing with the Court—shall be transcribed, recorded, typed, duplicated, copied, or otherwise prepared only by persons possessing an appropriate approval for access to classified information. Such activities shall take place in the secure area on approved word processing equipment and in accordance with the procedures approved by the CISO. All such documents and any associated materials containing classified information—such as notes, memoranda, drafts, copies, typewriter ribbons, magnetic recordings, and exhibits—shall be maintained in the secure area unless and until the CISO advises that those documents or associated materials are unclassified in their entirety. None of these materials shall be disclosed to government counsel unless authorized by the Court, by petitioner's counsel, or as otherwise provided in this TS/SCI Protective Order.

26. Petitioner's counsel may discuss classified information within the secure area or another area authorized by the CISO only. Petitioner's counsel shall not discuss classified information over any standard commercial telephone instrument or office intercommunication system and shall not transmit or discuss classified information in electronic mail communications of any kind.
27. The CISO or CISO designee shall not reveal to any person the content of any conversations he or she hears by or among petitioner's counsel, nor reveal the nature of documents being reviewed by them or the work generated by them, except as necessary to report violations of this TS/SCI Protective Order to the Court or to carry out their duties pursuant to this TS/SCI Protective Order. Additionally, the presence of the CISO or CISO designee shall not be construed to waive, limit, or otherwise render inapplicable the attorney-client privilege or work product protections.
28. A petitioner's counsel is presumed to have a "need to know" all the information in the government's possession concerning the detainee or detainees whom that counsel represents. This presumption is overcome to the extent the government seeks to withhold from a petitioner's counsel highly sensitive information or information concerning a highly sensitive source that the government presents to the Court *ex parte* and *in camera*. Except for good cause shown, the government must provide notice to petitioner's counsel the same day it files such information with the Court *ex parte*.
29. Petitioner's counsel shall not disclose the contents of any classified documents or information to any person, including counsel in related cases brought by Guantanamo Bay detainees in this or other courts, except those persons authorized by this TS/SCI Protective Order, the Court, and counsel for the government with the appropriate clearances and the need to know that information. Petitioner's counsel may seek, on a case-by-case basis, authorization from appropriate officials to disclose classified information to appropriately cleared counsel in related cases brought by Guantanamo Bay detainees in this or other courts or to receive such information from them. Such authorization shall not be unreasonably withheld. If petitioner's counsel believe authorization is being unreasonably withheld, counsel may seek this Court's intervention.
30. Petitioner's counsel shall not disclose to a petitioner-detainee classified information

not provided by that petitioner-detainee. Should a petitioner's counsel desire to disclose classified information not provided by a petitioner-detainee to that petitioner-detainee, that petitioner's counsel will provide in writing to the Privilege Team, *see infra* Section II.G, a request for release clearly stating the classified information they seek to release. The Privilege Team will forward a petitioner's counsel's release request to the appropriate government agency authorized to declassify the classified information for a determination. The Privilege Team will inform petitioner's counsel of the determination once it is made.

31. Except as otherwise provided herein, neither petitioner nor petitioner's counsel shall disclose or cause to be disclosed any information known or believed to be classified in connection with any hearing or proceeding in this case.
32. Except as otherwise stated in this paragraph, and to ensure the security of the United States of America, at no time, including any period subsequent to the conclusion of these proceedings, shall petitioner's counsel make any public or private statements disclosing any classified information or documents accessed pursuant to this TS/SCI Protective Order, including the fact that any such information or documents are classified. In the event that classified information enters the public domain, however, counsel is not precluded from making private or public statements about the information already in the public domain, but only to the extent that the information is in fact in the public domain. Counsel may not make any public or private statements revealing personal knowledge from non-public sources regarding the classified or protected status of the information or disclosing that counsel had personal access to classified or protected information confirming, contradicting, or otherwise relating to the information already in the public domain. In an abundance of caution and to help ensure clarity on this matter, the Court emphasizes that counsel shall not be the source of any classified or protected information entering the public domain. As stated in more detail in paragraph 52 of this TS/SCI Protective Order, failure to comply with these rules may result in the revocation of counsel's security clearance as well as civil and criminal liability.

//

//

//

//

//

//

33. The foregoing does not prohibit a petitioner's counsel from citing or repeating information in the public domain that petitioner's counsel does not know to be classified information or a classified document or derived from classified information or a classified document.
34. All documents containing classified information prepared, possessed or maintained by, or provided to, petitioner's counsel—except filings submitted to the Court and served on government counsel—shall remain at all times in the CISO's control for the duration of these cases. Upon final resolution of these cases, including all appeals, the CISO shall destroy all such documents.

**E. Designation Procedures for and Access to Protected Information and Documents**

35. Should government counsel in this case wish to have the Court deem any document or information "protected," government counsel shall disclose the information to qualified counsel for petitioner—*i. e.*, counsel who have satisfied the necessary prerequisites of this TS/SCI Protective Order for the viewing of protected information—and attempt to reach an agreement about the designation of the information prior to filing a motion with the Court. Petitioner's counsel shall treat such disclosed information as protected unless and until the Court rules that the information should not be designated as protected.
36. Without authorization from the government or the Court, protected information shall not be disclosed or distributed to any person or entity other than the following:
  - a. petitioner's counsel, provided such individuals signed the Acknowledgment, attached hereto as Exhibit B, attesting to the fact that they read this TS/SCI Protective Order and agree to be bound by its terms; and
  - b. the Court and its support personnel.
37. The execution of the Acknowledgment is a condition precedent to a petitioner's counsel having access to, or continued access to, protected information for the purposes of these proceedings. A copy of each executed Acknowledgment shall be kept by counsel making the disclosure until thirty days after the termination of this action, including appeals.
38. The substitution, departure, or removal of a petitioner's counsel from these cases for any reason shall not release that person from the provisions of this TS/SCI Protective Order or the Acknowledgment executed in connection with this TS/SCI Protective Order.
39. Petitioner's counsel shall not disclose the contents of any protected documents or information to any person, including counsel in related cases brought by Guantanamo Bay detainees in this or other courts, except as authorized by this TS/SCI Protective Order, the Court, or government counsel. Petitioner's counsel may share protected information with each other but only to the extent that counsel have appropriate security clearances and comply with all other procedures set forth in this TS/SCI Protective Order. Petitioner's counsel shall maintain all protected information and



documents received through this proceeding in a confidential manner.

40. Petitioner's counsel shall not disclose protected information not provided by a petitioner-detainee to that petitioner-detainee without prior concurrence of government counsel or express permission of the Court.
41. Except as otherwise provided herein, no petitioner or petitioner's counsel shall disclose or cause to be disclosed any information known or believed to be protected in connection with any hearing or proceeding in this case.
42. At no time, including any period subsequent to the conclusion of these proceedings, will petitioner's counsel make any public or private statements disclosing any protected information or documents accessed pursuant to this TS/SCI Protective Order, including the fact that any such information or documents are protected.
43. Protected information shall be used only for purposes directly related to these cases and not for any other litigation or proceeding, except by leave of the Court. Photocopies of documents containing such information shall be made only to the extent necessary to facilitate the permitted use hereunder.
44. Nothing in this TS/SCI Protective Order shall prevent the government from using for any purpose protected information it provides a party. Nothing in this TS/SCI Protective Order shall entitle another party to protected information.
45. Supplying protected information to another party does not waive privilege with respect to any person or use outside that permitted by this TS/SCI Protective Order.
46. Within sixty days of the resolution of these actions, and the termination of any appeals therefrom, all protected documents or information, and any copies thereof, shall be promptly destroyed, provided that the party to whom protected information is disclosed certifies in writing that all designated documents and materials have been destroyed, and further provided that government counsel may retain one complete set of any such materials that were presented in any form to the Court. Any such retained materials shall be placed in an envelope or envelopes marked "Protected Information Subject to Protective Order." In any subsequent or collateral proceeding, a party may seek discovery of such materials from the government, without prejudice to the government's right to oppose such discovery or its ability to dispose of the materials pursuant to its general document retention policies.

#### **F. Procedures for Filing Documents**

47. [OMITTED TO FACILITATE CONSISTENCY OF PARAGRAPH NUMBERING WITH SIMILAR ORDERS IN OTHER GUANTANAMO CASES]
48. Filings by Petitioner. Any pleading or other document filed by petitioner shall be filed, along with three copies, under seal with the CISO by 4:00 p.m., unless the petitioner obtains from the CISO permission, specific to a particular, non-substantive pleading or document (e.g., motions for extensions of time, continuances, scheduling matters) not containing information that is or may be

classified or protected, to file the pleading or document not under seal. Such pleading or document must be marked with the appropriate classification marking (e.g., "TOP SECRET/SENSITIVE COMPARTMENTED INFORMATION"), if any. The time of physical submission to the CISO shall be considered the date and time of filing. At the time of making a submission to the CISO, petitioner's counsel shall file on the public record in the CM/ECF system a "Notice of Filing," notifying the Court that the submission was made to the CISO and specifying in general terms the nature of the filing without disclosing any potentially classified information.

- a. Upon receipt, the CISO will deliver to the Court and government counsel any pleading or other document petitioner files. The CISO will forward the document to the appropriate government agencies and departments for their determination as to whether the pleading or other document contains classified information. To facilitate this review, petitioner's counsel shall identify each paragraph of a document that counsel believe may contain classified information by marking each paragraph with an appropriate classification marking or otherwise specifically identifying such paragraphs. If, following review by the appropriate government agencies and departments, it is determined that the pleading or other document contains classified information, the CISO must ensure that the document is marked with the appropriate classification marking and that the document remains under seal. The CISO will work with the appropriate government agencies or departments to prepare a redacted version of the pleading or other document appropriate for filing on the public record. Counsel shall then file the redacted version of the document in the CM/ECF system with a notation in the upper right hand corner of the first page stating "REDACTED VERSION FOR PUBLIC FILING CLEARED BY CISO." The docket entry description in the CM/ECF system for the document suitable for public viewing shall make specific reference to the earlier docket entry notifying the Court that the document was submitted to the CISO for review.
- b. If it is determined that the entire pleading or other document is classified, petitioner's counsel shall file notice in the CM/ECF system listing the caption of the case, a version of the title of the document that does not disclose classified or protected information, and a brief statement that the CISO informed counsel that the entire document is classified. The docket entry description in the CM/ECF system for the document suitable for public viewing shall make specific reference to the earlier docket entry notifying the Court that the document was submitted to the CISO for review.
- c. If it is determined that the pleading or other document does not contain classified information, counsel shall file the full submission in the CM/ECF system consistent with the regular electronic filing practices of this Court, *see* LCvR 5.4, and make specific reference to the earlier docket entry notifying the Court that the document was submitted to the CISO for review. The docket entry description shall also state that the CISO approved public filing of the document. The underlying document filed in the CM/ECF system shall contain a notation in the upper right hand corner of the first page stating "PREVIOUSLY FILED WITH CISO AND CLEARED FOR PUBLIC FILING."

- d. If it is determined that the pleading or other document does not contain classified information but does contain protected information, counsel shall file the pleading or document in accordance with the procedures outlined in Section I.F.50 of this TS/SCI Protective Order.

49. Classified Filings by Respondents.

- a. Any pleading or other document filed by respondents' counsel containing classified information shall be filed, along with three copies, under seal with the Court through the CISO by 4:00 p.m. The time of physical submission to the CISO shall be considered the date and time of filing. The CISO shall serve a copy of any classified pleading or document on petitioner's counsel at the secure facility. At the time of making a submission to the CISO, respondents shall file on the public record in the CM/ECF system a "Notice of Filing," notifying the Court that a submission was made to the CISO and specifying in general terms the nature of the filing without disclosing any potentially classified information. As soon as practicable following the original filing date, respondents' counsel shall file in the CM/ECF system a version of the pleading or document appropriate for filing on the public record, consistent with the procedures outlined in paragraphs 48.a-d of this TS/SCI Protective Order.
- b. Nothing herein requires the government to disclose classified information. Additionally, nothing herein prohibits the government from submitting classified information to the Court *in camera* or *ex parte* in these proceedings or entitles petitioner or petitioner's counsel access to such submissions or information. Except for good cause shown in the filing, the government shall provide petitioner's counsel or petitioner with notice served on petitioner's counsel on the date of the filing.

50. Protected Information Filing by Petitioner and Respondents.

- a. The presence, or potential presence, of protected information in any pleading or document that is governed by paragraph 48 or paragraph 49 of this TS/SCI Protective Order shall not affect the method of filing such pleading or document; it shall be governed by paragraph 48 or 49, as applicable. Any pleading or other document that does not contain classified information but that contains protected information shall be filed under seal pursuant to Local Civil Rule 5.1(h). Further, any pleading or other document that does not contain classified information but that petitioner's counsel or respondents have reason to believe contains or petitioner's counsel is uncertain whether it contains protected information shall be filed under seal pursuant to Local Civil Rule 5.1(h). At the time of the submission of a filing containing protected but not classified information, the party shall file on the public record in the CM/ECF system a "Notice of Filing," notifying the Court that a protected information submission was made and specifying in general terms the nature of the filing without disclosing any potentially protected information. As soon as practicable following the original filing date, counsel for the party submitting the protected information shall file in

the CM/ECF system a version of the pleading or document appropriate for filing on the public record, consistent with the procedures outlined in paragraphs 48.a-d of this TS/SCI Protective Order.

- b. This TS/SCI Protective Order shall constitute authorization for petitioner and respondents to file protected information under seal. That is, no motion to seal is required at the time of submission of the pleading or document to the Clerk's Office. Procedures for designation of protected information shall be governed by paragraph 35 of this TS/SCI Protective Order.
- c. Nothing herein requires the government to disclose protected information. Additionally, nothing herein prohibits the government from submitting protected information to the Court *in camera* or *ex parte* in these proceedings or entitles petitioner or petitioner's counsel access to such submissions or information. Except for good cause shown in the filing, the government shall provide counsel for the petitioner or petitioner with notice served on counsel on the date of the filing.

51. Disclosure of Protected or Classified Information on the Public Record. In the event respondents believe that a party has disclosed classified or protected information on the public docket, respondents shall notify the CISO, who shall work with the Clerk's Office to remove the filing from the public docket. A copy of the filing shall then be lodged with the CISO and treated according to paragraphs 48.b or 48.c of this TS/SCI Protective Order. Nothing herein limits the government's authority to take necessary remedial action to ensure the protection of the classified or protected information.

#### **G. Penalties for Unauthorized Disclosure**

52. Any unauthorized disclosure of classified information may constitute violations of United States criminal laws. Additionally, any violation of the terms of this TS/SCI Protective Order shall be immediately brought to the attention of the Court and may result in a charge of contempt of Court and possible referral for criminal prosecution. *See, e.g.*, Executive Order 13526, as amended. Any breach of this TS/SCI Protective Order may also result in the termination of access to classified information and protected information. Persons subject to this TS/SCI Protective Order are advised that direct or indirect unauthorized disclosure, retention, or negligent handling of classified documents or information could cause damage to the national security of the United States or may be used to the advantage of an adversary of the United States or against the interests of the United States. Persons subject to this TS/SCI Protective Order are also advised that direct or indirect unauthorized disclosure, retention, or negligent handling of protected documents or information could risk the security of United States government personnel and facilities and other significant government interests. This TS/SCI Protective Order is to ensure that those authorized to receive classified information and protective information will not divulge this information to anyone who is not authorized to receive it without prior written authorization from the original classification authority and in conformity with this TS/SCI Protective Order.

53. The termination of these proceedings shall not relieve any person or party provided classified information or protected information of his, her, or its obligations under this TS/SCI Protective Order.

//

//

//

//

//

//

//

//

//

//

//

//

//

## **II. PROCEDURES FOR COUNSEL ACCESS TO DETAINEES AT THE UNITED STATES NAVAL BASE IN GUANTANAMO BAY, CUBA, IN HABEAS CASES INVOLVING TOP SECRET/SENSITIVE COMPARTMENTED INFORMATION**

### **A. Applicability**

1. Except as otherwise stated in these Procedures for Counsel Access to Detainees at the U.S. Naval Base in Guantanamo Bay, Cuba, in Habeas Cases Involving TOP SECRET/SENSITIVE COMPARTMENTED INFORMATION ("Procedures"), or by other order issued in the United States District Court for the District of Columbia, the following procedures shall govern counsel access to certain detainees in the control of the Department of Defense ("DoD") at the U.S. Naval Base in Guantanamo Bay, Cuba ("GTMO"), whose cases may involve TOP SECRET/SENSITIVE COMPARTMENTED INFORMATION ("TS/SCI").
2. These Procedures do not apply to counsel who are retained solely to assist in a detainee's defense in a trial by military commission. Access and information obtained through access to a detainee by that counsel are covered by the procedures established in the Military Commissions Act, its implementing rules and regulations, as well as any applicable order of the military judge in those proceedings.

### **B. Definitions**

3. "Communications" means all forms of communication between counsel and a detainee, including oral, written, electronic, or by any other means.
4. As used in these Procedures, "counsel" means attorneys employed or retained by or on behalf of a detainee for purposes of representing the detainee in the United States District Court for the District of Columbia and admitted, either generally or *pro hac vice*, in this Court. Unless otherwise stated, "counsel" also includes co-counsel, interpreters/translators, paralegals, investigators, and all other personnel or support staff employed or engaged to assist in the litigation.
5. "Detainee" means an individual detained by DoD as an alleged enemy combatant at GTMO.
6. "Privilege Team" means a team comprised of one or more DoD attorneys and one or more intelligence or law enforcement personnel who have not taken part in, and, in the future, will not take part in, any domestic or foreign court, military commission, or combatant status tribunal proceedings involving the detainee, except in a similar role to that provided in these Access Procedures. If required, the Privilege Team may include interpreters/translators, provided that such personnel meet these same criteria.
7. "Special Litigation Team" means a team comprised of one or more Department of Justice ("DoJ") attorneys who have not taken part in, and, in the future, will not take part in, any domestic or foreign court, military commission, or combatant status tribunal proceedings involving the detainee. The Special Litigation Team is

authorized to represent the Privilege Team with respect to the execution of its duties.

8. "Legal mail" means letters written between a detainee's counsel and the detainee that are related to the counsel's representation of the detainee, as well as privileged documents and publicly filed legal documents relating to that representation. The Court is the final arbiter of whether documents fall within the definition of legal mail.

### **C. Requirements for Access to and Communications with Detainees**

9. Security Clearance.
  - a. Counsel must hold a valid, current United States security clearance at the TS/SCI level or its equivalent, as determined by appropriate DoD intelligence personnel.
  - b. Counsel who possess a valid security clearance shall provide to the Department of Justice, Litigation Security Division, in writing, the date of their background investigation, the date such clearance was granted, the level of the clearance, and the agency that granted the clearance. Access will be granted only after DoD verification of the security clearance.
  - c. Counsel who do not currently possess a TS/SCI clearance are required to submit an application for clearance to the Department of Justice, Litigation Security Division.
10. Acknowledgment of and Compliance with Access Procedures.
  - a. Before being granted access to a detainee, counsel will receive a copy of these Procedures. To have access to a detainee, counsel must agree to comply fully with these Procedures and must sign the Affirmation, attached hereto as Exhibit C, acknowledging an agreement to comply with them.
  - b. This Affirmation will not be considered an acknowledgment by counsel that these Procedures are legally permissible. Even if counsel elect to challenge these Procedures, counsel may not knowingly disobey an obligation imposed by these Procedures until such time, if any, that the Procedures are modified or revoked by DoD, a United States District Court or Court of Appeals, or the United States Supreme Court.

- c. DoD expects that counsel, counsel's staffs, and anyone acting on counsel's behalf will fully abide by the requirements of these Procedures. Counsel are required to provide DoD with signed Affirmations from interpreters/translators, paralegals, investigators and all other personnel or support staff employed or engaged to assist in the litigation, upon use of those individuals by counsel in a manner that implicates these Procedures.
- d. Should counsel fail to comply with these Procedures, access to or communication with detainees will not be permitted.

11. Verification of Representation.

- a. Prior to being permitted access to a detainee, counsel must provide DoJ with a Notification of Representation. This Notification must include counsel's licensing information, business and email addresses, and phone number, as well as the name of the detainee counsel represents. Additionally, counsel shall provide evidence of their authority to represent the detainee.
- b. Counsel shall provide evidence of their authority to represent the detainee as soon as practicable and, in any event, not later than ten days after the conclusion of a second visit with a detainee. The Court recognizes that counsel may not be in a position to present such evidence after the initial meeting with a detainee. Counsel for detainees and counsel for respondents shall cooperate to the fullest extent possible to reach a reasonable agreement on the number of counsel visits allowed. Should a detainee's counsel believe the government is unreasonably limiting the number of visits with the detainee, counsel may petition the Court at the appropriate time for relief.
- c. If counsel withdraw from representation of a detainee, or if representation is otherwise terminated, counsel shall inform DoJ immediately of that change in circumstances.
- d. Counsel must provide DoJ with a signed representation stating (a) that, to the best of counsel's knowledge after reasonable inquiry, the source of funds to pay counsel any fees or reimbursement of expenses are not funded directly or indirectly by persons or entities counsel believes are connected to terrorism or the product of terrorist activities, including "Specially Designated Global Terrorists," identified pursuant to Exec. Order No. 13,224, 66 Fed. Reg. 49,079 (Sept. 23, 2001), as amended, and (b) counsel has complied with ABA Model Rule 1.8(f).



12. Logistics of Counsel Visits.

- a. Counsel shall submit to DoD any request to meet with a detainee. DoD annually distributes guidance (Habeas Counsel Information Letter) for management of detainee visits and for making requests for such visits, including requirements for supplying information regarding specification of dates of availability for a meeting, the desired duration of the meeting, and the language that will be utilized during the meeting with the detainee. Reasonable efforts will be made to accommodate counsel's requests regarding the scheduling of a visit/meeting.
- b. Legal visits shall take place in a room designated by JTF-Guantanamo. No more than two attorneys (or one attorney and one assistant) plus one interpreter/translator shall visit with a detainee at one time, unless approved in advance by the Commander, JTF-Guantanamo. Such approval shall not be unreasonably withheld.
- c. Due to the mission and location of GTMO, certain logistical details, including arrangements for travel and lodging, will need to be coordinated by counsel prior to arrival. DoD will provide specific information regarding these issues.
- d. In order to travel to GTMO, counsel must have multiple clearances and DoD approvals for that specific visit. To begin the process of obtaining those clearances and approvals, counsel must have identified flight information for travel to GTMO and a valid, current United States security clearance at the TS/SCI level or its equivalent, as determined by appropriate DoD intelligence personnel. Accordingly, counsel shall provide DoD with the required information no later than twenty-seven days prior to the GTMO visit date. Requests for visits made inside of 27 days will not normally be granted. Modification of this timeframe is permissible to accommodate pandemic response measures.

**D. Procedures for Correspondence Between Counsel and Detainees**

13. Mail Sent by Counsel to Detainees ("Incoming Mail").

- a. Counsel shall send incoming legal mail for detainees to the Privilege Team at the appropriate address provided by DoD. Each envelope or mailer shall be labeled with the detainee's name and Internment Serial Number ("ISN") and shall include a return address for counsel sending the materials. The outside of the envelope or mailer for incoming legal mail shall be labeled clearly with the following annotation: "Attorney-Detainee Materials-For Mail Delivery to Detainee."
- b. Each page of legal mail shall be labeled "Attorney-Detainee Materials." No staples, paper clips or any non-paper items shall be included with the documents.

- c. Upon receiving legal mail from counsel for delivery to the detainee, the Privilege Team shall open the envelope or mailer to search the contents for prohibited physical contraband. Within two business days of receipt of legal mail, and assuming no physical contraband is present, the Privilege Team shall prepare the mail for transport via an appropriate courier system to military personnel at GTMO in a sealed envelope marked "Legal Mail Approved by Privilege Team" and clearly indicating the identity of the detainee to whom the legal mail is to be delivered. The Privilege Team shall return to the sender any incoming mail that does not comply with the terms of paragraphs 13.a and 13.b of these Procedures.
- d. Within two business days of receipt of legal mail from the Privilege Team, personnel at GTMO shall deliver the envelope or mailer marked by the privilege team as "Legal Mail Approved by Privilege Team" to the detainee without opening the envelope or mailer. If counsel desire confirmation that documents were delivered to the detainee, counsel shall provide a stamped, self-addressed envelope for that purpose. The detainee shall be responsible for mailing any confirmation of delivery to counsel as outgoing legal mail. This method shall be the sole and exclusive means by which confirmation of delivery is provided to counsel.
- e. Written correspondence to detainees not falling within the definition of legal mail shall be sent through the United States Postal Service to the appropriate address provided by DoD. Nonlegal mail includes, but is not limited to, letters from persons other than counsel, including family and friends of the detainee. These non-privileged communications will be reviewed by military personnel at GTMO under the standard operating procedures for detainee nonlegal mail.
- f. Counsel shall treat all information learned from a detainee, including any oral and written communications with a detainee, as classified at the TS/SCI level, unless and until the information is submitted to the Privilege Team and the Privilege Team, this Court, or another court determines it to be otherwise. Accordingly, if counsel's correspondence contains any summary or recitation of or reference to a communication with a detainee that has not been previously determined to be unclassified, the correspondence shall be prepared, marked, transported and handled as classified material as required by Executive Order 13526, DOD Manual 5200.01 (Volumes 1-3), and other applicable DoD security regulations.
- g. Written and oral communications with a detainee, including all incoming legal mail, shall not include any of the following information, in any form, unless directly related to the litigation of this action: (1) information relating to any ongoing or completed military, intelligence, security, or law enforcement operations, investigations, or arrests, or the results of such activities, by any nation or agency; (2) information relating to the current political events in any country; (3) information relating to security procedures at GTMO, including names of U.S. Government personnel and the layout of camp facilities; or (4) information relating to the status of other detainees.

14. Mail Sent by Detainees to Counsel ("Outgoing Mail").

- a. Detainees will be provided with paper to prepare communications to counsel. In the presence of military personnel, the detainee will seal the written communication in an envelope and it will be annotated as "Attorney-Detainee Materials-For Delivery To Counsel." Each envelope shall be labeled with the detainee's and counsel's names and the detainee's ISN. Envelopes annotated with the names of persons other than the detainee's counsel, including family, friends, or other attorneys, shall be processed according to the standard operating procedures for detainee nonlegal mail.
- b. Pending an appropriate classification review through the Privilege Team, any outgoing legal mail will be handled as if it is classified at the TS/SCI level, as defined by the TS/SCI Protective Order.
- c. Military personnel will collect the outgoing legal mail within one business day of being notified by a detainee that the communication is prepared for sealing and mailing.
- d. After outgoing legal mail is collected from a detainee, the envelope will be sealed into a larger envelope by military personnel at GTMO. The larger envelope will be marked as "Attorney-Detainee Materials-For Delivery To Counsel" and will be annotated with the detainee's and counsel's names and the detainee's ISN. The outgoing legal mail will be placed into a courier bag, which will then be locked and hand delivered to a Privilege Team member at GTMO. The Privilege Team member will send all approved legal mail to the secure facility in the Washington, D.C., area via a government-designated courier in a sealed container, in a manner designed to protect the classified material and attorney-client confidentiality. All originals of outgoing legal mail will be stored in a safe located in the secure area at GTMO in a manner designed to protect the classified material and attorney-client confidentiality. The Privilege Team will notify counsel via email when legal mail is received in the Washington, D.C., area.
- e. Detainees also are permitted to send nonlegal mail, including written communications to persons other than counsel, through the United States Postal Service. These communications shall be reviewed by military personnel at GTMO under the standard operating procedures for detainee nonlegal mail.
- f. In the event any nonlegal correspondence or messages from a detainee to individuals other than his counsel, including family, friends, or other attorneys, are sent to counsel as, or included with, legal mail, counsel shall return the documents to military personnel at GTMO for processing according to the standard operating procedures for detainee nonlegal mail.
- g. Classified information may not be sent through nonlegal mail channels.

**E. Materials Brought into Meetings with Detainees and Counsel**

15. Counsel shall bring only approved legal mail, writing utensils, and paper into any

meeting with a detainee, unless counsel receives prior approval from the Commander, JTF-Guantanamo. The Commander shall not unreasonably withhold approval for counsel to bring into a meeting with a detainee letters, tapes, or other communications introducing counsel to the detainee, if the government has first reviewed the communication and determined that sharing the communication with the detainee would not threaten the security of the United States. All legal mail counsel seeks to bring into a meeting with a detainee must be processed under the general review procedures of paragraph D.13 of these Procedures and be submitted to the Privilege Team for review and return at least 14 days prior to counsel's scheduled visit. During a meeting, counsel may provide the detainee with any written documents that were approved to be brought into the meeting. Subject to an appropriate contraband review, the detainee may bring back to his cell all such privileged documents and any documents, notes, and communications created by the detainee and counsel during the course of the meeting.

16. Written and oral communications with a detainee, including all documents brought into a meeting with a detainee, shall not include any of the following information, in any form, unless directly related to the litigation of this action:
  - (1) information relating to any ongoing or completed military, intelligence, security, or law enforcement operations, investigations, or arrests, or the results of such activities, by any nation or agency;
  - (2) information relating to the current political events in any country;
  - (3) information relating to security procedures at GTMO, including names of U.S. Government personnel and the layout of camp facilities; or
  - (4) information relating to the status of other detainees.

#### **F. Materials Brought out of Meetings with Detainees and Counsel**

17. Even if unclassified when brought into meetings, all materials brought out of meetings with detainees and counsel are presumptively TS/SCI. Upon completion of counsel's visit to GTMO, a Privilege Team member at GTMO will review originally unclassified materials brought out of the meeting that were reviewed by the Privilege Team prior to the meeting to determine whether they were modified in any way.
18. Upon completion of each meeting with a detainee or during any break in a meeting session, counsel will give the notes or documents used or produced during the meeting, except those left in the detainee's possession, to a designated individual at GTMO. These materials shall be sealed in counsel's presence and handled as TS/SCI material. If further meetings are scheduled at which some or all of these materials may be used, counsel will identify which materials may be used. The identified materials will be placed in a separate envelope and made available to counsel for use at the next meeting.
19. Upon completion of counsel's visit to GTMO, unclassified materials processed consistent with Paragraph 17 shall be sealed in counsel's presence and placed in an envelope labeled as "Attorney- Detainee Meeting Documents-For Delivery to Counsel." The envelope shall be sealed into a larger envelope marked as "Attorney-Detainee Meeting Documents- For Mail Delivery To Counsel" and annotated with the detainee's and counsel's names and the detainee's ISN. The envelope shall be sealed and, within two business days following completion of counsel's visit to GTMO,

mailed to an address provided by counsel or, if no address is provided, to the secure facility in the Washington, D.C., area. Materials other than unclassified materials also shall be sealed in counsel's presence and placed in an envelope labeled as "Attorney-Detainee Meeting Documents-For Delivery to Counsel." The envelope shall be sealed into a larger envelope marked as "Attorney-Detainee Meeting Documents-For Delivery To Counsel" and annotated with the detainee's and counsel's names and the detainee's ISN. The envelope will be placed into a courier bag, which will then be locked and hand delivered to a Privilege Team member at GTMO. The Privilege Team member will send the materials to the secure facility in the Washington, D.C., area via a government-designated courier in a sealed container, in a manner designed to protect the classified material and attorney-client confidentiality. The original materials will be stored in a safe located in the secure area at GTMO in a manner designed to protect the classified material and attorney-client confidentiality. The Privilege Team will notify counsel via email when the materials are received at the secure facility in the Washington, D.C., area.

20. Correspondence or messages from a detainee to individuals other than his counsel, including family, friends, or other attorneys, will not be handled through this process. If a detainee provides these communications to counsel during a visit, counsel shall give those communications to military personnel at GTMO to be processed under the standard operating procedures for detainee nonlegal mail.

#### **G. Classification Determination of Detainee Communications**

21. Pending an appropriate classification review, all information provided and materials sent by a detainee to counsel or, subject to the review described above, brought out of a meeting by counsel shall be handled and treated as classified at the TS/SCI level.
22. Counsel may submit information learned from a detainee to the Privilege Team located at the secure facility in the Washington, D.C., area for a determination of its appropriate security classification. Counsel shall memorialize the information submitted for classification review into a written memorandum outlining as specifically as possible the information for which counsel requests a classification determination. All documents submitted for classification review shall be transported, prepared, handled, and treated in a secure manner, as required by Executive Order 13526, DOD Manual 5200.01 (Volumes 1-3), and other applicable DoD security regulations. No information derived from these submissions shall be disclosed outside the Privilege Team pursuant to these Procedures until it has been reviewed through the Privilege Team for security and intelligence purposes. With counsel's consent, the Privilege Team may consult with an individual or individuals in appropriate federal agencies for the purpose of identifying classified information and marking documents with the appropriate classification. If counsel does not consent to such consultation, information for which consultation is required will remain classified. Absent express consent of the Court, or except as otherwise provided in these Procedures, the submissions shall not be disclosed to any person involved in the interrogation of a detainee, and no such individual may make any use of those communications, nor shall the submissions be disclosed to any government personnel involved in any domestic or foreign court, military commission, or combatant status tribunal proceedings involving the detainee.

23. Other than information contained in a court filing that is served on government counsel, the Privilege Team shall not disclose outside the Privilege Team any information counsel submit for classification review, except as provided by these Procedures or as permitted by counsel who submitted the information or the Court, or unless the disclosure is to the Special Litigation Team for the purpose of representing the Privilege Team. The Special Litigation Team may not disclose information provided by the Privilege Team or any information counsel provides to the Privilege Team for review, except as provided by these Procedures or as permitted by counsel who submitted the information or the Court. Through the Special Litigation Team, the Privilege Team may inform the Court of any issues or problems related to the release or processing of information related to a case.
24. All materials submitted for classification review must be in legible handwriting or transcribed by typewriter or computer. Materials that are not in English must be accompanied by an English translation. Each page of a document submitted for classification review shall be marked "Attorney-Detainee Materials" and "Classified."
25. As soon as possible after conducting the classification review, the Privilege Team shall advise counsel of the classification levels of the information contained in the materials submitted for review. The Privilege Team shall forward the classification determination directly to counsel after a review and analysis period not to exceed, from the time of receipt by the privilege team:
- a. seven business days for information written in English;
  - b. fourteen business days for any information that includes writing in any language other than English, to allow for translations by the privilege team; and
  - c. twenty business days for any information where the Privilege Team has reason to believe that a code was used, to allow for further analysis.
26. While conducting classification review, the Privilege Team shall promptly report to the Commander, JTF-Guantanamo any information that reasonably could be expected to result in immediate and substantial harm to the national security. In his discretion, the Commander, JTF-Guantanamo may disseminate the relevant portions of the information to law enforcement, military, and intelligence officials, as appropriate.
27. If, at any time, the Privilege Team determines that information in the documents submitted for classification review relates to imminent acts of violence, the Privilege Team shall report the contents of those documents to the Commander, JTF-Guantanamo. In his discretion, the Commander, JTF-Guantanamo may disseminate the relevant portions of the information to law enforcement, military, and intelligence officials, as appropriate.

#### **H. Telephonic Access to Detainees**

28. Requests for telephonic access to a detainee by counsel or other persons normally will not be approved

29. Any telephonic access by counsel is subject to appropriate security procedures. Such procedures shall not include contemporaneous monitoring or recording.
30. Any telephonic access by persons other than counsel is subject to appropriate security procedures, including contemporaneous monitoring and recording

#### **I. Counsel's Handling and Dissemination of Information from Detainees**

31. Subject to the terms of the TS/SCI Protective Order, *see supra* Section I, and any other applicable protective order, counsel may disseminate the unclassified contents of a detainee's communications for purposes reasonably related to their representation of that detainee.
32. Counsel shall treat all information learned from a detainee, including any oral and written communications with a detainee, as information classified at the TS/SCI level, unless and until the information is submitted to the Privilege Team and determined to be otherwise. All classified material must be handled, transported and stored in a secure manner, as provided by Executive Order 13526, DOD Manual 5200.01 (Volumes 1-3), and other applicable DoD security regulations. All documents containing information about or related to materials classified at the TS/SCI level shall be handled in accordance with the security procedures established in the TS/SCI Protective Order and these Procedures. Materials classified at the TS/SCI level shall not be handled by counsel outside the designated areas while at GTMO. All classified material created by counsel or the detainee that relates to a detainee's case shall be transmitted from GTMO to the secure facility in the Washington, D.C., area via a government-designated courier in a sealed container, in a manner designed to protect the classified material and attorney-client confidentiality.
33. Counsel shall disclose to DoJ or Commander, JTF-Guantanamo any information learned from a detainee involving future events that threaten national security or involve imminent violence.
34. Counsel may not divulge classified information not learned from the detainee to the detainee. Counsel may not otherwise divulge classified information related to a detainee's case to any person, except those authorized under these Procedures or the TS/SCI Protective Order, the Court, and government counsel with the requisite security clearance and need to know.

#### **J. JTF-Guantanamo Security Procedures**


35. Counsel shall comply with the following security procedures and force protection safeguards applicable to the U.S. Naval Base in Guantanamo Bay, Cuba, JTF-Guantanamo and the personnel assigned to or visiting these locations, as well as any supplemental procedures implemented by JTF-Guantanamo personnel.
36. Contraband is not permitted in JTF-Guantanamo, and all visitors are subject to search upon arrival and departure. Examples of contraband include, but are not limited to, weapons, chemicals, drugs, and materials that may be used in an escape attempt. Contraband also includes, but is not limited to, money, stamps, cigarettes,

and writing instruments. No items of any kind may be provided to a detainee without the advance approval of the Commander, JTF-Guantanamo.

37. Photography or recording of any type is prohibited without the prior approval of the Commander, JTF-Guantanamo. No electronic communication devices are permitted. All recording devices, cameras, pagers, cellular phones, PDAs, laptops, portable electronic devices and related equipment are prohibited in or near JTF-Guantanamo. Should any of these devices be inadvertently taken into a prohibited area, the device must be surrendered to JTF-Guantanamo staff and purged of all information.
38. Upon arrival at JTF-Guantanamo, security personnel will perform a contraband inspection of counsel using metal detectors, as well as a physical inspection of counsel's bags and briefcases and, if determined necessary, a physical inspection of counsel's persons.
39. Counsel shall not interview or question members of the Joint Task Force about their duties or interactions with detainees without first obtaining permission from the Commander, JTF-Guantanamo. Should permission be unreasonably denied, counsel may seek an order from this Court granting permission for good cause shown.
40. Counsel will meet with detainees in conference facilities provided by GTMO. These facilities are subject to visual monitoring by closed circuit TV for safety and security reasons. The only other method of visual observation available is for the door to remain open with military police sitting outside the door. No oral communications between counsel and the detainees will be heard.
41. At the conclusion of meetings with detainees, counsel will again be inspected using a metal detector and, if deemed necessary, by physical inspection of their persons.

**SO ORDERED.**

2/1/22, 2022

  
\_\_\_\_\_  
Richard J. Leon  
United States District Judge



# Exhibit A

UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

MUSTAFA AHMED AL-HAWSAWI,

Petitioner,

v.

No. 21-cv-2907 (RJL)

JOSEPH R. BIDEN JR. et al.,

Respondents.

MEMORANDUM OF UNDERSTANDING REGARDING ACCESS TO  
CLASSIFIED NATIONAL SECURITY INFORMATION

Having familiarized myself with the applicable statutes, regulations, and orders related to, but not limited to, unauthorized disclosure of classified information, espionage and related offenses; The Intelligence Identities Protection Act, 50 U.S.C. § 421; 18 U.S.C. § 641; 50 U.S.C. § 783; 28 C.F.R. § 17 et seq.; and Executive Order 13526; I understand that I may be the recipient of information and documents that belong to the United States and concern the present and future security of the United States, and that such documents and information together with the methods and sources of collecting it are classified by the United States government. In consideration for the disclosure of classified information and documents:

- (1) I agree that I shall never divulge, publish, or reveal either by word, conduct or any other means, such classified documents and information unless specifically authorized in writing to do so by an authorized representative of the United States government, or as expressly authorized by the TS/SCI Protective Order entered in the United States District Court for the District of Columbia in the above-captioned case(s).
- (2) I agree that this Memorandum of Understanding and any other non-disclosure agreement signed by me will remain forever binding on me.
- (3) I have received, read, and understand the TS/SCI Protective Order entered by the United States District Court for the District of Columbia in the above-captioned case(s), and I agree to comply with the provisions thereof.

Dated: \_\_\_\_\_

# Exhibit B

**EXHIBIT B**

**ACKNOWLEDGMENT**

The undersigned hereby acknowledges that he/she has read the TS/SCI Protective Order entered in *Hawsawi v. Biden*, No. 21-cv-2107 (D.D.C), understands its terms, and agrees to be bound by each of those terms. Specifically, and without limitation, the undersigned agrees not to use or disclose any protected information or documents made available to him/her other than as provided by the TS/SCI Protective Order. The undersigned acknowledges that his/her duties under the TS/SCI Protective Order shall survive the termination of this case and are permanently binding, and that failure to comply with the terms of the Protective Order may result in the imposition of sanctions by the Court.

DATED: \_\_\_\_\_ BY: \_\_\_\_\_  
(type or print name)

SIGNED: \_\_\_\_\_

# Exhibit C

**EXHIBIT C**

**AFFIRMATION**

The undersigned hereby acknowledges that he/she has read the Procedures for Counsel Access to Detainees at the U.S. Naval Base in Guantanamo Bay, Cuba, in Habeas Cases Involving TOP SECRET/SENSITIVE COMPARTMENTED INFORMATION entered in *Hawsawi v. Biden*, No. 21-cv-2107 (D.D.C), understands its terms, and agrees to be bound by each of those terms. The undersigned acknowledges that his/her duties under the Procedures for Counsel Access to Detainees at the U.S. Naval Base in Guantanamo Bay, Cuba, in Habeas Cases Involving TOP SECRET/SENSITIVE COMPARTMENTED INFORMATION shall survive the termination of this case and are permanently binding, and that failure to comply with the terms of the Procedures for Counsel Access to Detainees at the U.S. Naval Base in Guantanamo Bay, Cuba, in Habeas Cases Involving TOP SECRET/SENSITIVE COMPARTMENTED INFORMATION may result in revocation of counsel's security clearance, suspension or termination of counsel's access to the U.S. Naval Base in Guantanamo Bay, Cuba, and/or the imposition of sanctions by the Court.

DATED: \_\_\_\_\_ BY: \_\_\_\_\_  
(type or print name)

SIGNED: \_\_\_\_\_