IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	*	
	*	
v.	*	**CRIMINAL NO. 23-cr-257 (TSC)**
	*	
DONALD J. TRUMP,	*	
	*	
Defendant.	*	
	*	

CIPA PROTECTIVE ORDER PERTAINING TO CLASSIFIED INFORMATION

This matter comes before the Court upon the Government's Unopposed Motion for a Protective Order Pursuant to Section 3 of the Classified Information Procedures Act, 18 U.S.C. App. 3 ("CIPA"), to prevent the unauthorized use, disclosure, or dissemination of classified national security information and documents that will be reviewed by or made available to the defendant and the defendant's attorneys of record (collectively, "the Defense") in this case.[1]

Pursuant to the authority granted under Section 3 of CIPA; the Security Procedures established pursuant to Pub. L. 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information (reprinted following CIPA § 9) ("Security Procedures"); Federal Rules of Criminal Procedure 16(d) and 57; and the general supervisory authority of the Court; and to protect the national security; the Government's motion is GRANTED.

IT IS HEREBY ORDERED:

1. The Court finds that this case will involve classified national security information, the storage, handling, and control of which, by law or regulation, requires special security precautions, and access to which requires a security clearance and a need-to-know.

[1] This Protective Order applies to all of the defendant's counsel of record, both current and future, who possess or acquire the requisite clearance. Only the defendant and the defendant's counsel of record who possess the requisite clearance may have access to classified information.

2. The purpose of this Protective Order ("Order") is to establish the procedures that must be followed by the Defense, any court personnel, and all other individuals who receive access to classified information or documents in connection with this case.

3. The procedures set forth in this Order shall apply to all pre-trial, trial, post-trial, and appellate aspects of this case and may be modified by further order of the Court acting under Federal Rules of Criminal Procedure 16(d), Sections 3 and 9 of CIPA, and this Court's inherent supervisory authority to ensure a fair and expeditious trial.

Definitions

4. The terms "classified national security information and documents," "classified information," "classified documents," and "classified materials" refer to:

a. Any classified document or information that has been classified by any Executive Branch agency in the interest of national security or pursuant to Executive Order 13526 or its predecessor orders as "CONFIDENTIAL," "SECRET," "TOP SECRET," or additionally controlled as "SENSITIVE COMPARTMENTED INFORMATION" ("SCI");

b. Any document, recording, or information, now or formerly in the possession of a private party, that: (i) has been derived from information that has been classified by the U.S. Government, and/or (ii) has been classified by the U.S. Government as set forth above;

c. Classified information known to the Defense; and

d. Any document or information that the Defense has been notified by the Government in writing contains classified information;

5. The words "documents," "information," and "materials" shall 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 and graphs, interoffice and intra-office communications, notations of any sort concerning meetings or communications of any kind, bulletins, teletypes, telegrams and telefacsimiles, invoices, and worksheets, as well as 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, films, typewriter ribbons, word processing or other computer tapes or disks, and all manner of electronic data processing storage; and

d. Information acquired orally.

6. "Access to classified information" means having access to, reviewing, reading, learning, or otherwise coming to know in any manner any classified information.

7. "Secure Area" shall mean a sensitive compartmented information facility ("SCIF") approved by a Classified Information Security Officer ("CISO") for the storage, handling, and control of classified information.

8. All classified documents or material and the information contained therein shall

remain classified unless the documents or material bear a clear indication that they have been declassified by the agency or department that is the originating agency ("Originating Agency") of the document, material, or information contained therein.

9. Any classified information provided by the Government to the Defense is to be used solely by the Defense to prepare a defense in this case. The Defense may not disclose or cause to be disclosed in connection with this case any information known or reasonably believed to be classified information except as otherwise provided in this Order.

10. Classified Information Security Officer. In accordance with the provisions of CIPA and the Security Procedures, the Court designates for this case a CISO and Alternate CISOs, who are identified in a sealed order made available to the parties, for the purpose of providing security arrangements necessary to protect from unauthorized disclosure any classified information to be made available in connection with this case. The Defense shall seek guidance from the CISO with regard to appropriate storage, handling, transmittal, and use of classified information.

11. Government Attorneys. The Court has been advised that the Government attorneys working on this case have, or can expeditiously acquire, the requisite security clearances to have access to the classified information that relates to this case.

12. Protection of Classified Information. The Court finds that, in order to protect the classified information involved in this case, only the Government attorneys; appropriately cleared Department of Justice employees; personnel of the Originating Agency; cleared court personnel; and the Defense shall have access to the classified information in this case. Neither the defendant nor the defendant's counsel of record shall have access to any classified documents and information in this case unless such person shall first have:

a. Received permission of the Government or, where necessary, the Court

through a separate Court order; and

b. Received the necessary security clearance at the appropriate level of classification, through or confirmed by the CISO.

13. The Defense. Subject to the provisions of this Order, the Defense may be given access to classified information as required by the Government's discovery obligations. Any additional person whose assistance the Defense reasonably requires may have access to classified information in this case only after obtaining from the Court an approval for access to the appropriate level of classification on a need-to-know basis and after satisfying the other requirements described in this Order for access to classified information. The substitution, departure, or removal for any reason from this case of the defendant's counsel of record shall not release that person from the provisions of this Order.

14. Unless they already hold an appropriate security clearance and are approved for access to classified information in this case, the Defense shall complete and submit to the CISO a Standard Form 86 (Questionnaire For National Security Positions), attached releases, and "major case" fingerprints in order to obtain security clearances necessary for access to classified information that may be involved in this case. The CISO shall provide access to the necessary forms. The CISO shall take all reasonable steps to ensure the prompt processing of all security clearance applications.

15. Secure Area of Review. The CISO shall arrange for an appropriately approved Secure Area for use by the Defense. The CISO shall establish procedures to assure that the Secure Area is accessible to the Defense during normal business hours, after hours, and on weekends, in consultation with the United States Marshals Service, and once the Defense is approved for such access. The Secure Area shall contain a separate working area for the Defense and will be outfitted

with any secure office equipment requested by the Defense that is reasonable and necessary to the preparation of the defense in this case. The CISO, in consultation with the Defense, shall establish procedures to assure that the Secure Area may be maintained and operated in the most efficient manner consistent with the protection of classified information. No documents or other material containing classified information may be removed from the Secure Area unless authorized by the CISO. The CISO shall neither reveal to the Government the content of any conversations the CISO may hear among the Defense, nor reveal the nature of documents being reviewed by them, nor the work generated by them. In addition, the presence of the CISO shall not operate to waive, limit, or otherwise render inapplicable the attorney-client privilege.

16. Filings with the Court. Until further order of this Court, any motion, memorandum, or other document the parties file that counsel knows, or has reason to believe, contains classified information in whole or in part, or any document the proper classification of which counsel is unsure, shall be filed under seal with the Court through the CISO, or an appropriately cleared designee of the CISO's choosing. Pleadings filed under seal with the CISO shall be marked "Filed In Camera and Under Seal with the Classified Information Security Officer" and shall include in the introductory paragraph a statement that the item is being filed under seal pursuant to this Order, but need not be accompanied by a separate motion to seal. The date and time of physical submission to the CISO or a designee, which should occur no later than 4:00 p.m., shall be considered as the date and time of court filing. At the time of making a physical submission to the CISO or the CISO's designee, counsel shall file on the public record in the CM/ECF system a notice of filing. The notice should contain only the case caption and an unclassified title in the filing. The CISO shall arrange for prompt delivery, under seal, to the Court and opposing counsel (unless *ex parte*) any document to be filed by the parties that potentially contains classified

information. The CISO shall promptly consult with representatives of the appropriate agencies to determine whether the pleading or document contains classified information. If it is determined that the pleading or document contains classified information, the CISO shall ensure that that portion of the pleading or document, and only that portion, is marked with the appropriate classification markings and that the pleading or document remains under seal. The CISO also shall promptly provide the Defense with a properly marked pleading or document.

17. Sealing of Records. The CISO shall maintain a separate sealed record for those pleadings containing classified materials and retain such record for purposes of later proceedings or appeal.

18. Access to Classified Information. The Defense shall have access to classified information only as follows:

a. All classified information produced by the Government to the Defense, in discovery or otherwise, and all classified information possessed, created, or maintained by the Defense shall be stored, maintained, and used only in the Secure Area established by the CISO;

b. The Defense shall have free 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. However, the Defense shall not, except under separate Court order, disclose the classified information, either directly, indirectly, or in any other manner which would disclose the existence of such classified information;

c. Except as outlined in Paragraph 18(b), the Defense shall not copy or reproduce any classified information in any form, except with the approval

of the CISO, or in accordance with the procedures established by the CISO for the operation of the Secure Area;

d. All documents prepared by the Defense (including, without limitation, pleadings or other documents intended for filing with the Court) that do or may contain classified information, other than Court filings submitted in accordance with Paragraph 16, shall be transcribed, recorded, typed, duplicated, copied, or otherwise prepared only by persons who have received an appropriate approval for access to classified information and only in the Secure Area on equipment approved for the processing of classified information and in accordance with the procedures established by the CISO. All such documents and any associated materials (such as notes, drafts, copies, typewriter ribbons, magnetic recordings, exhibits, etc.) containing classified information shall be maintained in the Secure Area unless and until the CISO determines that those documents or associated materials are unclassified in their entirety. None of these materials shall be disclosed to counsel for the Government;

e. The Defense shall discuss classified information only within the Secure Area or in another area authorized by the CISO and shall not discuss or attempt to discuss classified information over any telephone instrument or communication system, including through electronic mail or the Internet; and

f. The Defense shall not disclose, without prior approval of the Court, any classified information to any person not authorized pursuant to this Order,

including defense witnesses, except to the Court, court personnel, and the Government attorneys who have been identified by the CISO as having the appropriate clearances and the need-to-know that information. Government counsel shall be given the opportunity to be heard in response to any defense request for disclosure to a person not named in this Order. Any person approved by the Court for disclosure under this paragraph shall be required to obtain the appropriate security clearance and to comply with all terms and conditions of this Order. If the preparation of the defense requires that classified information be disclosed to persons not named in this Order, then, upon further order of the Court, the CISO shall promptly seek to obtain security clearances for them.

g. Information that is classified that also appears in the public domain is not thereby automatically declassified unless it appears in the public domain as the result of an official statement by a U.S. Government Executive Branch official who is authorized to declassify the information. Individuals who by virtue of this Order or any other Court order are granted access to the classified information may not confirm or deny classified information that appears in the public domain. Prior to any attempt by the Defense to have such information confirmed or denied at trial or in any public proceeding in this case, the Defense must comply with the notification requirements of Section 5 of CIPA and all the provisions of this Order.

h. In the event that classified information enters the public domain, the Defense is precluded from making private or public statements where the

statements would reveal personal knowledge from non-public sources regarding the classified status of the information or would disclose that the Defense had personal access to classified information confirming, contradicting, or otherwise relating to the information already in the public domain.

19. Procedures for public disclosure of classified information in this case shall be those established by CIPA. The Defense shall comply with the requirements of CIPA § 5 prior to any disclosure of classified information during any proceeding in this case. As set forth in Section 5, the Defense shall not disclose any information known or believed to be classified in connection with any proceeding until notice has been given to Government counsel and until the Government has been afforded a reasonable opportunity to seek a determination pursuant to the procedures set forth in CIPA § 6, and until the time for the Government to appeal any adverse determination under CIPA § 7 has expired or any appeal under that section is decided. Any conferences with the Court involving classified information shall be conducted *in camera* in the interest of the national security, be attended only by persons granted access to classified information and a need-to-know, and the transcripts of such proceedings shall be maintained under seal.

20. Violations of this Order. Unauthorized use or disclosure of classified information may constitute violations of United States criminal laws. In addition, violation of the terms of this Order shall be brought immediately to the attention of the Court and may result in a charge of contempt of Court and possible referral for criminal prosecution. Any breach of this Order will result in the termination of a person's access to classified information. Persons subject to this Order are advised that direct or indirect unauthorized use, disclosure, retention, or negligent handling of classified information could cause serious damage, and in some cases exceptionally

grave damage, to the national security of the United States, or may be used to the advantage of a foreign nation against the interests of the United States. This Order is to ensure that those authorized by the Order to receive classified information will never divulge the classified information disclosed to them to anyone who is not authorized to receive it or otherwise use the classified information without prior written authorization from the Originating Agency and in conformity with this Order.

21. All classified information to which the Defense has access in this case is now and will remain the property of the United States. The Defense and anyone else who receives classified information pursuant to this Order shall return all such classified information in their possession obtained through discovery from the Government in this case, or for which they are responsible because of access to classified information, to the CISO upon request. The notes, summaries, and other documents prepared by the Defense that do or may contain classified information shall remain at all times in the custody of the CISO for the duration of this case. At the conclusion of all proceedings, including any final appeals, all such notes, summaries, and other documents are to be destroyed by the CISO, in the presence of the Defense if so desired.

22. Nothing in this Order shall preclude the Government from seeking a further protective order pursuant to CIPA and/or Rules 16(d) or 57 of the Federal Rules of Criminal Procedure as to particular items of discovery material.

SO ORDERED this 22 day of August 2023.

Tanya S. Chutkan

TANYA S. CHUTKAN
UNITED STATES DISTRICT JUDGE