UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
WEST PALM BEACH DIVISION

CASE NO. 23-80101-CR-CANNON-2

UNITED STATES OF AMERICA,

Plaintiff,

v.

WALTINE NAUTA,

Defendant.
_____/

PROTECTIVE ORDER PERTAINING TO CLASSIFIED INFORMATION DISCLOSED TO WALTINE NAUTA AND DEFENSE COUNSEL

THIS MATTER comes before the Court upon the Government's Renewed Motion for Protective Order pursuant to Section 3 of the Classified Information Procedures Act, Pub. L. 96-456, 94 Stat. 2025, 18 U.S.C. App. III § 3 (1980) ("CIPA § 3"), to prevent the unauthorized use, disclosure, or dissemination of classified national security information and documents that will be reviewed by or made available to, or are otherwise in the possession of, Defendant[1] and defense counsel in this case.[2] A sealed hearing was held on the Motion on September 12, 2023 [ECF No. 149].

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

[1] For purposes of this Order, "Defendant" refers to Waltine Nauta.

[2] This Order is entered without prejudice to any potential "[c]onstitutional and statutory challenges to the authority of the Special Counsel to maintain this action, to the "purported classification of certain documents at issue in this action," or to any arguments implicating the Presidential Records Act, 44 U.S.C. §§ 2201–09 [ECF No. 66 pp. 7–8].

the Protection of Classified Information (reprinted following CIPA § 9) (hereinafter the "Security Procedures"), Rules 16(d) and 57 of the Federal Rules of Criminal Procedure, the general supervisory powers of the Court; and, in order to protect the national security, the Government's Motion is **GRANTED** in accordance with this Order and as discussed during the hearing, and the following Protective Order is entered:[3]

1. The Court finds that this case will involve information that has been classified in the interest of national security. The storage, handling, and control of this information will require special security precautions mandated by statute, executive order, and regulation.[4]

2. The purpose of this Protective Order ("Order") is to establish the procedures that must be followed by Defendant, defense counsel, the parties, and all other individuals who receive access to classified information or documents in connection with this case. The procedures set forth in this Order shall apply to all pre-trial, trial, post-trial, and appellate matters concerning classified information in this case and may be modified from time to time by further order of the Court acting under this Court's inherent supervisory authority to ensure a fair and expeditious trial. The limitations on disclosure of classified information set forth in this Order are binding on Defendant and his counsel, and violations may result in criminal and/or civil penalties. The government and the defense may also move for modification of this Order at any time for good cause shown.

3. Definitions. The following definitions shall apply to this Order:

[3] The Court understands that the government may move for supplemental protective orders pursuant to CIPA and the Federal Rules of Criminal Procedure.

[4] Any individual to whom classified information is disclosed pursuant to this Order shall not disclose such information to another individual unless the U.S. agency that originated that classified information has validated that the proposed recipient possesses an appropriate security clearance and need-to-know.

a. "Government" or "the government" refers collectively to the Special Counsel for the United States Department of Justice and its prosecutors and support staff, as well as any law enforcement or intelligence community employees assisting in the prosecution of this matter.

b. "Defense" or "defense team" refers collectively to the Defendant's counsel and any support staff assisting the Defendant's counsel authorized to receive classified information pursuant to this Order.[5]

c. "Classified information" shall include:

i. Any document, recording, or information that has been classified by any Executive Branch agency in the interests of national security pursuant to Executive Order 13526 (or successor order), as amended, or its predecessor or successor orders, or under the Atomic Energy Act (AEA), 42 U.S.C. § 2011, *et seq.*, as "CONFIDENTIAL," "SECRET," "TOP SECRET," or "FORMERLY RESTRICTED DATA," or additionally controlled as "SENSITIVE COMPARTMENTED INFORMATION" ("SCI");

ii. Any document, recording, or information now or formerly in the possession of a private party that (A) has been classified by the United States Government as set forth above, and/or (B) has been derived from information that is classified by the United States Government;

[5] This Protective Order will apply to all defense counsel, both current and future, who possess the requisite clearance. Only defense counsel who possess the requisite clearance will have access to classified information.

iii. Verbal or other unwritten or unrecorded information known to the Defendant or the defense team that has been classified by the United States Government as set forth above;

iv. Any information, regardless of its origin, that the defense knows or reasonably should know contains classified information, including information acquired or conveyed orally;

v. Any document, recording, or information as to which the defense has been notified orally or in writing contains classified information; and

vi. Any document, recording, or information that is classified, as set forth in (i), that has been approved by the United States government for limited authorized disclosure to defense counsel in criminal case *United States v. Trump et al.*, 23-80101-CR-CANNON, pursuant to the restrictions set forth herein, along with the singular document described in paragraph 26.j below to be disclosed to Defendant, also subject to those same restrictions.[6]

d. "Document," "materials," and "information" shall include, but are not limited to:

[6] In the event that the government's discovery obligations require disclosure of government information that is not marked as classified but has been deemed to be classified, the government will inform defense counsel specifically what the information is and, if known, the level of classification. If the government is disclosing information that it has reason to believe is classified but the classification review for that information has not been completed, the government will inform the defense that information must be handled as classified, consistent with this Order, unless and until the government confirms that it is not classified. If the Court or a party to the case seeks to use or disclose information that has not been formally reviewed for classification, the Court and the parties shall address such use or disclosure pursuant to CIPA.

i. All written, printed, visual, digital, electronic, or audible 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), as well as metadata;

ii. Notes (handwritten, oral, or electronic); papers; letters; correspondence; memoranda; reports; summaries; photographs; maps; charts; graphs; inter-office communications; notations of any sort concerning conversations, meetings or other communications; bulletins; teletypes; telecopies; telegrams; telexes; transcripts; cables; facsimiles; invoices; worksheets and drafts; microfiche; microfilm; videotapes; sound recordings of any kind; motion pictures; 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, disks, or thumb drives and all manner of electronic data processing storage; and alterations, modifications, changes and amendments of any kind to the foregoing; and

iii. Information obtained orally.

e. "Access to classified information" shall mean having access to, reviewing, reading, learning, or otherwise coming to know in any manner classified information.

f. "SCIF" shall refer to a sensitive compartmented information facility approved by a designated CISO for the storage, handling, and control of classified information.

Classified Information

4. 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 of the document, material, or information contained therein.

5. All access to classified information shall conform to this Order.

6. The Defendant may disclose classified information to the defense as necessary for the preparation of his defense. Any classified information provided to the defense by the government or the Defendant is to be used solely by the defense and solely for the purpose of preparing the defense.

7. 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 herein. If the defense or the Defendant have any question regarding the disclosure of classified information, they shall consult with the CISO.

8. The defense may not disclose classified information to Defendant except as set forth in paragraph 26.j. or as permitted by any supplemental order. Any classified information the defense discusses with the Defendant in any way shall be handled in accordance with this Order, including such requirements as confining all discussions, documents, and materials to an accredited SCIF or other location authorized by the CISO.

9. The defense and the Defendant shall not disclose classified information to any person, except to the Court, government personnel who hold appropriate security clearances and have been determined to have a need-to-know that information, and those specifically authorized to access that information pursuant to this Order.

10. 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 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 in any public proceeding in this case, the defense must comply with the notification requirements of Section 5 of CIPA and all provisions of this Order.

11. If classified information enters the public domain, the defense and the Defendant are 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. If there is any question whether information is classified, the defense must handle that information as though it is classified unless counsel for the government or the CISO confirms that it is not classified.

Security Procedures

12. In accordance with the provisions of CIPA and the Revised Security Procedures, the Court has designated a CISO and alternate CISOs for this case [ECF No. 40], for the purpose of providing security arrangements necessary to protect against unauthorized disclosure of any classified information that has been made available to the Defendant and the defense 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.

13. The government has advised the Court that certain attorneys working on this case for the Office of the Special Counsel, including Counselor to the Special Counsel Jay I. Bratt, Assistant Special Counsels Julie A. Edelstein, David V. Harbach, II, Karen E. Gilbert, Michael Thakur, John Pellettieri, and their supervisors, have the requisite security clearances to have access to the classified information that counsel for the government intend to use, review, or disclose in this case.

14. The Court has been advised, through the CISO, that Defendant's counsel of record, possess at least interim security clearances, permitting them to have access to classified information designated as "CONFIDENTIAL," "SECRET," or "TOP SECRET," including (upon read-ins) the following SCI compartments: SI, SI-G, and TK, for which they have a need-to-know.[7]

15. *Protection of Classified Information*. The Court finds that, to protect the classified information involved in this case, to the extent that counsel have the requisite security clearances and a "need-to-know" the classified information, they shall be given authorized access to classified national security documents and information as required by the government's discovery obligations and subject to the terms of this Protective Order, the requirements of CIPA, and any other Orders of this Court.

16. The Defendant may have a continuing contractual obligation to the government not to disclose to any unauthorized person classified information known to them or in their possession. The government is entitled to enforce that agreement to maintain the

[7] Once counsel receive final clearances, they will promptly receive additional read-ins, at which time they will also be able to access additional SCI compartments for which they have a need-to-know.

confidentiality of classified information. The defense and the Defendant are subject to this Court's authority, contempt powers, and other authorities, and shall fully comply with any nondisclosure agreements he has signed, this Order, and applicable statutes.

17. No court personnel required by this Court for its assistance shall have access to classified information involved in this case unless that person shall first have received the necessary security clearance as determined by the CISO.

18. Any additional persons whose assistance the defense reasonably requires may have access to classified information in this case only if they are granted an appropriate security clearance through the CISO, obtain approval from this Court with prior notice of the identity of the additional persons to the U.S. government, and satisfy the other requirements described in this Order for access to classified information.

19. An individual with a security clearance and a need-to-know as determined by any government entity is not automatically authorized to disclose any classified information to any other individual, even if that other individual also has a security clearance. Rather, any individual who receives classified information may only disclose that information to an individual who has been determined by the CISO, in consultation with the appropriate government entity, to have both the required security clearance and a need-to-know the information.

20. Defendant's counsel and the Defendant agree they are subject to the terms of this Protective Order and any other Orders of this Court. The substitution, departure, or removal for any reason from this case of any counsel for the Defendant or any other member of the defense, shall not release that individual from the provisions of this Order.

21. *Secure Area of Review*. The CISO shall establish procedures to assure a SCIF is accessible

during business hours to the defense, and at other times upon reasonable request as approved by the CISO in consultation with the Court and United States Marshals Service. The SCIF shall contain a 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 Defendant's case. The CISO, in consultation with counsel for the Defendant, shall establish procedures to assure that the SCIF may be maintained and operated in the most efficient manner consistent with the protection of classified information and in compliance with security requirements. No classified documents, material, recordings, or other information may be removed from the SCIF unless so authorized by the CISO. Should the CISO overhear any defense conversations or see any defense work product (excluding filings intended to be provided to the Court and the government), the CISO shall not reveal to the government (or anyone else) the content of any conversations they may overhear among the defense, the nature of the documents being reviewed, or the work being generated. The presence of the CISO or any of his designees shall not operate to waive, limit, or otherwise render inapplicable, the attorney-client privilege.

22. *Filings with the Court*. Any pleading or other document filed by the defense that Defendant's counsel knows or reasonably should know contains classified information as defined in paragraph 3(c) shall be filed as follows:

a. Pleadings and other documents shall be filed under seal with the CISO or an appropriately cleared designee and shall be marked, "Filed in Camera and Under Seal with the Classified Information Security Officer." The time of physical submission to the CISO or an appropriately cleared designee shall be

considered the date and time of filing and should occur no later than 5:00 p.m. Within a reasonable time after making a submission to the CISO or an appropriately cleared designee, the defense 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 or an appropriately cleared designee. The notice should contain only the case caption and an unclassified title of the filing.

b. The CISO or an appropriately cleared designee shall immediately deliver under seal to the Court and counsel for the government any pleading or document to be filed by the defense that contains classified information, unless the pleading or document is an *ex parte* and in camera filing. 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 the pleading or document is marked with the appropriate classification markings and that the pleading or document remains under seal.

23. *Filing of Papers by the Government*. Any pleading or other document filed by the government that counsel for the government knows or reasonably should know contains classified information as defined herein, shall be filed as follows:

a. The document shall be filed under seal with the CISO or an appropriately cleared designee and shall be marked, "Filed in Camera and Under Seal with the Classified Information Security Officer." The time of physical submission to the CISO or an appropriately cleared designee shall be considered the date and time of filing and should occur no later than 5:00 p.m. Within a

reasonable time after making a submission to the CISO, counsel for the government 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. The notice should contain only the case caption and an unclassified title of the filing.

b. The CISO shall immediately deliver under seal to the Court and counsel for the defense any pleading or document to be filed by the government that contains classified information, unless the pleading or document is an *ex parte* filing.

24. *Record and Maintenance of Classified Filings*. The CISO shall maintain a separate sealed record for those materials which are classified. The CISO shall be responsible for maintaining the secured records for purposes of later proceedings or appeal.

25. *The Classified Information Procedures Act*. 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 Section 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 counsel for the government and until the government has been afforded a reasonable opportunity to seek a determination pursuant to the procedures set forth in CIPA Section 6, and until the time for the government to appeal any adverse determination under CIPA Section 7 has expired or any appeal under Section 7 by the government 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.

26. *Access to Classified Information*. In the interest of the national security, representatives of the defense granted access to classified information shall have access to classified information only as follows:

a. All classified information produced, possessed, created or maintained by the defense, including notes and any other work product, and all classified information disclosed by the United States government to the defense, shall be stored, maintained and used only in the SCIF established by the CISO, unless otherwise authorized by the CISO.

b. *Special procedures for audio recordings*. Any classified audio recordings that the government discloses to the defense shall be maintained by the CISO in the SCIF. Such recordings may only be reviewed on a stand-alone, non-networked computer or other device within the SCIF that does not have the capability to duplicate or transmit information. The defense must use headphones to review such recordings, and the headphones must be wired and not have any wireless capability.

c. The defense shall have free access to the classified information in the SCIF established by the CISO and shall be allowed to take notes and prepare documents with respect to those materials.

d. The defense shall not copy or reproduce any classified information in any manner or form, except with the approval of the CISO and in accordance with the procedures established by the CISO for the operation of the SCIF.

e. 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 must be prepared in the SCIF on word processing equipment approved by the CISO. All such documents and any associated materials (such as notes, drafts, copies, typewriter ribbons, magnetic recordings, exhibits, thumb drives, discs, CDs, DVDs exhibits, and electronic or digital copies) that may contain classified information shall be maintained in the SCIF unless and until the CISO determines those documents or associated materials are unclassified in their entirety, or if secure removal is authorized by the CISO. None of these materials shall be disclosed to counsel for the government or any other party.

f. The defense shall discuss classified information only within the SCIF or in an area authorized by the CISO.

g. The defense shall not disclose, without prior approval of the Court, classified information to any person not named in this Order except to the Court, Court personnel, and government personnel identified by the CISO as having the appropriate clearances and the need-to-know. Counsel for the government shall be given an opportunity to be heard in response to any defense request for disclosure to a person not identified in this Order. Any person approved by this Court for access to classified information under this paragraph shall be required to obtain the appropriate security clearance and to comply with all the terms and conditions of the Order. As set forth above, the defense shall not disclose classified information, even to an individual with the appropriate security clearance, without following the procedures referenced in this Order.

h. The defense shall not discuss classified information over any standard

commercial telephone instrument or office intercommunication systems, including but not limited to the Internet and electronic mail, or in the presence of any person who has not been granted access to classified information by the Court.

i. Any documents written by the defense that do or may contain classified information shall be transcribed, recorded, typed, duplicated, copied, or otherwise prepared only by persons who have received an appropriate approval for access to classified information.

j. The government agrees to disclose to Defendant as classified information only "the unredacted version of the picture included in paragraph 32 of the Superseding Indictment and the document charged in Count 8" [ECF No. 85 pp. 13–14, 33; ECF No. 120 p. 7]. Any future disclosures of classified information to Defendant shall be governed by subsequent order.

27. Any unauthorized disclosure or mishandling of classified information may constitute violations of federal criminal law. In addition, any 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 may also result in termination of an individual's access to classified information. Persons subject to this Order are advised that direct or indirect unauthorized disclosure, retention or handling of classified documents or 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. The purpose of this Order is to ensure that those authorized to receive classified

information in connection with this case will never divulge that information to anyone not authorized to receive it.

28. All classified documents and information to which the defense has access in this case are now and will remain the property of the United States. Upon demand of the CISO, all persons shall return to the CISO all 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. 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 the case. At the conclusion of this case, including any appeals or ancillary proceedings thereto, all such notes, summaries, and other documents are to be destroyed by the CISO in the presence of counsel for the Defendant if they choose to be present.

29. Nothing contained in this Order shall be construed as a waiver of any right of the Defendant. No admission made by the Defendant or his counsel during pretrial conferences may be used against the Defendant unless it is in writing and signed by the Defendant. *See* CIPA § 2.

30. A copy of this Order shall be issued forthwith to counsel for the Defendant who shall be responsible for advising the Defendant and representatives of the defense of the contents of this Order.

SO ORDERED in Chambers at Fort Pierce, Florida, this 13th day of September 2023.

HON. AILEEN M. CANNON
UNITED STATES DISTRICT COURT JUDGE

cc: counsel of record