IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	**No. 1:21-cr-245 (AJT)**
	)	
IGOR Y. DANCHENKO,	)	
	)	
Defendant.	)	

PROTECTIVE ORDER
PERTAINING TO CLASSIFIED INFORMATION

This matter comes before the Court upon the United States' *Consent Motion for Protective Order Pursuant To Section 3 of the Classified Information Procedures Act*. Pursuant to the authority granted under Section 3 of CIPA, the "Revised 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" ("Security Procedures") (reprinted after CIPA § 9), Rules 16 and 57 of the Federal Rules of Criminal Procedure, and the general supervisory powers of the Court, and to protect the national security, the following Protective Order is entered:

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, and access to this information requires appropriate security clearances and need-to-know, as set forth in Executive Order 13256 (or successor order), that has been validated by the Government.[1] The purpose of this

[1] 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

Order is to establish procedures that must be followed by counsel and the parties in this case. These procedures will apply to all pretrial, trial, post-trial, and appellate matters concerning classified information and may be modified from time to time by further Order of the Court acting under its inherent supervisory authority to ensure a fair and expeditious trial.

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

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

b. "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, as amended, or its predecessor or successor orders, as "CONFIDENTIAL," "SECRET," "TOP SECRET," 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 derived from information that was classified by the United States Government, and/or (B) has been classified by the United States Government as set forth above;

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

---

information has validated that the proposed recipient possesses an appropriate security clearance and need-to-know.

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

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

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

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.

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

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

Classified Information

3. All classified documents, and classified information contained therein, shall remain classified unless the documents bear a clear indication that they are not classified or have been declassified by the agency or department that originated the document or information contained therein ("originating agency").

4. All access to classified information shall conform to this Order and the Memorandum of Understanding described herein.

5. Any classified information provided to the Defense by the Government is to be used solely by the Defense and solely for the purpose of preparing the defense. 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.

6. Any classified information the Defense discloses to or discusses with the Defendant in any way shall be handled in accordance with this Order and the attached Memorandum of Understanding, including such requirements as confining all discussions, documents, and materials to an accredited SCIF.

7. The Defense 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.

8. 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 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 provisions of this Order.

9. 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. If there is any question as to whether information is classified, the Defense must handle that information as though it is classified unless counsel for the Government confirms that it is not classified.

Security Procedures

10. In accordance with the provisions of CIPA and the Security Procedures, the Court has designated Harry Rucker as the CISO and Daniel Hartenstine, Matthew W. Mullery, Carli Rodriguez-Feo, Daniella Medel, and W. Scooter Slade, as alternate CISOs for this case, for the purpose of providing security arrangements necessary to protect against unauthorized disclosure of

any classified information that has been made available to 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.

11. The Government has advised the Court that Assistant Special Counsels Andrew DeFilippis, Michael Keilty, Jonathan Algor, and Neeraj Patel, and U.S. Department of Justice National Security Division attorney Adam Small, as well as their supervisors ("counsel for the Government"), have the security clearances allowing them to have access to classified information that counsel for the Government intend to use, review, or disclose in this case.

12. The Court has been advised, through the CISO, that Defense team members Stuart A. Sears, Esq. and Danny C. Onorato, Esq. have been granted security clearances permitting them to have access to the classified information that counsel for the Government intend to use and disclose pursuant to this Order. Further, the Court has been advised that Defense team member Grace McMahon (paralegal) is in the process of obtaining the relevant security clearances.

13. *Protection of Classified Information*. The Court finds that to protect the classified information involved in this case, to the extent that the Defense team members 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, the Memorandum of Understanding attached hereto, and any other Orders of this Court.

14. As set forth in the Government's motion, the Defendant has a continuing contractual obligation to the Government not to disclose to any unauthorized person classified information known to him or in his possession. The Government is entitled to enforce that agreement to maintain

the confidentiality of classified information. Moreover, the Defendant must sign the Memorandum of Understanding. In addition, the Defendant is subject to this Court's authority, contempt powers, and other authorities, and shall fully comply with the nondisclosure agreements he has signed, this Order, the Memorandum of Understanding, and applicable statutes.

15. The signed original Memorandum of Understanding shall be filed with the Court under seal and executed copies of the Memorandum of Understanding shall be served upon the CISO and the Government. The substitution, departure, or removal for any reason from this case of counsel for the Defendant or any other member of the Defense team, shall not release that individual from the provisions of this Order or the Memorandum of Understanding executed in connection with this Order.

16. Pursuant to Section 4 of the security procedures promulgated pursuant to CIPA, 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.

17. Any additional persons whose assistance the Defense reasonably requires may only have access to classified information in this case 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 agency that originated the information, and satisfy the other requirements described in this Order for access to classified information.

18. 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 an appropriate Government entity to have both the required security clearance and a need-to-know the information.

19. *Secure Area for the Defense*. The Court is informed that the CISO has arranged for an approved Secure Area that has been accredited by the U.S. Intelligence Community for use by the Defense. The CISO shall establish procedures to assure the Secure Area is accessible during business hours to the Defense, and at other times upon reasonable request as approved by the CISO in consultation with the United States Marshals Service. 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. The CISO, in consultation with counsel for the Defendant, 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 and in compliance with accreditation requirements. No classified documents, material, recordings, or other information may be removed from the Secure Area unless so authorized by the CISO. Subject to the prior authorization of the CISO, the Defense shall be permitted to bring materials into the Secure Area for use in its work, and the Defense shall be permitted to remove unclassified materials from the Secure Area, including its unclassified notes and other work product, subject to inspection by the CISO. The CISO shall not reveal to the Government the content of any conversations he may hear among the Defense, nor reveal the nature of the documents being reviewed, or the work being generated. The presence of the CISO shall not operate to render inapplicable the attorney-client privilege or any other applicable privileges or related protections.

20. *Filing of Papers by the Defense*. Any pleading or other document filed by the Defense that counsel for the Defendant knows or reasonably should know contains classified information as defined in paragraph 2(a), 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 4:00 p.m. Within a reasonable time after making a submission to the CISO, 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. The notice should contain only the case caption and an unclassified title of the filing.

b. 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. The CISO 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* filing.

21. *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 in paragraph 2(a), 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 4:00 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 ensure the document is marked with the appropriate classification marking and remains under seal. 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.

22. *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.

23. *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. Pretrial conferences 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.

24. *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 by the Government to counsel for the Defendant in discovery or otherwise, and all classified information possessed, created or maintained by the Defense, including notes and any other work product, shall be stored, maintained and used only in the Secure Area 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 Secure Area. Such recordings may only be reviewed on a stand-alone, non-networked computer or other device within the Secure Area 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 made available to them in the Secure Area established by the CISO and shall be allowed to take notes and prepare documents with respect to those notes.

d. No representative of the Defense (including, but not limited to, counsel, investigators, paralegals, translators, experts and witnesses) shall 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 Secure Area.

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 Secure Area 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 Secure Area unless and until the CISO determines those documents or associated materials are unclassified in their entirety. 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 Secure Area 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, to sign and submit to this Court the Memorandum of

Understanding appended to the Order, and to comply with all the terms and conditions of the Order. If preparation of the Defense requires that classified information be disclosed to persons not named in this Order, the Department of Justice shall promptly seek to obtain security clearances for them at the request of Defense counsel. As set forth above, the Defense shall not disclose classified information, even to an individual with the appropriate security clearance, without following the procedure referenced in paragraph 17.

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 ("email"), 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.

25. 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.

26. 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.

27. 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.

28. A copy of this Order shall be issued forthwith to the Defense, and counsel for the Defendant shall be responsible for advising representatives of the Defense regarding the contents of this Order. Counsel for the Defendant, and any other representatives of the Defense who will be provided access to the classified information, shall execute the Memorandum of Understanding described in paragraph 15 of this Order, and counsel for the Defendant shall file executed originals of such documents with the Court and the CISO and serve an executed original upon the Government. The execution and filing of the Memorandum of Understanding is a condition

precedent for counsel for the Defendant and any other representative of the Defense to have access to classified information.

Dated: December 15, 2021

SO ORDERED.

Anthony J. Trenga
United States District Judge