

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION**

UNITED STATES OF AMERICA	:	CRIMINAL NO. 1:12MJ33
	:	
v.	:	
	:	PROTECTIVE ORDER
JOHN KIRIAKOU,	:	
Defendant.	:	
	:	

PROTECTIVE ORDER

This matter comes before the Court upon the Motion of the United States for a Protective Order to prevent the unauthorized disclosure or dissemination of classified information, which will be reviewed or made available to the defendant and his counsel by the government during the prosecution of this case. Pursuant to the authority granted under Section 3 of the Classified Information Procedures Act, 18 U.S.C. App. 3 (2000) ("CIPA"), the Security Procedures Established Pursuant to CIPA by the Chief Justice of the United States for the Protection of Classified Information (reprinted following CIPA Section 9), Rule 16(d) of the Federal Rules of Criminal Procedure and the general supervisory authority of the Court, and in order 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 the 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 which requires the appropriate security clearances. The purpose of this 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 and post-trial matters concerning classified information

and may be modified from time to time by further order of the Court.

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

a. "Classified information" shall mean:

i. any document or information which has been classified by any executive agency in the interests of national security or pursuant to Executive Order 13526 as "confidential," "secret," "top secret," or "sensitive compartmented information."

ii. any document or information now or formerly in the possession of a private party which (A) has been derived from information from the United States government that was classified, and (B) has been subsequently classified by the United States pursuant to Executive Order 13526 as "confidential," "secret," "top secret," or "sensitive compartmented information,"

iii. verbal classified information known to the defendant or defense counsel, or

iv. any information, regardless of place of origin and including "foreign government information," as that term is defined in Executive Order 13526, that could reasonably be believed to contain classified information, or that refers to classified national security or intelligence matters.

b. "Document" shall mean any material containing information. The term "document" shall include, without limitation, written or printed matter of any kind,

including originals, conforming copies, and non-conforming copies (e.g., a copy of an original with an added notation). The term “document” shall also include, without limitation, letters, reports, summaries, memoranda, notes, communications, telexes, cables, telecopies, telegrams, facsimiles, e-mails, microfilms, reports, photographs, charts, graphs, maps, invoices, accountings, worksheets, bulletins, transcripts, and messages, as well as alterations, amendments, modifications, and changes of any kind to the foregoing; and all recordings of information on magnetic, electronic, or optical media (including but not limited to those on CD-ROM), typewriter ribbons, films and all manner of electronic data processing storage.

c. “Access to classified information” means having access to, reviewing, reading, learning, or otherwise coming to know, in any manner, classified information.

d. “Secure area” means a secure facility approved by the Classified Information Security Officer for the storage, handling, and control of classified information.

3. Information in the public domain is ordinarily not classified. However, such information may be considered as classified and subject to the provisions of CIPA, if it is confirmed as being classified by any person who has, or has had, access to classified information and that confirmation corroborated the information in question. Any attempt by the defense to have such information confirmed or denied at trial or in any public proceeding in this case shall be governed by CIPA and all provisions of this Order.

4. All classified documents and information contained therein shall remain classified unless the documents bear a clear indication that they have been declassified by the agency or

department that originated the document or information contained therein (hereinafter, “originating agency”).

5. In accordance with the provisions of CIPA and the Security Procedures promulgated by the Chief Justice of the United States pursuant to that Act, this Court designates Christine E. Gunning as the Classified Information Security Officer and Jennifer H. Campbell, Branden M. Forsgren, Daniel O. Hartenstine, Joan B. Kennedy, Michael P. Macisso, Maura L. Peterson, Carli V. Rodriguez-Feo, Harry J. Rucker, and W. Scooter Slade as alternate Classified Information Security Officers for this case for the purpose of providing security arrangements necessary to protect any classified information or documents that will be made available to the defense in connection with this case or that may be in the possession of the defense from unauthorized disclosure. Defense counsel shall seek guidance from the Classified Information Security Officer with regard to appropriate storage, handling, transmittal, and use of classified information.

6. The Court has been advised that the Special Attorneys assigned to this case, Patrick J. Fitzgerald, David Glockner, Mark E. Schneider, Iris Lan, and Lisa L. Owings, and Department of Justice attorney Ryan Fayhce all have the requisite security clearances allowing them to have access to classified information that relates to this case. Any references to government attorneys as used in this Order refer only to the attorneys listed in this paragraph.

7. The defendant’s counsel, Plato Cacheris, John F. Hundley, and Mark J. MacDougall shall be given access to classified information as required by the government’s discovery obligations and in accordance with the terms of this Protective Order, and any other orders pursuant to CIPA, and upon receipt of appropriate security clearances. The defendant,

John Kiriakou, also will be given access to classified information as required by government discovery obligations and in accordance with the terms of this Protective Order, and any other orders pursuant to CIPA. As set forth in the Government's Motion for Protective Order, John Kiriakou 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 its agreement to maintain the confidentiality of classified information. Consequently, pursuant to federal common law and the ordinary principles of contract law, the defendant is hereby enjoined from breaching the terms of his secrecy agreements with the government, is prohibited from any future violations of the above referenced secrecy agreements, and is enjoined from disclosing any classified information to any unauthorized person unless authorized to do so by this Court. Any additional person whose assistance the defense reasonably requires may only have access to classified information in this case after first obtaining from this Court, with prior notice to the government, an approval for access to the required 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 from this case of defense counsel or any other cleared person associated with the defense as an employee or witness or otherwise, shall not release that person from the provisions of this Order or the Memorandum of Understanding executed in connection with this Order.

8. The Classified Information Security Officer shall arrange for and maintain an appropriately approved secure area for the use of defense counsel. The Classified Information Security Officer, in consultation with the United States Marshals Service, shall establish procedures to ensure that the secure area is accessible to defense counsel during business hours,

after business hours, and on weekends. The secure area shall contain a separate working area for defense counsel 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 Classified Information Security Officer, in consultation with defense counsel, 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 classified documents may be removed from the secure area unless so authorized by the Classified Information Security Officer, with notice provided to the Court. The Classified Information Security Officer shall not reveal to the government the content of any conversations she may hear among the defense, nor reveal the nature of the documents being reviewed or the work being generated. The presence of the Classified Information Security Officer shall not operate to render inapplicable the attorney-client privilege or the attorney work product doctrine.

9. Any pleading or other document filed by the defendant shall be filed under seal with the Court through the Classified Information Security Officer or an appropriately cleared designee of her choosing, unless defense counsel has obtained from the Classified Information Security Officer permission, specific to a particular, non-substantive pleading or document (e.g., motions for extensions of time, continuances, scheduling matters, etc.) not containing information that is or may be classified or under seal, to file the pleading or document not under seal.

Pleadings filed under seal with the Classified Information Security Officers or designee and shall be marked, "Filed in Camera and Under Seal with the Classified Information Security Officer." The date and time of physical submission to the Classified Information Security Officer or her designee, which should occur no later than 4:00 pm, shall be considered the date and time of

filing. At the time of making a physical submission to the Classified Information Security Officer or designee, counsel shall file on the public record in the CM/ECF system a notice of filing that notifies the Court that a filing has been made. The notice should contain only the case caption and an unclassified title of the filing. The Classified Information Security Officer shall make arrangements for the prompt delivery under seal to the Court and, except in the case of ex parte filings, to counsel for the United States any pleading or document to be filed by the defendant that may contain classified information. The Classified Information Security Officer shall promptly examine the pleading or document and, in consultation with representatives of the appropriate agencies, determine whether the pleading or document contains classified information. If the Classified Information Security Officer determines that the pleading or document contains classified information, she shall ensure that the portion of the document containing classified information, and only that portion, is marked with the appropriate classification marking and remains under seal. All portions of all papers filed by the defendants that are determined not to contain classified information will be placed in the public record.

10. Pleadings or documents filed by the United States that contain classified information shall be filed under seal with the Court through the Classified Information Security Officer or an appropriately cleared designee of her choosing. Such pleadings and documents shall be marked, "Filed In Camera and Under Seal with the Classified Information Security Officer." The date and time of physical submission to the Classified Information Security Officer or her designee, which should occur no later than 4:00 pm, shall be considered the date and time of filing. At the time of making a physical submission to the Classified Information Security Officer or designee, the government shall file on the public record in the CM/ECF system a notice of

filing that notifies the Court that a filing has been made. The notice should contain only the case caption and an unclassified title of the filing. The Classified Information Security Officer shall make arrangements for the prompt delivery under seal to the Court and, except in the case of ex parte filings, to counsel for the defendant any pleading or document to be filed by the United States that may contain classified information. All portions of all papers filed by the United States that are determined not to contain classified information will be placed in the public record.

11. Unless already holding an appropriate security clearance, and approved for access to classified information in this case, for the purpose of establishing security clearances necessary for access to classified information that may be involved in this case, Standard Form 86 ("Security Investigation Data for Sensitive Position"), attached Memorandum of Understanding, and full fingerprints shall be completed and submitted to the Classified Information Security Officer forthwith by defense counsel, and by all persons whose assistance the defense reasonably requires. The Classified Information Security Officer shall take all reasonable steps to process all security clearance applications.

12. The Classified Information Security Officer shall maintain a separate sealed record for those materials which are classified. The Classified Information Security Officer shall be responsible for maintaining the secured records for purposes of later proceedings or appeal.

13. The Court finds that in order to protect the classified information involved in this case, no individual other than counsel for the United States, appropriately cleared Department of Justice employees, personnel of the originating agency, the defendant, John Kiriakou, and his counsel, Plato Cacheris, John F. Hundley, and Mark J. MacDougall shall be allowed to obtain

access to classified information until and unless that person has been granted a security clearance by the Department of Justice through the Classified Information Security Officer, and has obtained permission of the Court. No other person except the defendant and counsel for the defendant shall have access to classified information involved in this case, unless and until that person, which includes any potential witness at trial, shall first have:

- a. received from the Classified Information Security Officer the appropriate security clearance for the level of the classified information involved in this litigation; and
- b. signed the Memorandum of Understanding, in the form attached hereto, thereby agreeing to comply with the terms of this Order.

The signed Memorandum of Understanding shall be filed with the Court. The substitution, departure, or removal for any reason from this case of counsel for the defense or anyone later cleared and associated with the defense as an employee or witness or otherwise shall not release that individual from the provisions of this Order or the Memorandum of Understanding executed in connection with this Order. Before any person other than counsel for the United States, appropriately cleared Department of Justice employees, and personnel of the originating agency is permitted by the Court to inspect and review classified information, he or she must also sign the attached Memorandum of Understanding.

14. Counsel for the defendant, Plato Cacheris, John F. Hundley, Mark J. MacDougall, the defendant, John Kiriakou, and any later cleared counsel for the defendant or cleared witnesses accompanied by counsel for the defendant (hereinafter, "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 Classified Information Security Officer. No classified information shall be maintained by the defense in any place other than the secure area established by the Classified Information Security Officer.
- b. Counsel for the defendant shall have free access to the classified information made available in the secure area established by the Classified Information Security Officer and shall be allowed to take notes and prepare documents with respect to those materials.
- c. No person, including counsel for the defendant, shall copy or reproduce any classified information in any manner or form, except with the approval of the Classified Information Security Officer or in accordance with the procedures established by the Classified Information Security Officer 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 must be prepared in a secure area on word processing equipment approved by the Classified Information Security Officer. All such documents and any associated materials (such as notes, drafts, copies, typewriter ribbons, magnetic recordings, exhibits) containing classified information shall be maintained in the secure area unless and until the Classified Information Security Officer determines that those documents or associated materials are unclassified in

their entirety. None of these materials shall be disclosed to counsel for the United States.

e. The defense shall discuss classified information only with other cleared persons and only in the secure area or in an area authorized by the Classified Information Security Officer.

f. The defense shall not disclose, without prior approval of the Court, the contents of any information to any person not named in this Order except the Court, Court personnel, and the attorneys for the United States identified by the Classified Information Security Officer as having the appropriate clearances and the need to know. Counsel for the United States shall be given an 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, to sign and submit to the 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 Classified Information Security Officer shall promptly seek to obtain security clearances for them at the request of defense counsel.

g. The defense, including the defendant, counsel for the defendant, and any other later cleared employees or defense witnesses, shall not discuss classified information over any standard commercial telephone instrument or office intercommunication systems, including but not limited to the internet, or in the

presence of any person who has not been granted access by the Court to classified information.

h. 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.

i. If counsel for the government advises defendant's counsel that certain classified information or documents may not be disclosed to the defendant, then defense counsel shall not disclose such information or documents to the defendant without prior concurrence of counsel for the government or, absent such concurrence, approval of the Court. Counsel for the government shall be given an opportunity to be heard in response to any defense request for disclosure to the defendant of such classified information.

15. No motion has been made by the defense for the disclosure of classified information. Procedures for the public disclosure of classified information by the defense shall be those established in sections 5 and 6 of CIPA. The Court may issue additional Protective Orders as needed.

16. No classified information may be disclosed by the defense except:

- a. to the Court, Court personnel, and government attorneys and their agents and employees identified by the Classified Information Security Officer as holding prior approvals for access to classified information;
- b. to representatives of the agency or department originating the classified information

who have been identified by the Classified Information Security Officer as holding appropriate security clearances and having the need to know the classified information;

c. in accordance with the procedures of CIPA and the procedures established by the Classified Information Security Officer; and

d. to persons who have been authorized to have access to classified information pursuant to this Order or to CIPA.

To facilitate the defense filing of notices required under Section 5 of CIPA, the Classified Information Security Officer shall make arrangements with the appropriate agencies for a determination of the classification level, if any, of materials or information either within the possession of the defense or about which the defense has knowledge and which the defense intends to use in any way in any pretrial proceeding or at trial. Nothing submitted by the defense to the Classified Information Security Officer pursuant to this paragraph shall be made available to counsel for the government unless so ordered by the Court, or so designated by the defense. Any and all items which are classified shall be listed in the defendant's Section 5 notice.

17. As the identity of government intelligence employees may be classified, and as certain security arrangements may be necessary to protect classified information which may be discussed, the parties agree that the defense may not contact any employee of any government intelligence agency without making prior arrangements for such contact with an attorney for the government, unless the defense files a motion with the Court -- which motion may be ex parte at the discretion of defense counsel -- to authorize such contact, gives the government notice of such motion without revealing the name of the employee the defense seeks to contact, and obtains a Court order authorizing that contact. Further, the defense shall give prior notice to government

attorneys of any contacts it intends to make with any employee of any government intelligence agency for the purpose of declassifying any classified information relating to this case.

18. Any unauthorized disclosure of classified information may constitute violations of United States criminal laws. In addition, any violation of the terms of this Order shall be brought immediately to the attention of this 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 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 Protective 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, without prior written authorization from the originating agency and in conformity with this Order.

19. All classified information to which the defense (including the defendant, counsel for the defendant, any later cleared employee of counsel for the defendant, or cleared defense witness) have access in this case are now and will remain the property of the United States. Upon demand of the Classified Information Security Officer, these persons shall return to the Classified Information Security Officer 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 Classified

Information Security Officer for the duration of the case. At the conclusion of this case, all such notes, summaries and other documents are to be destroyed by the Classified Information Security Officer in the presence of defense counsel if they choose to be present.

20. A copy of this Order shall be issued forthwith to the defendant, defense counsel who shall be responsible for advising the defendant, any co-counsel, employees of counsel for the defendants, and defense witnesses who need to know of the contents of this Order. Defendant, counsel for the defendant, and any other individuals who will be provided access to classified information shall execute the Memorandum of Understanding described in paragraph 13 of this Order, and counsel for the defendant shall file executed originals of such documents with the Court and the Classified Information Security Officer and serve an executed original upon the United States. The execution and filing of the Memorandum of Understanding is a condition precedent for defendant, counsel for the defendant, or any other person assisting the defense to have access to classified information.

SO ORDERED this 8th day of March, 2012, at Alexandria, VA.

_____/s/ _____ JFA
John F. Anderson
United States Magistrate Judge

JOHN F. ANDERSON
U.S. MAGISTRATE JUDGE
EASTERN DISTRICT OF VIRGINIA