IN THE UNITED STATES DISTRICT COURT

FOR THE SOUTHERN DISTRICT OF GEORGIA

AUGUSTA DIVISION

UNITED STATES OF AMERICA	)	
	)	
	)	
v.	)	CR 117-034
	)	
	)	
REALITY LEIGH WINNER	)	

PROTECTIVE ORDER

Pursuant to the authority granted under section 3 of the Classified Information Procedures Act, 18 U.S.C. App. III ("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 (reprinted following CIPA § 9) (hereinafter the "Security Procedures"); the Federal Rules of Criminal Procedure 16(d) and 57; the general supervisory authority of the Court; and, in order to protect the national security, the Court grants the government's request for a protective order, as modified below.

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, require special security precautions, and access to which requires a security clearance and a need-to-know.

2. The purpose of this Protective Order ("Order") is to establish the procedures that must be followed by all defense counsel of record, their designated

employees, all other counsel involved in this case, translators and investigators for the defense, 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 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.

Definitions

4. As used herein, the terms "classified national security information and documents," "classified information," "classified documents," and "classified material" 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," or "SECRET," or "TOP SECRET," or "SENSITIVE COMPARTMENTED INFORMATION ("SCI")"; or any information contained in such documents;

B. Any document or information, regardless of its physical form or characteristics, now or formerly in the possession of a private party, which has been derived from a United States Government classified document, information, or material, regardless of whether such document, information, or material has itself subsequently been classified by the Government pursuant to Executive Order 13526 or its predecessor orders as "CONFIDENTIAL" or "SECRET," or "TOP

SECRET," or "SCI;"

C. Verbal classified information known to the defense counsel;

D. Any document or information, including verbal information, which the defense counsel have been notified orally or in writing contains classified information;

E. Any information, regardless of place or origin and including "foreign government information" as that term is defined in Executive Order 13526, that could reasonably be believed to contain classified information; and

F. Any information obtained from an agency that is a member of the United States "Intelligence Community" (as defined in section 3(4) of the National Security Act of 1947, codified at 50 U.S.C. § 3003(4)), that could reasonably be believed to contain classified information or that refers to national security or intelligence matters.

5. The words "documents," "information," and "material" 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 conversations, meetings or other communications, bulletins, teletypes, telegrams, and telefacsimiles,

invoices, worksheets and drafts, alterations, modifications, changes, and amendments of any kind to the foregoing;

B. Graphic or oral records or representations of any kind, including but not limited to photographs, charts, graphs, microfiche, microfilm, videotapes, sound recordings of any kind, and motion pictures;

C. Electronic, mechanical, or electric records of any kind, including but not limited to tapes, cassettes, disks, recordings, films, typewriter ribbons, word processing or other computer tapes or disks, and all manner of electronic data processing storage; and

D. Information acquired orally or verbally.

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 an accredited facility or other appropriate location approved by a Classified Information Security Officer for 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 (hereinafter the "Originating Agency") of the document, material, or information contained therein.

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

10. Classified Information Security Officer. In accordance with the provisions of CIPA and the Security Procedures, the Court designates Carli V. Rodriguez-Feo as Classified Information Security Officer for this case, and Debra M. Guerrero-Randall, Daniel O. Hartenstine, Joan B. Kennedy, Shawn P. Mahoney, Maura L. Peterson, Winfield S. "Scooter" Slade, and Harry J. Rucker III, as Alternate Classified Information Security Officers 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. Defense counsel shall seek guidance from the Classified Information Security Officer 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, Assistant United States Attorney Jennifer Solari and U.S. Department of Justice Attorneys Julie Edelstein and David Aaron, and their respective supervisors (collectively referred to hereinafter as the "Government Attorneys"), have the requisite security clearances to have access to the classified information that relates to this case.

12. Protection of Classified Information. Only Government Attorneys,

appropriately cleared Department of Justice employees, personnel of the Originating Agency, defense counsel, employees of defense counsel, translators, and investigators employed or hired by defense counsel, shall have access to the classified information in this case.

A. Defense counsel, employees of defense counsel, defense consultants, experts or defense translators, and investigators may obtain access to classified documents or information only if such person has:

1) Received permission of the Court, either through this Order (for those named in paragraph 13 below) or by a separate Court order upon showing of a need-to-know;

2) Received the necessary security clearance at the appropriate level of classification, through or confirmed by the Classified Information Security Officer; and

3) Signed the Memorandum of Understanding in the form attached hereto, agreeing to comply with the terms of this Order.

B. Defense consultants and experts must, in addition to satisfying the other requirements in this Order, obtain approval for access to classified information from a Classification Specialist designated by the relevant Original Classification Authority ("OCA"), who shall be "walled off" from the prosecution team. The Defense shall submit its request for access to the Classified Information Security Officer, who shall submit the request to the OCA Classification Specialist. The

Defense may appeal to the Court any rejection by the OCA of the request for access.

The request for access shall not be disclosed to the prosecution team. However, the OCA may move the Court, with notice to the defense, for permission to disclose the request for access to the prosecution team.

C. Originals of the executed Memoranda of Understanding shall be filed with the Court under seal and served upon the Classified Information Security Officer.

D. Nothing in this Protective Order shall be construed as relieving the Defense of its otherwise applicable obligations under the Federal Rules of Criminal Procedure or Federal Rules of Evidence regarding disclosure of information about experts who will testify at trial.

E. The substitution, departure and removal for any reason from this case of counsel for the defendant, or anyone associated with the Defense as an employee or otherwise, shall not release that person from the provisions of this Order or the Memorandum of Understanding executed in connection with this Order.

13. Defense Counsel. Subject to the provisions of paragraph 12, the following attorney(s) for the defense and their approved employee(s), translator(s), and investigator(s) (collectively referred to hereinafter as "the Defense"), may be given access to classified information as required by the Government's discovery obligations: Titus Thomas Nichols, John C. Bell, Jr., Jill E. McCook, Joe D. Whitley, Matthew Scott Chester, Brett A. Switzer, and Thomas H. Barnard, counsel of record, Holly Hampton, paralegal, and Marie Jenkins, office manager, who have or will have received the appropriate security

clearance. 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.

14. Secure Area of Review. The Classified Information Security Officer shall arrange for an appropriately approved Secure Area for use by the Defense. The Classified Information Security Officer, in consultation with the United States Marshals Service, shall establish procedures to assure that the Secure Area is accessible to the Defense during normal business hours. After hours or weekend access may be obtained upon reasonable notification to the Court, and 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 in this case. 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 documents or other material containing classified information may be removed from the Secure Area unless authorized by the Classified Information Security Officer. The Classified Information Security Officer shall not reveal to the Government the content of any conversations he or she 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 Classified Information Security Officer shall not operate to waive, limit, or otherwise render inapplicable, the attorney-client privilege.

15. Filings with the Court. Until further order of this Court, any motion, memorandum, or other document filed by the Defense that defense counsel knows, or has reason to believe, contains classified information in whole or in part, or any document the proper classification of which defense counsel is unsure, shall be filed under seal with the Court through the Classified Information Security Officer or an appropriately cleared designee of his or her choosing. Pleadings filed under seal with the Classified Information Security Officer 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 Classified Information Security Officer or a designee, which should occur no later than 4:00 pm, shall be considered as the date and time of court filing. At the time of making a physical submission to the Classified Information Security Officer or a 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 Classified Information Security Officer shall make arrangements for prompt delivery under seal to the Court and counsel for the Government any document to be filed by the Defense that contains classified information. The Classified Information Security Officer shall promptly examine the document and, in consultation with representatives of the appropriate Government agencies, determine whether the document contains classified information. If

the Classified Information Security Officer determines that the document contains classified information, he or she shall ensure that the classified portions of the document, and only those portions, are marked with the appropriate classification marking and that the document remains under seal. All portions of any document filed by the Defense that do not contain classified information shall immediately be unsealed by the Classified Information Security Officer and placed in the public record.

16. Any document filed by the Government containing classified information shall be filed under seal with the Court through the Classified Information Security Officer or an appropriately cleared designee of her or his choosing. Pleadings filed under seal with the Classified Information Security Officer or a designee shall be marked "Filed In Camera and Under Seal with the Court 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 Classified Information Security Officer or a designee, which should occur no later than 4:00 pm, shall be considered the date and time of filing. The Classified Information Security Officer shall make arrangements for prompt delivery under seal to the Court and defense counsel (unless ex parte) any document to be filed by the Government that contains classified information. At the time of making a physical submission to the Classified Information Security Officer or a 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.

17. Sealing of Records. The Classified Information Security Officer 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 Classified Information Security Officer;

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, to pursue leads or in the defense of the defendant;

C. The Defense shall not copy or reproduce any classified information in any 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, 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 in the Secure Area on equipment approved for the processing of classified information, and in accordance with the procedures established by the Classified Information Security Officer. 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 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 Government;

E. The Defense shall discuss classified information only within the Secure Area or in another area authorized by the Classified Information Security Officer, and shall not discuss or attempt to discuss classified information over any standard commercial telephone instrument or office intercommunication system, including but not limited to 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, except to the Court, court personnel, and the Government Attorneys who have been identified by the Classified Information Security Officer as having the appropriate clearances and the need-to-know that information. Defendant's access shall be governed by a separate protective order. If preparation of the defense requires that classified information be disclosed to persons not named in

this Order, the OCA Classification Specialist and Classified Information Security Officer shall promptly seek to obtain access and security clearances for them at the request of defense counsel. Defense counsel must provide notice of any such request as provided in Paragraph 12. Any rejected request for access may be appealed to the Court as provided in Paragraph 12. Any person approved by the Court for disclosure under this paragraph shall be required to obtain the appropriate security clearance, to sign and submit the Memorandum of Understanding appended to this Order, and to comply with all the terms and conditions of the Order. Any such person will be instructed further by the designated OCA Classification Specialist to limit discussion with the Defense to only those matters which are within the specific access granted.

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. The Defense is not precluded from citing or repeating information in the public domain that counsel does not know or have reason to believe to be classified information, or derived from classified information.

19. Procedures for the use or disclosure of classified information by the Defense shall be those provided in sections 5, 6, and 8 of CIPA. To facilitate the Defense's 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 at any pre-trial proceeding, deposition 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 that are classified shall be listed in the defendant's CIPA section 5 notice. To the extent that any classified information is the basis of any motion filed by the Defense, such motion shall be preceded by a CIPA section 5 notice.

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 immediately brought 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 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. It shall not violate this Order for an individual subject to this Order to disclose information that the individual did not know, and reasonably should not have known based on information provided by the Government in this case, is classified. Any individual subject to this Order who intends to disclose information and is not certain whether that information is classified should consult with the Classified Information Security Officer.

22. 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 counsel, defense counsel employees, defense translators, investigators, 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 Classified Information Security Officer 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 Classified Information Security Officer 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 Classified Information Security Officer in the presence of defense counsel if so desired.

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

24. A copy of this Order shall be issued forthwith to counsel for the defendant, who shall be responsible for advising the defendant and defense counsel employees of the contents of this Order.

SO ORDERED this 3rd day of August, 2017, at Augusta, Georgia.

BRIAN K. EPPS
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF GEORGIA