

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

UNITED STATES OF AMERICA	:	CRIMINAL NO. 12-231 (RC)
	:	
v.	:	
	:	
JAMES F. HITSELBERGER,	:	
	:	
Defendant.	:	

GOVERNMENT’S UNOPPOSED MOTION FOR PROTECTIVE ORDER

The United States of America, by and through its attorney, the United States Attorney for the District of Columbia, respectfully moves the Court pursuant to Section 3 of the Classified Information Procedures Act (CIPA), 18 U.S.C. App. III § 3, for the entry of a protective order to govern the handling, use, and storage of classified national security documents and information produced in discovery in this matter. Counsel for Mr. Hitselberger has authorized the government to represent it does not oppose this motion and that the parties have reached an agreement as to a proposed protective order and a proposed “Memorandum of Understanding for CIPA Protective Order,” which is an exhibit to the Order. Accordingly, for the reasons set forth

in the proposed Order, the Court should grant the government's motion.

Respectfully submitted,

RONALD C. MACHEN JR.
UNITED STATES ATTORNEY

By:

_____/s/_____

JAY I. BRATT
Assistant United States Attorney
National Security Section
555 4th Street, NW, 11th Floor
Washington, D.C. 20530
(202) 252-7789
Illinois Bar No. 6187361
jay.bratt2@usdoj.gov

MONA N. SAHAF
Assistant United States Attorney
National Security Section
555 4th Street, NW, 11th Floor
Washington, D.C. 20530
(202) 252-7080
D.C. Bar 497854
mona.sahaf@usdoj.gov

DEBORAH CURTIS
Trial Attorney
Counterespionage Section
National Security Division
U.S. Department of Justice
600 E Street, NW, 10th Floor
Washington, D.C. 20530
(202) 233-2113
deborah.curtis@usdoj.gov

Certificate of Service

I, Jay I. Bratt, certify that I served a copy of the foregoing Government's Unopposed Motion for Protective Order by ECF on Mary Petras, Esq., counsel for defendant, this 3rd day of January, 2013.

_____/s/_____
Jay I. Bratt

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

UNITED STATES OF AMERICA : **CRIMINAL NO. 12-231 (RC)**
 :
 v. :
 :
 JAMES F. HITSELBERGER, :
 :
 Defendant. :

CIPA PROTECTIVE ORDER

This matter comes before the Court upon the Government’s Unopposed Motion for a CIPA Protective Order to prevent the unauthorized disclosure or dissemination of classified national security documents and information which will be reviewed by, or made available to, or are otherwise in the possession of, the defendant and defense counsel in this case.

Pursuant to the authority granted under Section 3 of the Classified Information Procedures Act, 18 U.S.C. App. III (“CIPA”); the Security Procedures Established Pursuant to Pub. L. 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information (reprinted following CIPA Section 9; hereinafter referred to as the “Security Procedures”); Rules 16(d) and 57 of the Federal Rules of Criminal Procedure; the general supervisory authority of the Court; and in order to protect the national security, it is this _____ day of December, 2012, hereby

ORDERED that the Government’s Unopposed Motion for a CIPA Protective Order is **GRANTED**; and it is

FURTHER ORDERED that:

1. The Court finds that this case will involve classified national security documents and information, the storage, handling and control of which, by law or regulation, requires

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

2. The purpose of this Order is to establish the procedures that must be followed by the defendant, all defense counsel of record, their designated employees, all other counsel involved in this case, translators for the defense, any Court personnel, and all other individuals who receive access to, or otherwise are in possession of, classified documents or information in connection with this case.

3. The procedures set forth in this Protective Order and CIPA 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 Fed. R. Crim. P. 16(d); Sections 3 and 9 of CIPA; and the 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,” and “classified documents” refer to:

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

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 United States government information that was classified, regardless of whether such document or information has subsequently been classified by the United States pursuant to

Executive Order 13526 or its predecessor Orders as “CONFIDENTIAL,” “SECRET,” or “TOP SECRET,” or additionally controlled as “SENSITIVE COMPARTMENTED INFORMATION (SCI);”

c. Oral classified information known to the defendant or defense counsel;

d. Any document and information, including oral information, as to which the defendant or defense counsel have been notified orally or in writing that such document or information contains classified information; or,

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, or that refers or relates to national security or intelligence matters; and,

f. Any information obtained from any agency, department or other governmental entity, including a member of the Intelligence Community, as defined in 50 U.S.C. § 401a, that could reasonably be believed to contain classified information or that refers to national security or intelligence matters.

5. The words “documents” or “information” 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, inter-office and intra-office communications, notations of any sort concerning conversations, meetings, or other communications, bulletins, cables, telexes,

telecopies, teletypes, telegrams, and telefacsimiles, invoices, accountings, 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, maps, 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. 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 is the originating agency of the document or the information contained therein (hereinafter, the "originating agency").

7. Information in the public domain is ordinarily not classified. However, if classified information is reported in the press or otherwise enters the public domain, the information does not lose its classified status merely because it is in the public domain. And information reported in the press or otherwise in the public domain may be considered classified and subject to the provisions of CIPA if the information in fact remains classified and is confirmed by any person who has, or had, such access to classified information and that confirmation corroborates the information in question. Accordingly, any attempt by the defense to have classified information that has been reported in the public domain confirmed or denied at

trial or in any public proceeding in this case shall be governed by CIPA and all provisions of this Order.

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

9. “SCIF” shall mean a sensitive compartmented information facility accredited by a Classified Information Security Officer for the storage, handling, and control of classified documents and information, or other Secure Area so approved by the Classified Information Security Officer.

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

11. Government Attorneys - The Court has been advised that the following government attorneys working on this case, Assistant United States Attorneys Jay I. Bratt and Mona N. Sahaf, and United States Department of Justice Trial Attorney Deborah Curtis, and

their respective supervisors, have the requisite security clearances to have access to the classified documents and information that relate to this case. All references to government attorneys, or attorneys for the government, as used in this Order, refer only to the attorneys listed in this paragraph and their respective supervisors.

12. Protection of Classified Information - The Court finds that, in order to protect the classified documents and information involved in this case, no person, including the defendant and any witness for the defense, except government attorneys, appropriately cleared Department of Justice employees, personnel of the originating agency, defense counsel, and defense counsel employees, including translators, shall have access to the classified documents and information in this case. No defense counsel or defense counsel employee, including any translator, shall have access to any classified documents and information in this case unless that person shall first have:

a. Signed the Memorandum of Understanding in the form attached hereto, 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 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.

b. Persons other than government attorneys, appropriately cleared Department of Justice employees, and personnel of the originating agency, can only obtain access to classified documents and information after having been granted a security clearance by the Classified Information Security Officer and with permission of the Court, either through this

Order (for those named in paragraph 13 below), or by a separate Order upon a showing of a need to know. Before any person other than government attorneys, appropriately cleared Department of Justice employees, and personnel of the originating agency, is permitted by the Court to inspect and review classified documents or information, that person must also sign the Memorandum of Understanding.

13. Defense Counsel - Subject to the provisions of paragraph 12, the following attorneys for the defense, her approved co-workers, and their translator(s) (collectively referred to herein as “the defense” or “defense counsel”) shall be given access to classified documents and information as required by the government’s discovery obligations and otherwise as necessary to prepare for proceedings in this case: Mary Petras and Rosanna Taormina. This Order shall apply to any substituted counsel in the event that any of the above-named attorneys discontinue their involvement in this matter.

Any additional person whose assistance the defense reasonably requires may only have access to classified documents and information in this case after obtaining from the Court – with prior notice to the United States – 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 documents and information.

14. Unless already holding an appropriate security clearance and approved for access to classified documents and information in this case, for the purpose of establishing security clearances necessary for access to classified documents and information that may be involved in this case, standard Form 86 (“Security Investigation Data for Sensitive Position”), attached releases, and fingerprints shall be completed and submitted to the Classified Information

Security Officer forthwith by defense counsel, all persons whose assistance the defense reasonably requires, and by such Court personnel as the Court requires for its assistance. The Classified Information Security Officer shall take all reasonable steps to process all security clearance applications.

15. Area of Review - The Classified Information Security Officer shall arrange for an appropriately approved SCIF or Secure Area for use by the defense. The Classified Information Security Officer shall, in consultation with the United States Marshals Service, establish procedures to assure that the SCIF or Secure Area is accessible to the defense during normal business hours, after hours, and on weekends.. The SCIF or 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 defendant's defense in this case. The Classified Information Security Officer, in consultation with defense counsel, shall establish procedures to assure that the SCIF or Secure Area is maintained and operated in the most efficient manner consistent with the protection of classified documents and information. No documents containing classified information may be removed from this SCIF or Secure Area unless authorized by the Classified Information Security Officer. The Classified Information Security Officer shall not reveal to the United States the content of any conversations she or he may hear among the defense, nor reveal the nature of documents being reviewed by them, or the work generated by them. In addition, the presence of the Classified Information Security Officer shall not operate as a waiver of, limitation on, or otherwise render inapplicable, the attorney-client privilege.

16. If, upon the entry of a separate order of the Court, it becomes necessary for the defendant to review or discuss classified matters, or otherwise meet with defense counsel, in the SCIF or Secure Area, this will only occur under appropriate supervision to ensure that the defendant does not remove, copy, alter, or destroy classified documents and information, or obtain access to classified documents and information that the defendant is not entitled to review, and to ensure that the defendant does not use the opportunity to review the classified materials to circumvent any applicable security restrictions, including any other orders of this Court governing discovery in this case.

17. Filings with the Court - Until further order of this Court, any pleading or other document filed by the defense that it reasonably expects may contain classified information shall be filed under seal with the Court through the Classified Information Security Officer or a designee of her choosing who has obtained the necessary security clearance by 4 p.m. on the day of filing. Pleadings filed under seal with the Classified Information Security Officer or a designee of her choosing who has obtained the necessary security clearance 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 a designee of her choosing who has obtained the necessary security clearance shall be considered the date and time of filing. At the time of making a submission to the Classified Information Security Officer or a designee of her choosing who has obtained the necessary security clearance, defense counsel 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 Classified Information Security Officer or a designee of her

choosing who has obtained the necessary security clearance and providing a title of the document which does not disclose any potentially- classified information.

The Classified Information Security Officer or a designee of her choosing who has obtained the necessary security clearance 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 or a designee of her choosing who has obtained the necessary security clearance determines that the pleading or document contains classified information, she or he shall ensure that that portion of the pleading or document, and only that portion, is marked with the appropriate classification marking and that the pleading or document remains under seal. All portions of any pleading or document filed by the defense that does not contain classified information shall immediately be unsealed by the Classified Information Security Officer or a designee of her choosing who has obtained the necessary security clearance and placed in the public record. The Classified Information Security Officer or a designee of her choosing who has obtained the necessary security clearance shall immediately deliver under seal to the Court and counsel for the United States (unless such filing is ex parte) any pleading or document to be filed by the defense that contains classified information.

18. Any pleading or other document filed by the United States containing classified information shall be filed under seal with the Court through the Classified Information Security Officer or a designee of her choosing who has obtained the necessary security clearance following the same procedures as outlined in paragraph 17. The date and time of physical submission to the Classified Information Security Officer or a designee of her choosing who has

obtained the necessary security clearance shall be considered the date and time of the filing.

The Classified Information Security Officer or a designee of her choosing who has obtained the necessary security clearance shall immediately deliver under seal to the Court and counsel for the defense (unless such filing is ex parte) any pleading or document to be filed by the government that contains classified information.

19. 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 also maintaining the secured records for purposes of later proceedings or appeal.

20. Access to Classified Information - Defense counsel, their designated employees and translators, shall have access to classified documents and information only as follows:

a. All classified documents and information produced by the United States to the defense, in discovery or otherwise, and all classified documents and information possessed, created, or maintained by the defense, shall be stored, maintained, and used only in the SCIF or Secure Area established by the Classified Information Security Officer, unless otherwise authorized by the Classified Information Security Officer;

b. The defense shall have free access to the classified documents and information made available to them in the SCIF or 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 documents and information, either directly, indirectly, or in any manner which would disclose the existence of such, to pursue leads or in the defense of the defendant;

c. No person, including the defense, shall copy or reproduce any classified documents and 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 SCIF or 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 documents and information, and in the SCIF or Secure Area on approved word processing equipment and in accordance with the procedures approved by the Classified Information Security Officer. All such documents and any associated materials (such as notes, drafts, copies, typewriter ribbons, magnetic recordings, and exhibits) containing classified information shall be maintained in the SCIF or 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 documents and information only within the SCIF or Secure Area authorized by the Classified Information Security Officer, and shall not discuss or attempt to discuss classified documents or information over any standard commercial telephone instrument or office intercommunication system, including but not limited to the Internet;

f. The defense shall not disclose, without prior approval by the United States in the first instance or by the Court upon notice to and opportunity to be heard by the United

States, the contents of any classified documents or information to any person not authorized pursuant to this Order, including the defendant and defense witnesses, except the Court, Court personnel, and the attorneys for the United States, who have been identified by the Classified Information Security Officer as having the appropriate clearances and the need to know that information. Counsel for the United States shall be given notice of and an opportunity to be heard by the Court in response to any defense request to the Court for disclosure to a person not named in this Order. Any person approved by the United States in the first instance or by the Court upon notice to and an opportunity to be heard by the United States for disclosure under this paragraph shall be required to obtain the appropriate security clearance as necessary, to sign and submit to the Court the Memorandum of Understanding appended to this Order, and to comply with all terms and conditions of this Order. If preparation of the defense requires that classified documents or information be disclosed to persons not named in this Order, then, upon approval by the United States in the first instance or by the Court upon notice and an opportunity to be heard by the United States, the Classified Information Security Officer shall promptly seek to obtain security clearances for them at the request of defense counsel.

21. Procedures for the use or the public disclosure of classified documents and information by the defense shall be those provided in Sections 5 and 6 of CIPA. No classified documents or information may be used or 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 proper approvals for access to classified information;

b. In accordance with the procedures of CIPA and the procedures established by the Classified Information Security Officer;

c. To persons who have been authorized to have access to classified documents or information pursuant to this Order or to CIPA; and,

d. 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.

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 at any pretrial 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 United States 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.

22. Violations of this Order - Any unauthorized disclosure or dissemination of classified documents or information may constitute violations of United States criminal laws. In addition, any 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 the Court and possible referral for criminal prosecution. Any breach of this Order may also result in the termination of a person's access to classified documents or information. Persons subject to this Order are advised that direct or

indirect unauthorized use, disclosure, retention, or negligent 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. This Order is intended to ensure that those authorized by the Order to receive classified documents or information will never divulge the classified documents or information disclosed to them in connection with this case to anyone who is not now authorized to receive it, or otherwise use the classified documents or information, without prior written authorization from the originating agency and in conformity with this Order.

23. All classified documents and information to which defense counsel and defense counsel employees, including translators, have access in this case are now and will remain the property of the United States. The defense counsel and defense counsel employees, including translators, who receive classified documents and information shall return all such classified documents and information in their possession obtained through discovery from the United States in this case, or for which they are responsible because of access to classified documents and information, upon demand of the Classified Information Security Officer. 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 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 so desired.

24. Nothing in this Order shall preclude the United States from seeking a further protective order pursuant to Rule 16(d) as to particular items of discovery material.

25. 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, including translators, of the contents of this Order. The defense counsel and defense counsel employees to be provided access to classified information shall execute the Memorandum of Understanding appended to this Order, and defense counsel shall file executed originals with the Court and the Classified Information Security Officer and serve executed originals of such document upon the United States. The execution and filing of the Memorandum of Understanding is a condition precedent for defense counsel, defense counsel employees, and any other person working for the defense to have access to classified information. It is also a condition precedent for the defendant and any defense witness to have access to classified information pursuant to paragraph 20f above.

Rudolph Contreras
Judge
United States District Court
for the District of Columbia

copied to:

Jay I. Bratt
Mona N. Sahaf
Assistant United States Attorneys
United States Attorney's Office
555 4th Street, NW, 11th Floor
Washington, D.C. 20530

Deborah Curtis
Trial Attorney
U.S. Department of Justice
600 E Street, NW, 10th Floor
Washington, D.C. 20530

Counsel for the Government

Mary T. Petras
Assistant Federal Public Defender
Federal Public Defender
625 Indiana Avenue, NW
Washington, D.C. 20004

Counsel for Defendant James F. Hitselberger

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

UNITED STATES OF AMERICA)	
)	
v.)	Cr. No.: 10-225 (CKK)
)	
STEPHEN JIN-WOO KIM,)	
also known as Stephen Jin Kim,)	
also known as Stephen Kim,)	
also known as Leo Grace,)	
)	
Defendant.)	

MEMORANDUM OF UNDERSTANDING

1. Having familiarized myself with the applicable laws, I understand that I have already received and/or may be the future recipient of information and documents which pertain to the national security of the United States and which are the property of the United States, and that such information and documents, together with the methods of collecting such information, are classified according to security standards set by the United States government.

2. I agree that I shall never divulge, publish, or reveal, either by word, conduct, or any other means, such classified information or documents unless specifically authorized in writing to do so by an authorized representative of the United States government, or as authorized by the Court pursuant to the Classified Information Procedures Act (“CIPA”) or the CIPA Protective Order entered in the above-captioned case, or as otherwise ordered by the Court,

3. I agree that this Memorandum of Understanding and any other nondisclosure agreement signed by me in connection with this case will remain forever binding upon me.

4. I have received, read, and understand the CIPA Protective Order entered by the United States District Court for the District of Columbia in the above-captioned case, and I agree to comply with the provisions contained therein.

5. I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge, information, and belief.

Name:

Date and Place of Birth:

(signature)

Date: _____