



U.S. Department of Justice

Executive Office for Immigration Review

Office of the Chief Immigration Judge

5107 Leesburg Pike, Suite 2545
Falls Church, Virginia 22041

February 5, 2009

MEMORANDUM

TO: All Assistant Chief Immigration Judges
 All Immigration Judges
 All Court Administrators
 All Attorney Advisors and Judicial Law Clerks
 All Immigration Court Staff

FROM: Thomas G. Snow *T. Snow*
 Acting Chief Immigration Judge

SUBJECT: Operating Policies and Procedures Memorandum 09-01:
Classified Information in Immigration Court Proceedings

Table of Contents

I. Introduction..... 2

II. Definitions..... 3

III. Security Coordinator..... 3

IV. Access to Classified Information..... 4

 A. Requirements for Access to Classified Information..... 4

 B. Responsibilities to Ensure the Safeguarding of Classified Information 4

 C. How to Obtain Clearance..... 5

V. Custody and Storage of Classified Materials..... 6

 A. Materials Covered..... 6

 B. Safeguarding Classified Information..... 6

VI. Security Procedures..... 7

 A. Oral Discussions..... 7

 B. Telephone and Facsimile Security 7

 C. Reproduction Security.....7

 D. Computer Security..... 8

VII.	Procedure for Cases Involving Classified Information.....	10
	A. Notices.....	10
	B. Custody and Bond Redetermination.....	11
	C. Pre-hearing Conference.....	12
	D. Motion for an <i>In Camera</i> Hearing.....	12
	E. Hearings.....	13
	F. Final Decision by an Immigration Judge.....	14
	G. Remands.....	15
VIII.	Transmittal of Classified Information.....	15
	A. Confidential or Secret Information.....	15
	B. TOP SECRET Information.....	16
IX.	Final Disposition and Destruction.....	16
	A. Return Original Classified Documents.....	16
	B. Destroy Copies of Classified Information.....	16
	C. Storage Until Destruction.....	16
	D. Archiving Classified Evidence.....	16
	APPENDIX.....	18
	I. Executive Order.....	18
	II. Regulatory Provisions Pertaining to Classified Issues.....	18
	III. Booklets and Secondary Materials.....	20

I. Introduction

This Operating Policies and Procedures Memorandum (OPPM) provides guidance on proper handling of classified information in Immigration Court proceedings and within the Immigration Courts and supersedes OPPM 98-10, *Classified Information in Immigration Court Proceedings*, dated December 28, 1998, which is hereby rescinded. Handling of classified information requires that certain procedural safeguards be followed to protect the nature and source of the information. Whenever circumstances appear to be beyond the scope of this OPPM, request assistance of your Assistant Chief Immigration Judge and the Executive Office for Immigration Review (EOIR) Security Office. The purpose of the following procedures is to protect against unauthorized disclosure of classified information, classified pursuant to Executive Order (EO) 12958 (1995), as amended by EO 13292 (2003), and the implementing regulations Information Security Oversight Office, Directive 1, September 22, 2003; 32 C.F.R. Parts 2001 through 2004; and the Department of Justice Security Program Operating Manual, dated May 5, 2005.

II. Definitions

Classified national security information or classified information (hereafter, “classified information”) means any information or material that has been determined pursuant to Executive Order (EO) 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure for reasons of national security.

There are three levels of classification under EO 12958, as amended:

- Top Secret: The unauthorized disclosure of this information reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
- Secret: The unauthorized disclosure of this information reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe; and
- Confidential: The unauthorized disclosure of this information reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

III. Security Coordinator

The Court Administrator in each Court handling classified information is the Security Coordinator for all cases involving classified information. The Court Administrator, as Security Coordinator, is responsible for ensuring that security procedures are followed by appropriately cleared Court personnel with regard to classified materials. This includes overseeing handling of classified information, transmission and storage of classified materials, and that all those with access to the information follow procedures so that unauthorized disclosure of classified information does not occur.

The Court Administrator, as Security Coordinator, must notify his or her Assistant Chief Immigration Judge and the EOIR Security Office as soon as possible upon learning that a case will involve presentation of classified information.

In a case involving classified information, the Court Administrator, as Security Coordinator, may designate appropriately cleared Court personnel to assist with ensuring that security safeguarding procedures are followed in a specific case, or on all cases. This is necessary so that if the Court Administrator is unable to be present at a particular hearing site, or if there are several cases involving classified information under the control of one Court Administrator, there is an additional person(s) to aid in maintaining the security procedures. There must be an employee or employees responsible for ensuring security procedures are followed at each Court that handles classified information.

The Court Administrator, with assistance of any appropriately cleared Court personnel that he or she designates, must establish and maintain a control and accountability system for all classified information received by, or transmitted from, the Court. The control system must provide a plan for the Court to accurately keep track of any classified materials within its control, to establish a method for ensuring responsibility for the classified materials at all times, and procedures to prevent unauthorized access to the materials. The control and accountability system should account for the individual and unique characteristics of each Court. The system need not be elaborate, but it should be written so that all Court personnel may refer to it, when necessary.

IV. Access to Classified Information

A. Requirements for Access to Classified Information

Court personnel to whom classified cases are assigned must:

1. Possess the appropriate level security clearance;
2. Must have demonstrated a need-to-know the information; and

a. “Need-to-know” is a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

b. No person is entitled to receive classified information solely by virtue of office, position, rank, or security clearance. Ensure that any individual requesting access to classified information under your control has: the appropriate level security clearance for access, signed an approved non-disclosure agreement; and a legitimate need-to-know the information.

The classifying agency must certify in writing that a third-party, not employed by the Department of Justice (DOJ), wanting access to classified information has a legitimate need-to-know the classified information prior to the information being released. The classifying agency’s certification authorizing the release of classified information must be contained in the record.

3. Must have signed an approved classified information non-disclosure agreement on file with the EOIR Security Office.

B. Responsibilities to Ensure the Safeguarding of Classified Information

1. No Unauthorized Disclosure of Classified Information

a. Generally

Appropriately cleared Immigration Judges and Court personnel shall not disclose classified information to anyone who does not have a security clearance at the appropriate level, who has not signed an approved non-disclosure agreement, and who does not possess a legitimate need-to-know the information, that is, those who do not require the information in the discharge of an official function.

b. Disclosure to Court Personnel

Classified information may be discussed among appropriately cleared Court personnel so long as each person has the appropriate level security clearance, has signed an approved non-disclosure agreement, and has a legitimate need-to-know the information. Appropriately cleared Court personnel, as authorized holders, are not required to have certification from the classifying agency to disclose classified information to Court personnel so long as the personnel have the appropriate level security-clearance and a need-to-know the information.

c. Disclosure to Persons Outside the Court

If disclosure to other DOJ components or other Federal departments and agencies is requested, security-cleared Court personnel are responsible for ensuring that individuals with whom they must discuss classified information or documents possess the appropriate level security clearance and a legitimate need-to-know the information. There must be written certification from the classifying agency to disclose the information to a party not employed by the DOJ. Disclosure of classified information to individuals not employed by the DOJ for which written certification is received from the classifying agency will also require that the Security Officer of their employing department/agency forward written certification of the individual's security clearance to the DOJ Security Officer or that the DOJ Security Officer grant that individual a security clearance.

d. Confirmation that an individual has security clearance can be requested from the EOIR Security Office.

2. Personnel and Security Related Concerns

If there is a question of the possible loss or compromise, or suspected compromise, of classified information, the EOIR Security Office must be immediately contacted and informed of the situation.

C. How to Obtain Clearance

1. Requests for security clearance should be directed to the EOIR Security Office. The EOIR Security Office will notify the employee when clearance (Top Security, Secret, or Confidential) has been granted.

2. The EOIR Security Office will provide each Court employee granted a security clearance with a package of materials concerning the proper handling and protection of classified material and a security briefing. Court employees must receive this briefing prior to access to classified information. The briefing may be conducted telephonically by EOIR Security Personnel. Contact the EOIR Security Office if you need additional copies of any information contained in the security clearance packet.

3. If security clearance cannot be obtained promptly, Court personnel who have the requisite clearances may be temporarily assigned to assist on a particular case.

V. Custody and Storage of Classified Materials

A. Materials Covered

These security procedures apply to all papers, documents, and materials that contain classified information and are in the custody of the Court (*e.g.*, motions, pleadings, briefs, notes, transcripts, and tapes taken during *in camera* proceedings).

B. Safeguarding Classified Information

1. Classified information submitted to the Court shall be handled only by personnel with the appropriate security clearance, who are working on the particular case or court matter and possess a legitimate need-to-know the information.

2. When not in use, all classified materials shall be stored in a security container approved by the General Services Administration (GSA). The combinations to the security containers are classified at the same level as the highest level of classified material stored within the container. Combinations to security containers shall be changed by the Security Coordinator to convert the factory pre-set combination when the combination has been subject to possible compromise or an individual knowing the combination no longer requires access to the combination. Classified materials relating to separate cases within the same security container shall be segregated by placing the materials in separate envelopes or folders that are appropriately labeled as to the classification level and are identified by the alien ("A") number. The combination to the security container may be given to any Court employee (Immigration Judge, Judicial Law Clerk, Legal Assistant, or Court Administrator) who possesses the appropriate security clearance, has signed an approved non-disclosure agreement, has need-to-know, and requires access to the container. Unclassified materials must not be stored in these security containers (safes).

3. Classified material must be kept in secure facilities and must never be taken to a person's home. This is true even if a person has appropriate security clearance. Classified material should never leave the Court, unless it is being returned to the agency where the material originated, sent to the Board of Immigration Appeals (Board), or archived. *See also* section VIII, Transmittal of Classified Information.

4. Access to classified information by Court personnel shall be limited to the minimum number of cleared persons necessary for operating purposes. Access includes presence at an *in camera* hearing or any other proceedings during which classified information may be disclosed.

5. In accordance with procedures established by the Security Coordinator at each Court, all materials containing classified information should be accounted for when they are taken from the security container. The Security Container Checklist, Form SF-702, affixed to the outside of the container, may be used to track who had access to the container and the date(s) and time(s) of such access. Additionally, an unclassified document register, to be kept in the container, should be used to track who had access to the security container, who took classified material from the security container, and when the material was returned.

VI. Security Procedures

A. Oral Discussions

Meetings at which classified information will be discussed must be held in an area that affords sufficient security against unauthorized disclosure. The classified information must not be able to be overheard or seen by a person who does not have both an appropriate level security clearance and a legitimate need-to-know the information.

B. Telephone and Facsimile Security

Classified information may not be discussed or transmitted over standard commercial telephone instruments, office intercommunication systems (*e.g.*, e-mail), or standard commercial facsimile equipment. Classified information may only be discussed or transmitted over appropriate security level Secure Terminal Equipment (STE) or Secure Telephone Units (commonly referred to as STU-IIIs) and their accompanying secure facsimile machines. Contact the EOIR Security Office if access is required to a STE or STU-III.

C. Reproduction Security

1. Courts handling classified information should designate one copier within the Court for the reproduction of classified material. The attached handout entitled "Rules for Reproduction of Classified Material" should be posted at the copier. Use of digital copiers for classified reproduction must be approved by the Department Security Officer through the EOIR Security Office. These devices are computer driven and constitute an Information

Technology system subject to the same vulnerabilities as any other computer device. Network copiers must not be used to copy classified information.

2. Before making copies, personnel should ensure that persons without security clearance and a legitimate need-to-know the information are unable to access or view classified information during reproduction.

3. Reproduce only the number of copies absolutely necessary. Ensure that all copies of all pages are received, that no pages remain inside the copier, and that all classified waste is removed and disposed of properly. *See also* section IX, Final Disposition and Destruction.

4. Upon completion of classified reproduction, five copies of a test pattern, or unclassified material, should be run through the copier.

D. Computer Security

1. Generally

All computers and printers used to process classified information must be certified, accredited and approved by the EOIR Information Resources Management Staff (IRM), in consultation with the EOIR Security Office in Falls Church, Virginia, for the processing of classified information prior to initiation of any processing.

2. Approved Laptop Computers Must Be Used

a. Any document prepared by Immigration Court personnel containing classified information must only be processed using an approved laptop computer. The computer must not be connected to any network or e-mail system. The approved laptop computer should be used only to create or process classified documents related to the cases for which it was intended and must be stored in a GSA-approved security container when not in use.

b. When a Court anticipates that it will be required to take notes or create a written document containing classified information, the Security Coordinator should request an approved laptop computer from IRM.

c. Once the Court no longer requires use of the approved laptop computer for the designated case(s), the Security Coordinator must ensure that the computer is returned to IRM. The same procedures that must be followed for transmitting classified information must be used for returning the laptop computer (*i.e.*, for Confidential or Secret information, the computer must be double-wrapped with the appropriate markings on the inside wrapping or box and no indication of the classification level on the outside wrapping or box; and for Top Secret information, the laptop must be double-wrapped as indicated above and hand-carried to its destination). *See* section VIII, Transmittal of Classified Information.

d. The approved laptop must not be taken outside of the premises unless it is kept within the carrier's control at all times. The carrier must go directly to the destination without allowing the laptop to leave his or her control. *See* section VIII, Transmittal of Classified Information. The approved laptop must never be taken home.

3. Computer Location

a. Computer equipment used to process classified information should, whenever possible, be located in a room to which access can be limited and where processing can be accomplished without being observed or monitored by persons who do not possess the appropriate security clearances and have a legitimate need-to-know the information.

b. Depending upon the type of facility where the Court is located and the classification level of any classified materials, additional safeguards may be required. Courts handling classified documents or creating classified attachments should contact the EOIR Security Office for assistance prior to creating any classified decisions.

4. Disks or Compact Discs (CD's)

a. Any classified documents created on approved laptop computers should be maintained on disks or CD's. The information should not be saved on the laptop computer's hard drive. Any disks or CD's must be stored according to the security procedures set forth above. The disk or CD should be labeled according to highest level of classified information that it contains. The sticker labels used to mark tapes of classified hearings are appropriate for labeling a disk or CD. A disk or CD containing a copy of a written decision should be treated like a paper reproduction.

b. Disks or CD's may be used to transfer information to another appropriately certified and accredited computer so long as the disk or CD is transported in compliance with the security procedures listed below for the transmittal of classified information. *See* section VIII, Transmittal of Classified Information.

c. As soon as a disk or CD is no longer needed for operational needs, it should be destroyed, for a disk by taking apart the outside case, removing the interior floppy film, and running the floppy film through a cross-cut shredder that produces residue no longer than 1 mm in width by 5 mm in length. *See* section IX, Final Disposition and Destruction.

5. Printers

a. Any classified attachment or document (*e.g.*, notes containing classified information) should be printed on a printer that is certified and accredited to process classified information and provided by IRM to EOIR Security. EOIR Security will forward a stand-alone printer to the immigration court for its use in a case involving classified information, and the court security coordinator will, on receipt, store the printer in the court's approved

security container. When the case is completed at the court level, the printer will be returned to EOIR Security.

b. The printer used to process classified information should, whenever possible, be located in a room to which access can be limited and where processing can be accomplished without being observed or monitored by persons who do not possess the appropriate security clearances and do not have a legitimate need-to-know the information.

c. Once the printer has completed printing any classified document, five pages of an unclassified document or documents should be printed at that printer to clear the printer's memory.

VII. Procedure for Cases Involving Classified Information

A. Notices

1. The Immigration Judge must notify his or her Assistant Chief Immigration Judge and the EOIR Security Office as soon as possible upon learning that a case will involve presentation of classified information. Generally, the Immigration and Customs Enforcement (ICE) Counsel will file a motion stating ICE's intention to present classified information with the Immigration Court and serve the alien with a copy. This motion will be unclassified and will detail the anticipated length of the presentation but will not reveal any details about the nature of the material or its anticipated classification level.

2. The Immigration Judge should direct that the appropriate degree of disclosure is made to the alien according to the type of relief the alien is requesting. Prior to releasing any information to an alien or third party, the Immigration Judge should consult the classifying agency, in coordination with the EOIR Security Office.

3. Asylum Requests

a. When the alien is requesting asylum and the Immigration Judge receives classified information that he or she determines to be relevant to the hearing, the Immigration Judge shall inform the alien. 8 C.F.R. §§ 1240.11(c)(applications for asylum and withholding of removal in removal proceedings); 1240.33(c)(applications for asylum and withholding of deportation in exclusion proceedings); 1240.49(c)(applications for asylum and withholding of deportation in deportation proceedings). The alien should be notified orally at a hearing and on the record, or written notification should be sent to the alien noting that classified information is being received into evidence.

b. The alien must be informed of the use of the classified information, but the classifying agency determines if it will release an unclassified summary of the information. 8 C.F.R. §§ 1240.11(c)(applications for asylum and withholding of removal in removal proceedings); 1240.33(c)(applications for asylum and withholding of deportation in exclusion proceedings); and 1240.49(c)(applications for asylum and withholding of deportation in deportation proceedings).

4. Adjustment of Status Requests

When the alien is requesting adjustment of status and the Immigration Judge receives classified information that he or she determines to be admissible, the Immigration Judge should inform the alien of the general nature of the information so that the alien may have an opportunity to offer opposing evidence. 8 C.F.R. §§ 1240.11(a)(3)(adjustment of status in removal proceedings); 1240.49(a)(adjustment of status in deportation proceedings). Note that prior to releasing any information to an alien or third party, the Immigration Judge should consult with the classifying agency, in coordination with the EOIR Security Office.

5. An Alien's Access to Classified Information

a. An alien must not be provided access to classified information contained in the record or outside the record, unless the classifying authority has agreed in writing to such disclosure. 8 C.F.R. § 103.2 (a)(16)(iv). If the classifying agency authorizes any disclosure of classified information, the agency's certification must be made part of the record.

b. An alien must be notified that classified evidence will be presented to the Immigration Judge. While notice should be given prior to and following any presentation of classified evidence, the alien should not be advised of the identity(ies) of the agency(ies) or witness(es) providing classified information, nor of the dates(s) and time(s) of such presentations.

B. Custody and Bond Redetermination

1. A custody or bond proceeding in which Immigration and Customs Enforcement (ICE) intends to present classified information must be recorded. The tapes of the proceedings must be labeled to indicate the appropriate security classification level (*i.e.*, CONFIDENTIAL, SECRET, or TOP SECRET) of the information presented. When not being used, the tapes will be stored in a GSA-approved security container.

2. Pursuant to 8 C.F.R. § 1003.19(d), "consideration by the Immigration Judge of an application or request of a respondent regarding custody or bond under this section shall be separate and apart from, and shall form no part of, any deportation or removal hearing...." However, "the determination of the Immigration Judge as to custody status or bond may be based upon any information that is available to the Immigration Judge or that is presented to him or her by the alien or the Service." This includes classified information that ICE offers for consideration.

3. If classified materials are placed in the record, the Immigration Judge must ensure that appropriate procedures are followed to ensure that the classified information is not viewed by those who do not have the appropriate security clearance and need-to-know. The information should be placed in an envelope separate from any unclassified information and labeled with the correct level of classification on the outside of the envelope. The information must then be stored in a GSA-approved security container. If the Immigration Judge determines that it is necessary to take notes, any notes containing classified information must be dated when created, marked top and bottom with the highest level of classification contained in the notes, and stored in a GSA-approved security container. Once the notes are no longer needed, they should be destroyed using a cross-cut shredder. *See* section IX, Final Disposition and Destruction.

4. If a written bond memorandum is required and classified information is a basis for the decision, the Immigration Judge should follow the procedures as outlined for written decisions. *See* section VII, part F, Final Decision by an Immigration Judge.

5. If the bond and custody determination is appealed, the transmittal of any classified information must be transmitted in compliance with the security procedures listed below. *See* section VIII, Transmittal of Classified Information.

C. Pre-hearing Conference

Any party may move for a pre-hearing conference to consider matters relating to classified information that may arise in connection with the immigration proceedings. Following such motion, or on its own motion, the Court will hold a pre-hearing conference to consider any matters which relate to classified information or which may promote a fair and expeditious hearing. 8 C.F.R. § 1003.21.

D. Motion for an *In Camera* Hearing

The ICE Counsel may request that the Court conduct an *in camera* hearing to make determinations concerning the use, relevance, or admissibility of classified information that would otherwise be made during the hearing or pre-hearing proceedings. 8 C.F.R. §§ 1240.9 and 1240.47. Upon such a request, the Court shall conduct such an *in camera* hearing. The Court may hold *in camera* hearings for the presentation of classified information during the course of proceedings.

1. Any hearing held pursuant to this subsection (or any portion of such hearing specified in the ICE request) shall be held *in camera* if the ICE Counsel certifies to the Court in its motion that a public proceeding may result in the disclosure of classified information. *See Jay v. Boyd*, 351 U.S. 345 (1956) (upholding denial of suspension of deportation based upon confidential information undisclosed to the petitioner).

2. An alien must be notified of an *in camera* hearing or review of classified evidence. An alien must be notified that classified evidence will be presented to the Immigration Judge. While notice should be given prior to and following any presentation of classified evidence, the alien should not be advised of the identity(ies) of the agency(ies) or witness(es) providing classified information, nor of the dates(s) and time(s) of such presentations.

3. At the close of an *in camera* hearing, or any portion of a hearing that is held *in camera*, that concerns classified information, the record of that hearing must be marked like a final document, sealed, labeled with the classification level, and stored by the Court in a GSA-approved security container for use in the event of an appeal.

E. Hearings

1. Testimony

Whenever classified testimony is taken and proceedings are recorded, tapes used to record the proceedings must be labeled to indicate the appropriate security classification (*i.e.*, CONFIDENTIAL, SECRET, or TOP SECRET). The tapes shall be stored in a GSA-approved security container when not being used. If a transcript of the tapes is required, the Court must forward the tapes to the EOIR Security Office following the transmittal procedures set forth in Section VIII below. Transcripts of tapes containing classified information will be forwarded by the Security Office to the appropriate agency(ies) for required classified markings.

2. Note-Taking

Court personnel should avoid taking notes that contain classified information extracted from classified documentary evidence or oral testimony. If it becomes necessary to take notes, it is recommended that two sets of notes be maintained; one set containing only unclassified information and one set containing any classified information. The notes that contain any classified information shall be considered working papers. Working papers must be:

- dated when created;
- marked with the highest classification level of information they contain;
- maintained in a GSA-approved security container; and
- destroyed when no longer needed.

3. Access to Hearings

a. No person without the requisite level of security clearance and a need-to-know shall be allowed access to any hearings where classified information will be discussed. This includes the exclusion of the alien and the alien's representatives. *See, e.g., Jay v. Boyd*, 351 U.S. 345 (1956).

b. To prevent the alien from being unnecessarily excluded from all portions of the hearing, the Immigration Judge should schedule a separate hearing time to hear classified information.

c. The Immigration Judge should ensure that the courtroom is cleared of all persons without an appropriate level security clearance during any hearing scheduled for the presentation of classified information. Prior to and following any *in camera* hearing, the alien and his representative(s) should be allowed to present any opposing evidence.

F. Final Decision by an Immigration Judge

1. Form of the Decision

An Immigration Judge must render a written decision.

2. Written Decision Involving Classified Information

a. If it is necessary to include specific classified information as part of a decision, the classified information should be drafted as an attachment so that the decision itself may be released to the public. The Immigration Judge must confine any classified information to the classified attachment. The decision should state that the “attached” classified information was a factor in that decision. The following procedures must, to the extent possible, be observed in “marking,” or labeling, the classified attachment:

- A cover sheet showing the classification level must be attached to the document.
- Overall Classification Marking: The overall classification is the highest classification level of information contained in the document. Conspicuously place the overall classification at the top and bottom of the page. When using a computer, these markings can be entered as headers and footers.
- Portion Marking: Subjects, titles and paragraphs shall be marked to show the level of classified information contained in that portion. Indicate classification level immediately preceding or following the portion to which it applies: (TS) for Top Secret; (S) for Secret, © for Confidential; and (U) for Unclassified.
- “Derived from” Line: The information on this line is obtained from the source document used in the proceedings.
- “Declassify on” Line: The information on this line is obtained from the source document used in the proceedings.

b. For a detailed explanation and illustration of the above markings, see the booklet, “Marking,” published by the Information Security Oversight Office. The briefing packet provided by the EOIR Security Office contains this booklet.

c. Prior to releasing the decision, the decision and the classified attachment shall be forwarded to the EOIR Security Office following the transmittal procedures set forth in Section VIII below. The Security Office will forward the documents to the agency(ies) which originally provided the classified information, to ensure that no classified information has been disclosed in the decision and that all classified information in the attachment has been marked correctly. The Immigration Judge's analysis and use of substantive law shall not be affected by this review. The role of the classifying agency is strictly to ensure correct marking of any classified information. The agency will not alter the content of the Immigration Judge's decision.

G. Remands

Any remand from the Board of a case including classified information should be handled in accordance with the procedures outlined in this memorandum. All security procedures must be maintained to protect the unauthorized disclosure of any classified material.

VIII. Transmittal of Classified Information

The record on appeal, or any portion thereof, which contains classified information shall be transmitted to the Board in the following manner:

A. Confidential or Secret Information

1. Contact the EOIR Security Office at (703) 605-0348 to obtain the name(s) and telephone number(s) of the appropriate individual(s) at the Board of Immigration Appeals to whom the information is to be transmitted. Then notify the Chief Clerk, Board of Immigration Appeals, at (703) 605-1077, that the information will be transmitted. Classified information shall be transmitted and received in an authorized manner which ensures that evidence of tampering can be detected, that inadvertent access can be precluded, and timely delivery is made to the intended recipient.

2. All classified information physically transmitted shall be enclosed in two layers, both of which provide reasonable evidence of tampering and conceal the contents. The inner enclosure shall clearly identify the address of both the sender and the intended recipient, the highest classification level of the contents, and any appropriate warning notices. A classified document receipt, Form DOJ-34, may then be attached to the outside of the inner envelope. Care should be taken to ensure that the document receipt itself does not contain any classified information. The outer enclosure shall be the same, except that no markings to indicate that the contents are classified shall be visible. The name of the intended recipient may only be used as part of an attention line.

3. For classified information at the Confidential or Secret level, this double-wrapped package must be transmitted by United States Postal Service (USPS) Registered Mail, Return Receipt Requested, or by USPS Express Mail, Return Receipt Requested. Packages must

be hand-carried to the Post Office. Do not use a street-side mail collection box. The Waiver of Signature and Indemnity Block, Item 11-B on the USPS Express Mail Label, shall not be completed.

4. If a package containing classified information is to be sent to the Board, notify the individual to whom it is addressed of the estimated date of arrival.

B. TOP SECRET Information

Any record containing TOP SECRET information cannot be mailed and must be double-wrapped as described above. This package must be hand-carried from the court to its destination by an individual cleared at the Top Secret level. Special arrangements will have to be made for the transport of any material containing Top Secret material to the Board, and the sending Court should contact the EOIR Security Office for assistance.

IX. Final Disposition and Destruction

A. Return Original Classified Documents

Original classified documents obtained from other Federal departments or agencies should be returned to the classifying agency when they are no longer needed by the Court. Classified decisions or documents created by the Courts should be retained in appropriate storage until archived. [See procedures for transmission and storage above.]

B. Destroy Copies of Classified Information

Copies of classified information (*e.g.*, drafts, working papers and notes, waste from reproduction, extra copies, compact discs, and DVD's, etc.) should be destroyed as soon as the documents or materials are no longer needed. Strip shredders are not authorized for destruction of classified material. An approved cross-cut shredder producing residue which does not exceed 1 mm in width and 5 mm in length must be used to destroy the classified material. The EOIR Security Office will provide cross-cut shredders to the Courts as needed.

C. Storage Until Destruction

Until a cross-cut shredder can be used to destroy the classified material, all classified waste materials must be stored in a GSA-approved security container. Once the material has been shredded, the residue may be disposed of with unclassified waste material.

D. Archiving Classified Evidence

1. The form used to archive records, SF-135, must indicate the classification level of the classified records being archived and the Records Center must be notified that a cleared driver will be required to transport the materials. Otherwise, the procedures for archiving Secret and Confidential records are substantially the same as for unclassified records.

2. Records containing TOP SECRET material must be transported from the Courts to the Records Center by the Defense Courier Service.

3. Classified records should, where possible, be segregated from unclassified material in separate boxes.

If you have any questions regarding the procedures outlined in the OPPM, please contact your Assistant Chief Immigration Judge or my Chief Counsel at (703) 305-1247.

APPENDIX - RELEVANT AUTHORITY

I. Executive Order

“Classified National Security Information,: Executive Order 12958 (1995), as amended.

II. Regulatory Provisions Pertaining to Classified Issues

A. Classified National Security Information and Access to Classified Information, 28 C.F.R. § 17, *et. al.*

B. Aliens and Nationality, 8 C.F.R. § 103.2(b)(16) - Inspection of evidence. An applicant or petitioner shall be permitted to inspect the record of proceeding which constitutes the basis for the decision, except as provided in the following paragraphs. . . . (iv) Classified information. An applicant or petitioner shall not be provided any information contained in the record or outside the record which is classified ... as requiring protection from unauthorized disclosure in the interest of national security, unless the classifying authority has agreed in writing to such disclosure. Whenever he/she believes he/she can do so consistently with safeguarding both the information and its source, the regional commissioner should direct that the applicant or petitioner be given notice of the general nature of the information and an opportunity to offer opposing evidence. The regional commissioner's authorization to use such classified information shall be made a part of the record. A decision based in whole or in part on such classified information shall state that the information is material to the decision.

8 C.F.R. § 103.22(b)(1) - Access to records. A request for information classified by the Service ... on National Security Information requires the Service to review the information to determine whether it continues to warrant classification under the criteria of the Executive Order. Information which no longer warrants classification shall be declassified and made available to the individual, if not otherwise exempt. If the information continues to warrant classification, the individual shall be advised that the information sought is classified; that it has been reviewed and continues to warrant classification

8 C.F.R. § 103.23 (a) - Records of other agencies. When information sought from a system of records of the Service includes information from other agencies or components of the Department of Justice that has been classified ..., the request and the requested documents shall be referred to the appropriate agency or other component for classification review and processing. Only with the consent of the responsible agency or component, may the requester be informed of the referral as specified....

C. Aliens and Nationality, 8 C.F.R. § 1240 - Proceedings to Determine Removability: Regulations Relating to Adjustment of Status

8 C.F.R. § 1240.11(a)(3) - Removal proceedings. In exercising discretionary power when considering an application for status as a permanent resident under this chapter, the immigration judge may consider and base the decision on information not contained in the record and not made available for inspection by the alien, provided the Commissioner has determined that such information is relevant and is classified under the applicable Executive Order as requiring protection from unauthorized disclosure in the interest of national security. Whenever the immigration judge believes that he or she can do so while safeguarding both the information and its source, the immigration judge should inform the alien of the general nature of the information in order that the alien may have an opportunity to offer opposing evidence. A decision based in whole or in part on such classified information shall state that the information is material to the decision.

8 C.F.R. § 1240.49(a) - Deportation proceedings. The respondent may apply to the immigration judge for suspension of deportation under section 244(a) of the Act; for adjustment of status under section 245 of the Act, or under section 1 of the Act of November 2, 1966, or under section 101 or 104 of the Act of October 28, 1977; or for the creation of a record of lawful admission for permanent residence under section 249 of the Act. ... In exercising discretionary power when considering an application under this paragraph, the immigration judge may consider and base the decision on information not contained in the record and not made available for inspection by the respondent, provided the Commissioner has determined that such information is relevant and is classified under the applicable Executive Order as requiring protection from unauthorized disclosure in the interest of national security. Whenever the immigration judge believes that he or she can do so while safeguarding both the information and its source, the immigration judge should inform the respondent of the general nature of the information in order that the respondent may have an opportunity to offer opposing evidence. A decision based in whole or in part on such classified information shall state that the information is material to the decision

D. Regulations Relating to Asylum and Withholding of Deportation

8 C.F.R. § 1240.11(c)(3)(iv) - Removal proceedings. Service counsel may call witnesses and present evidence for the record, including information classified under the applicable Executive Order, provided the immigration judge or the Board has determined that such information is relevant to the hearing. When the immigration judge receives such classified information, he or she shall inform the alien. The agency that provides the classified information to the immigration judge may provide an unclassified summary of the information for release to the alien, whenever it determines it can do so consistently with safeguarding both the classified nature of the information and its sources. The summary should be as detailed as possible, in order that the alien may have an opportunity to offer opposing evidence. A decision based in whole or in part on such classified information shall state whether such information is material to the decision.

8 C.F.R. § 1240.33(c)(4) - Exclusion proceedings. The Service counsel for the government may call witnesses and present evidence for the record, including information classified under the applicable Executive Order, provided the immigration judge or the Board has determined that such information is relevant to the hearing. The applicant shall be informed when the immigration judge receives such classified information. The agency that provides the classified information to the immigration judge may provide an unclassified summary of the information for release to the applicant whenever it determines it can do so consistently with safeguarding both the classified nature of the information and its source. The summary should be as detailed as possible, in order that the applicant may have an opportunity to offer opposing evidence. A decision based in whole or in part on such classified information shall state that such information is material to the decision.

8 C.F.R. § 1240.49 (c)(4)(iv) - Deportation proceedings. The Service counsel for the government may call witnesses and present evidence for the record, including information classified under the applicable Executive Order, provided the immigration judge or the Board has determined that such information is relevant to the hearing. When the immigration judge receives such classified information he or she shall inform the applicant. The agency that provides the classified information to the immigration judge may provide an unclassified summary of the information for release to the applicant, whenever it determines it can do so consistently with safeguarding both the classified nature of the information and its source. The summary should be as detailed as possible, in order that the applicant may have an opportunity to offer opposing evidence. A decision based in whole or in part on such classified information shall state whether such information is material to the decision.

III. Booklets and Secondary Materials

A. Department of Justice Security Program Operating Manual, available on the Department of Justice Intranet at:

<http://10.173.2.12/jmd/seps/spom.html>

B. Marking, published by the Information Security Oversight Office of the National Archives and Records Administration. A copy of this booklet should have been included in your Security Clearance Packet. The booklet is a general guide on marking classified information in order to place recipients of the information on alert about its sensitivity. Additional copies may be obtained from the EOIR Security Office.