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

December 28, 1998

MEMORANDUM

TO: Immigration Judges
Judicial Law Clerks
Court Administrators
Court Staff

FROM: The Office of the Chief Immigration Judge

SUBJECT: Operating Policy and Procedures Memorandum OPPM 98-10: Classified Information in Immigration Court Proceedings (replacing previous OPPM 98-5 of the same title and dated July 21, 1998)

This OPPM 98-10 cancels OPPM 98-5, dated July 21, 1998, and provides new instructions.

The handling of classified information by the Immigration Courts requires that certain procedural safeguards are followed to protect the nature and source of the information. The following procedures are a guide to the proper handling of classified information within the Immigration Courts. Whenever circumstances appear to be beyond the scope of this Operation Policy and Procedure Memorandum (OPPM), request the assistance of your Assistant Chief Immigration Judge and the EOIR Security Office.

The purpose of the following procedures is to protect against the unauthorized disclosure of classified information pursuant to the provisions of Executive Orders 12,958, 60 Fed. Reg. 19,825 (1995); 3 C.F.R. 1995, Comp., p. 333 [hereinafter E.O. 12,958], and 12,968, 60 Fed. Reg. 40,245 (1995); 3 C.F.R. 1995, Comp., p. 391 [hereinafter E.O. 12,968], and the regulations implementing these Orders at 28 C.F.R. § 17 (1998). These procedures apply to Immigration Court proceedings involving classified information.

Table of Contents

I. Definitions

Classified information, as used in this OPPM, means any information or material that has been determined by the United States government pursuant to an Executive Order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security. E.O. 12,958, supra, at § 1.1 (c).

There are three levels of classification:

A. 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. E.O. 12,958, supra, at § 1.3 (a)(1);

B. 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. E.O. 12,958, supra, at § 1.3 (a)(2); and

C. 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. E.O. 12,958, supra, § 1.3 (a)(3).

II. Security Coordinator

A. 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 security-cleared Court personnel with regard to classified materials. This includes overseeing the handling of classified information, the transfer 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.

B. 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 the presentation of classified information.

C. **If there is a case involving classified information, the Court Administrator, as Security Coordinator, may designate security 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 a personnel member(s) responsible for ensuring security procedures are followed at each Court that handles classified information.**

D. **The Court Administrator, with the assistance of any security-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 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 down so that all Court personnel may refer to it when necessary.**

III. Personnel Security Clearance

A. Requirements for Access to Classified Information

1. **Court personnel to whom classified cases are assigned must possess the appropriate level of security clearance, and;**

2. **They must have demonstrated a need-to-know the information.**

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. E.O. 12,958, supra, § 4.1(c).**

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 both the appropriate level security clearance 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.

B. Responsibilities to Ensure the Safeguarding of Classified Information

1. No Unauthorized Disclosure of Classified Information

a. Generally

Security-cleared Immigration Judges and Court personnel shall not disclose classified information to anyone who does not have security clearance 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 security-cleared Court personnel so long as each person has the appropriate level security clearance and a legitimate need-to-know the information. Security-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 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 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 Secret, 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. The briefing may be conducted telephonically. 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.

IV. 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, and 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 "A" number. The combination to the security container may be given to any Court employee (Immigration Judge, Judicial Law Clerk, Legal Technician, or Court Administrator) who possesses the appropriate security clearance and requires access to the container.**

3. **Classified material must be kept in secure facilities, meaning that classified materials must not 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 VII, Transmittal of Classified Information, infra.**

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, may be used to track who took the classified material from the security container and when it was returned.**

V. 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 security clearance and does not possess 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 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 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.

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 are removed and disposed of properly. See also section VIII, Final Disposition and Destruction, infra.

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 accredited and approved by the EOIR Information and Program Analysis Office (IPA) in consultation with the EOIR Security Office in Falls Church, Virginia, for the processing of classified information prior to the 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 typed 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 IPA.

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 IPA in Falls Church, Virginia. 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 VII, Transmittal of Classified Information, infra.

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 VII, Transmittal of Classified Information, infra. 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

a. Any classified documents created on the approved laptop computers should be maintained on disks. The information should not be saved on the laptop computer's hard drive. Any disks must be stored according to the security procedures set forth above. The disk 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. A disk containing a copy of a written decision should be treated like a paper reproduction.

b. Disks may be used to transfer information to another security cleared computer so long as the disk is transported in compliance with the security procedures listed below for the transmittal of classified information. See section VII, Transmittal of Classified Information, infra.

c. As soon as a disk is no longer needed for operational needs, it should be destroyed 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 1/32 inch in width by 1/2 inch in length. See section VIII, Final Disposition and Destruction, infra.

5. Printers

a. Any classified attachment or document (e.g., notes containing classified information) should be printed on a printer that is

dedicated to the laptop computer used to process classified information.

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 have a legitimate need-to-know the information.

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

VI. Procedure for Cases Involving Classified Information

A. Notice

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 the presentation of classified information. Generally, the Service will file a motion stating the Service'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.

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. §§ 240.11 (c)(3)(iv)(1998)(applications for asylum and withholding of removal in removal proceedings); 240.33

(c)(4) (1998)(applications for asylum and withholding of deportation in exclusion proceedings); 240.49 (c)(4)(iv)(1998)(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. §§ 240.11 (c)(3)(iv) (1998)(applications for asylum and withholding of removal in removal proceedings); 240.33 (c)(4)(1998)(applications for asylum and withholding of deportation in exclusion proceedings); and 240.49 (c)(4)(iv)(1998)(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. §§ 240.11 (a)(3)(1998)(adjustment of status in removal proceedings); 240.49 (a) (1998)(adjustment of status in deportation proceedings). Prior to releasing any information to an alien or third party, the Immigration Judge should consult with the classifying agency.

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)(1998). If the classifying agency authorizes any disclosure of classified information, the agency's certification must be made part of the record. Id.

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 the Immigration and Naturalization Service 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. § 3.19 (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." Id. This includes classified information that the Immigration and Naturalization Service ("Service") 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 security clearance. 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 an GSA-approved security container. If the Immigration Judge determines that it is necessary to take notes, any notes containing classified information must be marked 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 VIII, Final Disposition and Destruction, infra.

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 VI, part F, Final Decision by an Immigration Judge, infra.

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 VII, Transmittal of Classified Information, infra.

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 trial. 8 C.F.R. § 3.21 (1998).

D. Motion for an In Camera Hearing

The Service 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. INA § 240 (a)(2)(C) (1998); 8 C.F.R. §§ 240.9 and 240.47 (1998). 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 Service's request) shall be held in camera if the Service 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 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 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 VII below. Transcripts of tapes containing classified information will be forwarded by the Security Office to the appropriate agency(ies) for required portion 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;**
- **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 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:

- **Each paragraph must be marked to indicate its classification level;**
- **The top and bottom of each page must be marked to indicate the overall classification level of the document. When using a computer, these can be entered as headers and footers appearing on the top and bottom of every page;**
- **The first page must identify the original classifying authority, the reason(s) for classification, and the date of declassification. These markings can be copied from the classified document(s) used in the proceedings; and**
- **A coversheet showing the classification level must be attached to the document.**

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 VII 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 utilizing classified information should be handled in accordance with the procedures outlined in this memorandum. All security procedures must be maintained in order to protect the unauthorized disclosure of any classified material.

VII. 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. Place classified material in a sealed, opaque envelope. The envelope will be marked top and bottom, back and front, with the classification level of the information of the materials. The addresses of the sender and the recipient will be placed on the envelope.

2. This envelope will be placed into a second sealed, opaque envelope. The addresses of the sender and the recipient, the Board, will be placed on

the envelope. The double-wrapped package must be marked to the personal attention of an appropriately cleared staff member of the Appeals Management Team. Contact the Security Office, at (703)305-1754, to obtain the names and telephone numbers of the appropriate individuals. There shall be no additional markings on this envelope to indicate that classified information is contained within.

3. **This double-wrapped package must be mailed by United States Postal Service Registered Mail, Return Receipt Requested, or by United States Postal Service Express Mail, Return Receipt Requested. Packages must be hand-carried to the Post Office. Do not use a street-side mail collection box.**
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 for Top Secret. 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.

VIII. 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 section VIII; part D - Archiving, infra.

B. Destroy Copies of Classified Information

Copies of classified information (e.g., drafts, working papers and notes, waste from reproduction, extra copies, floppy diskettes, etc.) should be destroyed as soon as the documents or materials are no longer needed. Strip shredders are NOT authorized for the destruction of classified material. An approved cross-cut shredder producing residue which does not exceed 1/32 inch in width by 1/2 inch 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, the 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 Legal Counsel, Michael Straus, at (703)305-1716.

Michael J. Creppy

Chief Immigration Judge

ADDENDUM - RELEVANT AUTHORITY

I. Executive Orders

A. Classified National Security Information, Executive Order No. 12,958 of April 17, 1995, 60 Fed. Reg. 19,825 (1995); 3 C.F.R. 1995, Comp., p. 333.

B. Access to Classified Information, Executive Order No. 12,968 of August 4, 1995, 60 Fed. Reg. 40245 (1995); 3 C.F.R. 1995, Comp., p. 391 [hereinafter E.O. 12,968].

II. Regulatory Provisions Pertaining to Classified Issues

A. Classified National Security Information and Access to Classified Information, 28 C.F.R. § 17 (1998).

B. Aliens and Nationality, 8 C.F.R. § 103 (1998) - Powers of the Service:

8 C.F.R. § 103.2 (b)(16)(iv) - 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 under Executive Order No. 12356 (47 FR 14874; April 6, 1982) [repealed and replaced by E.O. 12958 (60 FR 40245, August 2, 1995)] 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 under Executive Order 12356 [replaced and repealed by E.O. 12958] 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 under Executive Order 12356 [repealed and replaced by E.O. 12958], 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 in section 3.4(f) of Executive Order 12356 [repealed and replaced by E.O. 12958].

C. Aliens and Nationality, 8 C.F.R. § 240 - Proceedings to Determine Removability:

<u>Regulations Relating to Adjustment of Status</u>

8 C.F.R. § 240.11 (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. § 240.49 (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

<u>Regulations Relating to Asylum and Withholding of Deportation</u>

8 C.F.R. § 240.11 (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. § 240.33 (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. § 240.49 (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. Classified National Security Information, Reference Booklet, January 1997, U.S. Department of Justice, Justice Management Division, Security and Emergency Planning Staff, Information Security Policy Group. A copy of this booklet should have been included in your Security Clearance Packet. Additional copies of this booklet may be obtained from the EOIR Security Office or the Special Security Center, Room 6744, MAIN Justice Building.

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.