U.S. Department of Justice

Executive Office for Immigration Review

Board of Immigration Appeals

Chairman

5107 Leesburg Pike, Suite 2400
Falls Church, Virginia 20530

April 22, 2014

BIA 14-02

MEMORANDUM TO: All Board Staff and Contractors

FROM: David L. Neal, Chairman

SUBJECT: Classified National Security Information Document Control

This memorandum contains directives for the receipt and processing of case-related classified National Security Information ("NSI") at the Board of Immigration Appeals ("Board") of the Executive Office for Immigration Review ("EOIR"). This memorandum supersedes any previously issued directives on Classified NSI Document Control.

The handling of classified information at the Board requires that certain procedural safeguards be followed in order to protect the nature and source of the information. In compliance with the regulations concerning classified information, the Board has instituted measures to ensure the protection of the material to provide the necessary equipment, such as safes and approved computers, for handling and reviewing classified information.

Due to the seriousness of classified information, failure to follow the attached outlined procedures, or any breach of classified information, is a serious offense and may result in severe penalties, up to and including criminal charges against the violator.

Should you encounter a case with classified information, consult the appropriate personnel. The appendix to this memo has the names and contact information for personnel cited in this memorandum (and therefore may be more current than the date of this memorandum). This memorandum also addresses the handling of cases that contain classified information which may have been obtained via WikiLeaks.

If you have any questions concerning this memorandum, please contact Senior Legal Advisor Amy Minton at (703) 605-0317.

VII. ORAL ARGUMENT (cont.)

I. WHAT IS CLASSIFIED INFORMATION

A. Definition

Classified National Security Information (hereafter, "classified information" or "classified material") means information that, pursuant to Executive Order 13526 or any predecessor order, has been determined to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

B. Levels of Classification

Executive Order 13526 provides that information may be classified at one of the following three levels.

- **Top Secret**. Unauthorized disclosure of the information could reasonably be expected to cause *exceptionally grave damage* to the national security that the original classification authority is able to identify or describe.

- **Secret**. Unauthorized disclosure of the information could reasonably be expected to cause *serious damage* to the national security that the original classification authority is able to identify or describe.

- **Confidential**. Unauthorized disclosure of the information could reasonably be expected to cause *damage* to the national security that the original classification authority is able to identify or describe.

II. ACCESS TO CLASSIFIED INFORMATION

A. Requirements for Access to Classified Information

An employee's office, position, rank, or security clearance does not automatically render him or her eligible for access to classified information. A person may be given access to classified information *only* if that person meets three criteria:

1. Holds the appropriate clearance.

   To confirm a security clearance level, contact the EOIR Office of Security ("EOIR/OS").

2. Has demonstrated a "need-to-know" the information.

   Need-to-know means that the person seeking access to the classified information needs the information in order to perform (or assist in) a lawful and authorized governmental function.

3. Has signed an appropriate non-disclosure agreement (SF-312).

   Non-disclosure Agreement is kept on file with the EOIR/OS.

B. Responsibility to Ensure the Safeguarding of Classified Information

1. Generally

   All Board employees and contractors are individually obligated to protect classified information. Classified information shall not be disclosed to anyone who does not have the requisite security clearance, has not signed an approved non-disclosure agreement, and does not possess a legitimate need-to-know the information.

   Board employees and contractors must ensure that classified information is discussed only with individuals with both the appropriate level of security clearance and a legitimate need-to-know the information. If the classifying agency authorizes any disclosure of classified information, the agency's certification must be part of the record.

2. Disclosure to Other Board Employees and Contactors

   Classified information may be discussed *only* among those Board employees or contractors who have the appropriate security clearance, signed an approved non-disclosure agreement, *and* have a legitimate need to know the information. Under these circumstances, written certification from the classifying agency to disclose classified information to other Board employees is not required before disclosure is made.

3. Disclosure to Persons outside the Board

   Written certification from the classifying agency is required before any Board employee or contractor may disclose information to aliens, their attorneys, or individuals not employed by the Department of Justice ("DOJ"). Also before any disclosure can be made to a person outside of EOIR, the DOJ Office of Security must receive written certification of that individual's security clearance. The written certification (in redacted form) must also be made part of the record before disclosure may be made.

4. Confirmation of Security Clearance

   Confirmation of your own or another EOIR employee's level of security clearance can be obtained from EOIR/OS on an "as needed" basis.

5. Unauthorized Disclosure

   All Board employees and contractors are responsible for protecting classified information at all times. The unauthorized disclosure of classified information in other media or venues (whether in print, on blog, or on a website) does not affect information's classified status or automatically result in the declassification of that information. In other words, *unauthorized disclosure does not declassify* that information. Classified information remains classified and must be treated as such by federal employees and contractors *until* it has been declassified by the classifying

agency. Contact EOIR/OS immediately when there has been possible loss, compromise, or suspected compromise of any classified information, whether in EOIR's possession or encountered elsewhere.

Unless authorized to do so, Board employees and contractors are not allowed to access information marked or labeled classified. It does not matter if that information is publicly available (e.g., WikiLeaks). It also does not matter if that information is being accessed from a personal computer (e.g., at home, public library) or other device (e.g., Blackberries or Smart Phones). Board employees or contractors who believe that they may have downloaded classified information to non-classified government systems should immediately contact EOIR's Chief IT Security Officer, and provide notification to the EOIR/OS.

6. Discovery of Unauthorized Disclosure

If you become aware of any violation or possible violation of security regulations or security procedures at the Board, you must immediately contact the EOIR/OS which will determine whether further investigation of a violation is required.

7. Penalties for Unauthorized Disclosure

The unauthorized disclosure of classified information is defined in Executive Order 13526 as the communication or physical transfer of classified information to an unauthorized recipient. A violation is defined as any knowing, willful, or negligent action that could reasonably be expected to result in the disclosure of classified information to an unauthorized recipient. Board employees and contractors may be subject to sanctions if they knowingly and willfully allow access to classified information in violation of security regulations or procedures. Sanctions include reprimand, suspension without pay, removal, or termination of security clearance, as well as possible criminal and civil penalties.

III. RECEIPT AND STORAGE OF CLASSIFIED INFORMATION AT THE BOARD

A. Media

Classified information may be stored in any number of media, including but not limited to: paper documents, recorded testimony, audio tapes, compact disks (CDs), and portable drives (e.g., thumb drives, flash drives, and portable hard-drives) and must be labeled with the appropriate security classification (i.e., CONFIDENTIAL, SECRET, or TOP SECRET). The media shall be stored in the Board's safe in the Restricted Access Room.

B. Advance Notice that Classified Information is Being Sent to the Board

The entity transmitting the information to the Board – the immigration court or the Department of Homeland Security ("DHS") – is supposed to give the Board and EOIR/OS advance notice that classified material is being forwarded.[1]

Any Board personnel who are contacted by the immigration court or by the DHS regarding the transmission of classified information to the Board must contact the Chief Clerk, a Deputy Chief Clerk, or the Classified Case Coordinator at the Office of the Clerk ("Clerk's Office") immediately.

C. Instructions for Receipt of Classified Materials at the Clerk's Office

The immigration courts have been given specific procedures for the sending and receiving of classified information. Thus, an immigration court is not supposed to send classified information directly to the mail room of the Clerk's Office, nor should a court be sending classified information electronically.

When an immigration court sends classified information at the Confidential or Secret level to the Board, the mailing will be sent through U.S. Postal Service ("USPS") via Registered Mail, Return Receipt Requested, USPS Express Mail. Return Receipt Requested, or through FedEx. The court is supposed to provide the tracking number of the package to the Board in advance of its arrival, so that the Classified Case Coordinator can monitor the package.

After arrival at our local Post Office, the package will be picked up by a designated person from the Clerk's Office, and that person will *immediately* hand-carry the package to the Classified Case Coordinator or other designated person. The package may *never* be left on that person's desk.

The Classified Case Coordinator will then place the classified information in a GSA-approved security container (e.g., safe) in the Restricted Access Room on the 24th floor of the Tower or temporarily in an authorized designated safe in the Clerk's Office. The log book (which is kept in the Restricted Access Room) must be updated to reflect the receipt of the materials, along with a description and date.

Once the classified materials arrive at the Board, the Case Access System for EOIR ("CASE") must be updated by the Classified Case Coordinator to reflect its arrival.

- The CASE identifier "Secure Access Case" must be selected under the Appeals Tab, General Appeal Information, Special Issue.

- Verification of Secure Access coding by the immigration court in CASE under the Case Info Tab, Secure Access Status.

[1] The Office of the Chief Judge has issued an Operating Policies and Procedures Memorandum for Classified Information in Immigration Court Proceedings (OPPM 09-01). That memorandum is available on the EOIR website at www.justice.gov/eoir.

- The Comments screen in CASE also must have notations using the identifier "Secure Access Case" to (1) reflect receipt of the classified information, and (2) advise that inquiries and correspondence in the case are to be directed to the Classified Case Coordinator.

D. Secure Access Report

The Classified Case Coordinator will maintain a report that monitors and tracks all cases with classified material from the time it is received at the Board until it is archived. The monthly report shall be made part of the Board's permanent record keeping, but it will not include any classified information. Also, the report will be distributed to designated senior managers. The report will also be made available to the EOIR/OS upon their request.

E. Restricted Access Room

Classified information must be kept in the "Restricted Access Room" located on the 24th floor of the Skyline Tower.

1. Access to the Restricted Access Room

   The Restricted Access Room is alarmed 24 hours a day/ 7 days a week, and is monitored by Kastle Alarm Systems. The door to the Restricted Access Room has a card reader on the wall to enable permitted access. EOIR/OS staff, the Classified Case Coordinator, designated Senior Legal Advisor, and other designated personnel are authorized to access the Restricted Access Room.

2. Contents of the Restricted Access Room

   The Restricted Access Room contains several GSA-approved security containers or "safes" (with one safe designated for the Board), two desks, two stand-alone computers approved for the processing of classified information (and equipped with removable hard-drives to be stored in a GSA-approved security container when the computer is not in use), a laptop (assigned to the Board, approved for the processing of classified information, and stored in the designated Board safe), a dedicated printer (i.e., not networked/connected to any other computers), a dedicated copier (not networked), a phone (for routine use), Secure Terminal Equipment (STE) (which consists of a phone and a facsimile that can be used to transmit classified information), a table, chairs, and a cross-cut shredder.

   Computers used to process classified information must be accredited and approved for the processing of classified information. *Prior* to the initiation of any processing, contact EOIR's Chief IT Security Officer to ensure that computers are accredited and approved.

3. Posted Procedures

   Procedures for handling classified information materials must be posted.

4. Admittance in the Restricted Access Room and Record Log

   Access to the Restricted Access Room shall be made by appointment with one of the designated individuals from the Clerk's Office, the designated Senior Legal Advisor, or the EOIR/OS.

   Any admittance into the Restricted Access Room shall be recorded in the Restricted Access Room log book. This log book shall reflect who was admitted into the room, the time and date of admission, and the time of departure. Also, the Restricted Access Room log book shall be used to record who accessed the safe, what material was reviewed, and what material was added/or removed from the safe. No classified information shall be recorded in this log book.

   In addition, Security Container Check Sheet (SF-702) will be maintained to reflect who accessed the safe, the time, and the date of access. The SF-702 will also reflect who closed the safe, the time, and the date. The SF-702 shall not include classified information.

   Use of the accredited and approved laptop assigned to the Board shall be recorded in the EOIR Classified Computer Usage log. This log shall reflect who used the laptop assigned to the Board as well as the time and date of usage. The log shall not include classified information.

   Upon completion of a classified case/document review, the following actions must take place: (i) the classified materials must be placed back in the safe, (ii) the time of the completion must be entered in the log book in the safe, (iii) the safe must be locked, (iv) the time of that person's departure must be recorded, and (v) the Restricted Access Room must be closed and locked.

5. Removal of Classified Material

   Classified material/information cannot be removed from EOIR Headquarters and taken to a personal residence under any circumstances. Removal of classified material from EOIR Headquarters must comport with the directives of Sections III (regarding receipt and storage of classified information) and IX (regarding transmittal of classified information).

IV. RECORDS THAT CONTAIN CLASSIFIED NSI

As a practical matter, it seldom happens that an entire record of proceedings ("ROP") is classified. The following procedures apply generally when an unclassified ROP contains classified information.

A. Receipt of Notice of Appeal

The Notice of Appeal ("NOA") will initially be received by the Priority Case Management Team, the Eastern Team Region, or the Western Team Region. If an unclassified ROP contains classified materials, the Classified Case Coordinator is to take over the processing of the case. These cases should always be handled on an expedited basis, even if the respondent is not detained.

B. Completion of Briefing Schedule/Case Assignment

Upon completion of the briefing schedule, the Classified Case Coordinator will advise the designated Senior Legal Advisor that the matter is ready for adjudication. The Senior Legal Advisor will then contact the Chairman and/or Vice Chairman regarding the assignment of the case to a Panel comprised of Board Members with the requisite security clearance. Also, the Senior Legal Advisor will contact the Director of Operations and the Senior Panel Attorneys for assignment of the case to a Senior Legal Advisor or staff attorney with the requisite security clearance.

The designated Senior Panel Attorney and/or Team Leader is responsible for advising the staff attorney assigned to the case of the classified nature of the case. The attorney will be advised by the Senior Panel Attorney and/or Team Leader that, if review of the classified information is necessary for the disposition of the case, the attorney must first contact the Classified Case Coordinator or other designated Board personnel for admission into the Restricted Access Room.

The non-classified portion of the ROP shall be hand-delivered to the designated attorney after that individual has met with the designated Senior Panel Attorney and/or Team Leader.

C. Review of the Non-Classified Portion of the Record

The non-classified portion of the ROP may be stored in Board Member or attorney offices unless it is determined that they are to be kept in the Restricted Access Room. However, none of the ROP, even the unclassified portions, may be physically removed from the Board workspace. If any part of an ROP is classified, the entire ROP must be reviewed and remain on-site at all times.

D. Review of Classified Material

Where review of the classified information is necessary to adjudicate a case, the assigned Board Members and/or staff attorney must contact the Classified Case Coordinator or other designated Board personnel for admission into the Restricted Access Room. The designated Board Panel Members or attorney *may not* remove classified information from the Restricted Access Room. *See also* Section VI. D. (regarding notes of classified information).

E. Preparation and Circulation of Proposed Board Decision

A laptop and printer in the Restricted Access Room has been designated for the Board's use for preparation of the Board's decision. Only the laptop and printer located in the

Restricted Access Room may be used to prepare the Board's decision. *See also* Section VI. B. (regarding computer security). The Board's decision/order *may not* be removed from the Restricted Access Room.

When the proposed Board decision/order is ready to be reviewed by the designated Board Members, a circulation sheet should be prepared and placed on top of the proposed decision. Also, the staff attorney should advise the designated Board Members that the Board decision/order has been prepared and is ready for review in the Restricted Access Room. The designated Board Members must contact the Classified Case Coordinator or other designated Board personnel for admission into the Restricted Access Room to review the decision.

V. RECORDS THAT ARE COMPLETELY CLASSIFIED

If the entire record of proceedings (ROP) is classified, all ROPs will be placed and kept in the Restricted Access Room at all times while at the Board. All processing by the Classified Case Coordinator will be conducted in the Restricted Access Room. Review of the classified information by the designated Board Panel Members and/or staff attorney assigned to prepare the Board's decisions will also be conducted in the Restricted Access Room.

VI. PROCESSING CLASSIFIED INFORMATION

A. Transcription

The Board's transcription contract has provisions limiting transcription to contractors of the proper clearance and the work performed in the Restricted Access Room. Before the transcription contractor will be given access to the classified material, EOIR/OS must confirm the clearance level of that particular contractor. This can be accomplished by providing the designated contractor's name, social security number, date and place of birth to the EOIR/OS; or the Contracting Officer's Technical representative ("COTR") may submit a request to the contract Facility Security Officer, who then submits a clearance certification to the EOIR/OS.

Completed transcripts are reviewed for marking by the classifying agency. The Board will forward the completed transcripts to the EOIR/OS, which is responsible for forwarding transcripts to the Department's National Security Division and the original classifying agency for the required review and classification markings. The EOIR/OS will contact the Board when the classifying agency has completed its review and returned the transcripts to EOIR.

B. Computer Security

Prior to processing classified information, all computers and printers in the Restricted Access Room must be certified, accredited, and approved by EOIR's Chief IT Security Officer, in consultation with the EOIR/OS.

1. Laptop. A laptop has been designated for the Board's use, and must be stored in the safe assigned to the Board when not in use. Only the laptop and printer in the Restricted Access Room may be used for transcribing classified information. Similarly, only this equipment may be used for preparing the Board's decision or any other document containing classified information from that case (e.g., notes).

2. Printer. The printer's memory buffer must be cleared at the end of that day's work. When a print job has been completed, the user must print another five pages of *unclassified* information to clear the buffer.

3. Copier. A standalone copier is located in the Restricted Access Room. This copier may be used to copy classified information, when necessary. *See* Sections VI. D. and VI. E. (regarding reproduction rules). The copier's memory buffer must be cleared at the end of each use and, therefore, the user must copy an additional five pages of an *unclassified* document to clear the buffer.

C. Review of Record of Proceedings

Where a record of proceedings (ROP) is deemed classified, any and all review of the ROP must take place in the Restricted Access room.

D. Notes of Classified Materials

Board employees should avoid taking notes (extracting information from classified documentary evidence or oral testimony) of classified information. Notes include paraphrasing or restating classified information. If it becomes necessary to take notes, then two sets of notes should 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 to reflect when they were created,
- marked with the highest classification level that applies to any of the information therein,
- protected at the highest level of classification,
- maintained in a GSA-approved security container (i.e., the safe in the Restricted Access Room), and
- completely destroyed when no longer needed.

Under circumstances unlikely to apply at the Board, working papers must be "marked" in the same manner as any classified attachment to the Board's decision. *See* Section VIII. (regarding the Board's decision).

E. Reproductions / Copies

Unless restricted by the originating agency, classified information may be reproduced, but *only* to the extent required by operational needs. Copies of classified information are subject to the same controls as the original information. Reproduction may only be performed by authorized persons (who must be knowledgeable of the procedures for

classified reproduction), and only standalone copiers that have been cleared and approved by the DOJ Security Officer may be used. Networked copiers may *not* be used to copy classified information.

F. Oral Discussions

Meetings at which classified information will be discussed must be held in an area that affords sufficient security against unauthorized disclosure. Participants should take precautions against being overheard or observed by a person who does not have the requisite security clearance or possess a genuine need-to-know the information.

G. Telephone and Facsimile

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 Terminal Equipment ("STE") or Secure Telephone Units (commonly referred to as STU-IIIs) and associated secure facsimile machines. A STE phone and facsimile machine are located in the Restricted Access Room for the Board's use. Contact the EOIR/OS if access to the STE is required.

VII. ORAL ARGUMENT

If classified information must be presented to, or discussed with, Board Members during an Oral Argument ("OA"), the information must be presented or discussed *in camera*. DHS must request *in camera* proceedings by certifying that a public proceeding may result in the disclosure of classified information.

A. Notification

If an *in camera* hearing or review of the classified evidence will take place, the alien must be notified that classified evidence is being presented to the Board. The notice should be given both prior to and following any presentation of classified evidence, the alien and the alien's attorney should not be advised of the identities(ies) of the agency(ies) or witness(es) providing classified information, nor should the alien be advised of the date(s) and time(s) of such presentations.

At the close of an *in camera* hearing, or any portion of a hearing that is held *in camera*, concerning classified information, the record of that hearing must be labeled with the proper classification level, sealed, and stored in the Board safe in the Restricted Access Room.

B. Access to OA

If classified information is to be discussed in the course of an OA, no one may be present in the OA room without both the appropriate security clearance and a legitimate need-to-know.

C. Recording

The Board will not use Digital Audio Recording ("DAR") technology to record an OA involving classified information. In such instances, the recording should be made on analog cassette tapes. The cassettes used during this portion of the OA must be labeled with the appropriate security classification (i.e., CONFIDENTIAL, SECRET, or TOP SECRET). The cassettes shall be stored in the Board's safe in the Restricted Access Room.

D. Transcription

If OA tapes need to be transcribed, the transcription will be conducted in the Restricted Access Room by a contractor who possesses the appropriate security clearance. The EOIR/OS must confirm the level of security clearance of the specific transcriber before access to the classified material will be allowed.

E. Classification / Marking and Review

The procedures for marking and review of the transcripts of the OA by the original classifying agency are the same as outlined in Section VIII. B., Classifying Agency Review, of this memorandum.

F. Note-taking

Any written material created during the *in camera* proceedings will be treated as "working papers" and therefore must be dated when created, marked with the highest classification level of any information contained in them, protected at that level, stored in the Board safe in the Restricted Access Room, and destroyed when no longer needed. *See* Section VI. D. (regarding notes of classified information).

VIII. RENDERING A BOARD DECISION IN A CASE INVOLVING CLASSIFIED INFORMATION

A. Generally

All Board personnel must take great care not to disclose any classified information in rendering of any Board decision. If the classified information must be discussed in a decision, the classified information should be discussed in a separate attachment so that the non-classified portion of the decision may be released. The decision should state that there is a classified attachment and that the classified information relied upon was material and considered in making the decision.

B. Classifying Agency Review

The classifying agency is responsible for reviewing the Board's signed decision and the classified attachment, if any, to make sure that the classified information has been properly segregated from the non-classified decision. It is the responsibility of the EOIR/OS to forward a copy of the Board's decision and classified attachment, if any, to the Department's National Security Division for classification review, and then to the agency that originally classified the information. It may be necessary to also provide a copy of the Immigration Judge's decision to the classifying agency for review. Note that the Board's decision shall not be affected by the classifying agency review. Rather, the role of the classifying agency is strictly to ensure that the classified information is correctly marked and to provide a redacted version of the Board's decision.

C. Marking or Labeling Classified Attachment of the Board's Decision

The classifying agency shall mark the classified attachment of the Board's decision as follows:

1. Portion Marking. Each paragraph will be marked to indicate its classification level via a parenthetical symbol immediately preceding or following the portion to which it applies. The classification level symbols are: (TS) for Top Secret; (S) for Secret; (C) for Confidential; and (U) for Unclassified.

2. Overall Classification Marking. The highest classification level of any information contained in the document will be placed at the top and bottom of each page of the document. There will be a "Derived from" line to indicate the source, and a "Declassify on" line which will indicate the duration of the classification.

3. Cover Sheet. A front and back cover sheet will show the overall classification level (top and bottom of the page).

For a detailed explanation and illustration of the above markings, see the booklet, "Marking Classified National Security Information" published by the Information Security Oversight Office. The document is available at the EOIR Security Office as well as online at www.archives.gov/isoo.

D. Disclosure to Alien and Unclassified Summaries

Where classified information is used in a case involving an asylum issue or an adjustment of status case, the alien must be informed of this fact. *See* 8 C.F.R. §§ 1240.11(c)(3)(iv), 1240.33(c)(4), 1240.49(c)(4)(iv) (asylum; 8 C.F.R. §§ 1240.11(a)(3), 1240.49(a) (adjustment). At no time, however, should an alien or third party be provided access to classified information unless the classifying agency authorizes any disclosure. Also, the agency that provides the classified information to the Immigration Judge, or the Board during an Oral Argument, may provide an unclassified summary of the information for release to the alien.

IX. TRANSMITTAL OF CLASSIFIED INFORMATION

Classified information must be transmitted and received in an authorized manner that ensures evidence tampering will be detected, that inadvertent access will be precluded, and that timely delivery to the intended recipient will be ensured. The record of proceedings ("ROPs"), tapes, or other documentary evidence containing classified information must be sent from the Board to an immigration court in the following manner:

A. Confidential or Secret Information

1. EOIR/OS. Contact the EOIR/OS to confirm that the EOIR employee you are sending classified information has the appropriate level security clearance. Usually, this will be the Court Administrator of the immigration court.

2. Wrapping. The classified material must be wrapped or covered in two opaque layers, both of which will not only conceal the contents but also provide reasonable evidence of any attempted tampering. The inner wrapping or cover must clearly identify (i) the name and address of the sender, (ii) the name and address of the intended recipient, (iii) the highest classification level of the contents marked on the top and bottom, front and back, and (iv) any appropriate warning notices. The outer enclosure shall be the same, except that there should be no indication that the contents are classified (i.e., no markings). The name of the intended recipient may be used only as part of an attention line.

3. Transmittal. For classification information at the confidential and secret level, the double-wrapped package must be transmitted by the United States Postal Service – either by Registered Mail, Return Receipt Requested, or Express Mail, Return Receipt Requested; however, the Waiver of Signature block on the USPS Express Mail Label must *not* be completed. FedEx may also be used, but other commercial carriers are prohibited. Packages must be hand-carried to the Post Office; street collection boxes may never be used.

4. Notify Receiver. The Classified Case Coordinator will notify the Court Administrator of the immigration court (or other designated individual) that the package containing the classified information is en route and will provide the tracking number. The Classified Case Coordinator will also monitor the tracking number to ensure that the package is received.

B. Top Secret Information

The same wrapping procedures addressed in section A.2 above shall be followed, except that classified material containing Top Secret information *cannot* be mailed or sent by commercial carrier. Material containing Top Secret information must *always* be hand-carried to the immigration court or other destination by an individual cleared at the Top Secret security level and designated as a classified courier. The EOIR/OS must be contacted for assistance in making the special arrangements for the transport of any material containing Top Secret information to and from the Board.

X. FINAL DISPOSITION AND DESTRUCTION

A. Return to Office of the Clerk Following Board Review

Upon completion of the Board's review, the non-classified record of proceedings ("ROPs") must be forwarded to the Classified Case Coordinator. The ROPs should not be returned to the Docket Team or Case Storage Team.

B. Destruction of Reproductions

Copies of classified information (such as drafts, working papers, notes, waste from reproduction, extra copies, and diskettes) which are no longer required for operational purposes must be destroyed by shredding in the cross-cut shredder in the Restricted Access Room. Bags containing the remains of shredded classified information may then be disposed of with unclassified waste material. Otherwise, classified waste materials must be stored in the Restricted Access Room until destruction can be accomplished.

C. Access to Board Decisions

A hard copy of the non-classified Board decision will be served on the parties. However, a hard copy of the Board's decision will not be available in the Public Reading Room, nor will an electronic version be available via eDecisions on the EOIR Intranet. A coversheet referring interested persons to contact the Chief Clerk or Deputy Chief Clerk will be scanned by the Classified Case Coordinator or other designated person and made available via eDecisions.

D. Return to the Immigration Court

Classified materials which are part of the ROPs will remain with the file rather than be returned to DHS. However, the unclassified portion of the ROPs may be returned to the immigration court using routine mail handling. All classified portions of an ROP must be returned under the guidelines in Section IX. (regarding transmittal of classified information).

E. Archiving

Archiving ROPs will be the responsibility of the immigration court or DHS.

XI. CERTIFICATION OF CLASSIFIED DOCUMENT / CASE

The Board may be requested to certify a classified document or case that contains classified information. If the Board does not have the record of proceedings ("ROPs"), the ROPs will need to be obtained from the immigration court, and the procedures for receipt of classified materials in Section III. C. (regarding receipt of classified information) must be followed.

A. Verification of Certification Request

The certification request will initially be received by the Clerk's Office. Thereafter, the Classified Case Coordinator or other designated Board personnel will take responsibility over processing the certification request.

Prior to processing the certification request from the Office of Immigration Litigation ("OIL"), the Classified Case Coordinator or other designated Board personnel must obtain the following: (i) docket number of the alien's federal court proceedings; (ii) number of certified copies requested; (iii) date certified copies due to OIL, and (iv) the name(s) and telephone number(s) of the individual(s) at OIL to who the certified classified copies is to be transmitted. Also, the EOIR/OS should be contacted to verify that the individual(s) at OIL have the appropriate security clearance.

B. Reproduction / Copies

The certification of a copy of a classified document or a case that contains classified information must take place in the Restricted Access Room. Copies of the classified information are subject to the same controls as the original information. *See* Section VI. E. (regarding reproduction notes).

C. Transmittal of Certified Copies

The same wrapping procedures addressed in Section IX shall be followed, except that the certified copy of the classified document or case will *not* be mailed or sent by Federal Express. The certified classified copy or copies *must* be hand-carried to OIL by an individual with the appropriate security clearance. The EOIR/OS or other designated Department of Justice personnel must be contacted for assistance in making the arrangements for the transport of the certified copies by a designated classified courier.

D. Notify Receiver

The Classified Case Coordinator or other designated Board personnel will notify the individual at OIL that the certified classified copy(ies) is en route to ensure that the package is received.

XII. PROCESSING FORMERLY CLASSIFIED CASE

The Board may receive a case from an immigration court or DHS which has classified information when previously at the Board but no longer contains such information. Although such a case may no longer contain classified information, the Board will nonetheless employ heightened processing procedural safeguards.

A. Post-Board Decision Case Monitoring

Since the Board is unlikely to receive advance notice that a case previously contained classified information but no longer does, the Classified Case Coordinator shall maintain a report to monitor the activity on cases that were previously processed at the Board. The

Classified Case Coordinator is responsible for reporting findings to the Chief Clerk and the designated Senior Legal Advisor. This report shall be part of the Board's permanent record keeping but will not include any classified information.

B. Receipt of Notice of Appeal or Motion

The Notice of Appeal or motion on a formerly classified case will initially be received by the Clerk's Office. Thereafter, the Classified Case Coordinator will take responsibility over processing the case through the Clerk's Office.

1. Verification of non-classified status of case. The Classified Case Coordinator shall verify with the immigration court or DHS that the case no longer involves or contains classified information. If the pending matter before the Board does not involve classified information, the matter will be processed by the appropriate team in the Clerk's Office. If it is discovered, however, that the case still involves classified information, the Classified Case Coordinator will advise the Chief Clerk immediately, and the case will be processed according to the appropriate procedures outlined above.

2. Non-classified status verified. The Classified Case Coordinator shall continue to monitor the case even though no classified information is presently involved. When a case is ready for adjudication, the Classified Case Coordinator will advise the designated Senior Legal Advisor, who will contact the Chairman and/or Vice Chairman regarding the assignment of the case to a Board Panel. Also, to the Senior Legal Advisor will contact the Director of Operations and Senior Panel Attorneys for assignment of the case to a staff attorney.

XIII. PROCESSING A CASE UPON DISCOVERY OF POSSIBLE CLASSIFIED DOCUMENTS AND INFORMATION OBTAINED VIA WIKILEAKS

The Board may receive a case which has classified documents and information which may have been obtained via WikiLeaks. This information may be submitted directly to the Board by the parties. Also, it is possible that this information was submitted at the immigration court level but is not discovered at the trial level and will not come to light until on review before the Board.

WikiLeaks information can appear in the record of proceedings in any number of ways. There may be a reproduction of a WikiLeaks page or a reference in a document that information came from WikiLeaks. There also may be a transcript reference to a document as coming from WikiLeaks, or there may be testimony that repeats or summarizes information obtained through WikiLeaks.

As noted in Section II. B. (regarding safeguarding), all Board employees and contractors are individually obligated to protect classified information. The fact that classified information has been leaked to the public does *not* change the fact that the information is still classified. WikiLeaks' disclosure does not relieve a government employee or contractor from their obligation to treat the information as classified when it comes into the custody of the Board.

A. Steps to take if information is found or suspected

If a Board employee or contractor discovers, or even believes, that they have encountered classified information, the following steps should be immediately taken to ensure that information is handled properly.

1. Secure the information *immediately*.

2. Do *not* attempt to verify whether the information is classified.

3. Notify a supervisor, who will notify the Board's Classified Case Coordinator and/or designated Senior Legal Advisor of the receipt and the case involved. If your supervisor or another supervisor is not available, contact the Case Coordinator and/or designated Senior Legal Advisor directly. The EOIR/OS should be contacted *only if* the Classified Case Coordinator and/or designated Senior Legal Advisor are not available.

4. Keep a written record of the handling of the document since it came into your custody (e.g., how you came upon it, what steps you took to secure and notify, and the time and date of each step).

EOIR-issued laptops and computers are *not* certified to process classified information and should not be used to process classified information. *See* Section II. B. 5 (regarding unauthorized disclosure).

B. Steps to take if working at home

The process is the same. If the Board employee is working on a case at home and discovers, or believes that they have discovered, classified information obtained via WikiLeaks, follow the steps listed above.

C. Classification markings – indicator of classified information

In general, classified information is marked or labeled by the classifying agency. *See* Section VII. C (regarding marking or labeling). Entire documents may be classified or just portions; and a given document may have different levels of classification in different parts of the document, with each part annotated for its particular level. The following classification levels and/or symbols may be seen in the document:

Top Secret	"(TS)"	Unclassified	"(U)"
Secret	"(S)"	Sensitive but Unclassified	"(SBU)"
Confidential	"(C)"		

Be aware that, just because a document may contain unclassified information, that does not change the overall classification of the document. The entire document is still considered classified at the highest level until declassified by an appropriate U.S. Government authority.

D. Department of State Cables

WikiLeaks disclosed a number of cables, and some have appeared in filings at the immigration courts and the Board. Be aware that a filing may not indicate that the cable was obtained through WikiLeaks or that it may contain classified information.

APPENDIX

Contact Information
as of November 4, 2014

Office of the Chairman

Amy Minton, Senior Legal Advisor.....(703) 605-(b) (5)

- contact for general procedural information or elaboration on the contents of this Classified Document Control Memo
- contact upon discovery or suspected discovery of classified information/WikiLeaks

Office of the Clerk

Donna Carr, Chief Clerk.....(703) 305-(b) (6)

Paulomi Dhokai, Classified Case Coordinator.....(703) 305-(b) (6)

Subhadra Chennubhotla, Deputy Classified Case Coordinator.....(703) 305-(b) (6)

- contact Classified Case Coordinator and/or Chief Clerk for physical handling of classified information and/or processing a case that involves classified information
- contact upon discovery or suspected discovery of classified information/WikiLeaks

Office of Security

James McDaniel, Chief of Security.....(703) 305-(b) (6)
Billie Jo Agambar, Deputy Chief of Security.....(703) 605-
Office of Security main line.....(703) 605-

- contact the Office of Security main if you need assistance with the physical handling of a file or classified information, or access to the STE

Information Resource Management (IRM)

Annette Thomas, Chief IT Security Officer..... 703) 605-(b) (6)

- contact Annette Thomas if you need assistance with information technology security of classified information