U.S. Department of Justice

Executive Office for Immigration Review

Board of Immigration Appeals

5107 Leesburg Pike, Suite 2000
Falls Church, Virginia 22041

MEMORANDUM

TO: ALL BIA Personnel

FROM: David H. Wetmore
Chief Appellate Immigration Judge

DAVID WETMORE Digitally signed by DAVID WETMORE Date: 2024.07.02 15:47:52 -04'00'

DATE: July 1, 2024

RECISSION: BIA 17-02:
Classified National Security Information Document Control

SUBJECT: BIA Operating Policies and Procedures Memorandum 24-01:
Classified Information at the Board of Immigration Appeals

I. Introduction and Scope

This Operating Policies and Procedures Memorandum (OPPM) provides directives on the proper handling of classified information at the Board of Immigration Appeals (BIA) of the Executive Office for Immigration Review (EOIR). This OPPM supersedes the BIA Chairman's Memorandum, BIA 17-02, *Classified National Security Information Document Control*, dated June 5, 2017, which is hereby rescinded.

The handling of classified information at the BIA requires that certain procedural safeguards be followed to protect the nature, source, and existence of the information for reasons of national security. The purpose of the procedures set forth herein is to establish an updated framework governing the use and handling of classified information within the immigration court system, and to protect against the unauthorized disclosure of any such classified information, in accordance with applicable authority, including Executive Order (E.O.) 13526 (2009) and 32 C.F.R. Part 2001. Other authority for this OPPM includes all relevant regulations under Title 8 of the C.F.R., executive orders, and Department of Justice (DOJ) orders, policy statements, and instructions, and all other applicable provisions of law. Nothing in this memorandum is intended to supplant or modify DOJ policies and procedures regarding the use of information obtained or derived from the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq*. The use of, and litigation relating to, any such information, whether classified or unclassified, is subject to statutory requirements and DOJ policy memoranda and must be coordinated with DOJ's National Security Division.

The procedures set forth in this memorandum are intended to comply with all relevant DOJ and originating agency requirements regarding equipment, facilities, and protection of classified information. EOIR must comply with all U.S. Government requirements for safeguarding classified materials and for approving and maintaining the security of information technology (IT) equipment and facilities used for such materials. Whenever circumstances appear to be beyond the scope of this OPPM, BIA personnel shall request assistance from the BIA Security Coordinator and/or the EOIR Office of Security (EOIR/OS).

BIA personnel must protect classified information and prevent its unlawful or unauthorized disclosure. BIA personnel who disclose without authorization or otherwise mishandle classified information may be subject to discipline, administrative sanction, or possible criminal and civil penalties, including but not limited to reprimand, termination of security clearance, suspension without pay, removal from the position, and/or criminal prosecution.

If you have any questions regarding the procedures set forth in this OPPM, please contact EOIR/OS.[1]

[1] This memorandum is not intended to, does not, and may not be relied up on to, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States; its departments, agencies, or entities; its officers, employees, or agents; or any other person.

II. Definitions

Classified information includes any information or material that, pursuant to applicable executive order, an original classification authority has classified based on the determination that "the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security," such that the information "require[s] protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form." E.O. 13526 §§ 1.1, 6.1(i); *see also* 8 U.S.C. § 1189(d)(1), 18 U.S.C. app. 3 § 1 (defining classified information, for purposes of the Immigration and Nationality Act (INA) and Classified Information Procedures Act, as "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"); 8 U.S.C. § 1189(d)(2) (defining "national security" under the INA as "the national defense, foreign relations, or economic interests of the United States"). As used herein, "original classification authority" "means an individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to classify information in the first instance," 49 C.F.R. § 8.5, and "originating agency" refers to the agency of the original classification authority, *i.e.*, the agency that originally classified the information in question.

Information may be classified at one of the following three levels, as currently defined in E.O. 13526:

1. Top Secret: The unauthorized disclosure of the 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";

2. Secret: The unauthorized disclosure of the 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

3. Confidential: The unauthorized disclosure of the 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. 13526 § 1.2 (emphasis added).

Sensitive Compartmented Information (SCI) refers to a subset of classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled pursuant to formal access control systems established by the Director of National Intelligence. *See* Intelligence Community Directive 703 (2013). Because of the procedures that apply to the handling of SCI, BIA personnel must contact the Central Security Coordinator (*see infra* Section III.A) immediately if a party notices the intent to use SCI or BIA personnel otherwise learn that a proceeding may involve SCI. The Central Security Coordinator is responsible for coordinating with DOJ Security and Emergency Planning Staff (SEPS) to ensure that SCI is properly handled, including with respect to transport and storage in a Sensitive Compartmented Information Facility (SCIF), in accordance with the relevant access control procedures applicable to the particular SCI and in consultation with the agency

from which the SCI originated. Upon notification that SCI will be introduced for a case or hearing, the Central Security Coordinator will work with SEPS to ensure that all personnel required for the case are properly cleared and read-into the appropriate SCI compartment, and to designate a SCIF location for those personnel to review/process the material. The Central Security Coordinator will also work with the agency submitting the SCI to ensure that the BIA personnel receiving the material is cleared to do so.

III. Security Personnel

A. Central Security Coordinator

1. To ensure consistency in the implementation of these procedures and the proper handling and protection of classified information across the immigration courts and the BIA, EOIR has established the role of Central Security Coordinator within its Office of Security. The Central Security Coordinator is responsible for overseeing the national implementation of these procedures and will serve as the point of contact for all EOIR personnel when any questions or issues arise relating to these procedures and/or the handling of classified information in a particular proceeding.

2. The BIA Security Coordinator (*see infra* Section III.B) will report to and receive guidance from the Central Security Coordinator related to these procedures and handling of classified information.

3. The Central Security Coordinator must maintain Top Secret (TS)//SCI clearance.

4. As part of overseeing the implementation of these procedures, the Central Security Coordinator is responsible for, among other things, (1) coordinating the process for obtaining security clearances for EOIR personnel; (2) maintaining a list of cleared EOIR personnel authorized to handle classified information; (3) coordinating the reassignment of cleared immigration court personnel from one court to another court when necessary for the handling of classified information in particular proceedings; (4) coordinating with EOIR's Office of Information Technology (EOIR/OIT) to ensure the necessary equipment and technology are allotted and provided to EOIR personnel to properly process and safeguard classified information; and (5) coordinating initial and subsequent annual trainings for all EOIR personnel on these procedures.

B. BIA Security Coordinator

1. BIA's Chief Clerk is designated as the Security Coordinator for all cases at the BIA involving classified information.

2. The Chief Clerk, Classified Case Coordinator, and designated Senior Legal Advisor, must obtain and maintain TS//SCI clearance.

3. The Chief Clerk is responsible for ensuring that these procedures are properly implemented at the BIA, and that all BIA personnel are aware of these procedures and their obligation to follow them.

4. The Chief Clerk's responsibilities as the BIA's Security Coordinator include, among other things, overseeing the transmission, handling, and storage of classified information, and ensuring that all BIA personnel authorized to access such information follow these procedures, so that the unauthorized disclosure of classified information does not occur.

5. The Chief Clerk must notify the Central Security Coordinator immediately upon learning that a case may involve the use of classified information. BIA personnel who learn that a case may involve the use of classified information must immediately notify the Chief Clerk.

6. In a case involving classified information, the Chief Clerk (as the BIA's Security Coordinator) is responsible for physically taking possession of any classified materials directly from the filing party or immigration court and immediately securing the materials in a secure container approved by the General Services Administration (GSA) or in a secure open storage area (also called a "secure room"),[2] as set forth below in Section V.B, Safeguarding Classified Information.

C. Other Cleared BIA Personnel

1. The BIA's Security Coordinator, who is the Chief Clerk, may designate appropriately cleared BIA personnel, *see infra* Section IV, Access to Classified Information, to assist with ensuring that the security safeguarding procedures set forth herein are followed in a particular case, or in all cases, at the BIA, including to assist with ensuring that the proper "Secure Access Status" identifier is entered into the Case Access System for EOIR (CASE). This is necessary, in part, if the BIA's Security Coordinator is unable to be present at a hearing or oral argument (OA) where classified information will be used, or if there are several cases involving classified information at the BIA at a given time, designated additional BIA personnel are available to assist in implementing the appropriate security procedures.

2. The Chief Clerk, as the BIA's Security Coordinator(s), shall designate one or more Classified Case Coordinator(s) to assist the Chief Clerk in fulfilling the BIA Security Coordinator's responsibilities for all cases at the BIA involving classified information. The Classified Case Coordinator(s) must maintain TS//SCI clearance.

3. The Chief Clerk and Classified Case Coordinator(s) will work in conjunction with one or more designated Senior Legal Advisor(s) (SLA), who will assist them in fulfilling their responsibilities. The designated SLA(s) shall also work with the Central Security

---

[2] An open storage area for classified information is a secure space that meets the requirements of 32 C.F.R. § 2001.53 and is authorized by the Central Security Coordinator for storage of classified information. EOIR/OS (not BIA) is authorized to designate a space to be a secure room for storing classified information in accordance with these standards. BIA personnel should consult with EOIR/OS for guidance on whether a secure container or open storage area meets minimum security requirements and can be designated for the storage of classified information.

Coordinator, and EOIR/OS to ensure that the security safeguarding procedures set forth herein are followed. The designated SLA(s) must maintain a TS//SCI clearance.

IV. Access to Classified Information

The BIA has Appellate Immigration Judges (AIJs) who have TS or TS//SCI clearances. The BIA also has Attorney Advisors and designated Support Staff in the Clerk's Office with TS or TS//SCI clearances. The BIA, in coordination with EOIR/OS, regularly reviews which and how many BIA employees have clearances in order to ensure, among other things, that there are sufficient personnel to process cases at the BIA that involve classified information.

When BIA personnel have a need to access classified information in connection with their duties, EOIR/OS must confirm that the BIA personnel possess the requisite clearance level for accessing the information. EOIR/OS, and not BIA personnel, is responsible for assessing and determining whether any particular BIA personnel is authorized to access classified information, before the BIA personnel is permitted to access the information.

A. Requirements for Access to Classified Information

1. EOIR/OS is responsible for authorizing BIA personnel to access classified information. BIA personnel may be authorized by EOIR/OS to access classified information only if the BIA personnel meets the following three criteria:

    a. Possesses the requisite level of security clearance;

    b. Has demonstrated a need-to-know the information; and

    c. Has signed a classified information non-disclosure agreement, Form SF-312, and Form 4414 for access to SCI information, if appropriate, on file with EOIR/OS.

2. "Need-to-know" means that the prospective recipient of specific classified information requires access to that information in order to perform or assist in a lawful and authorized governmental function. No person is entitled to receive classified information solely by virtue of office, position, rank, or security clearance. *See* E.O. 12968.

3. BIA personnel must possess the requisite security clearance before accessing classified information. Requests for security clearances for BIA personnel must be made by EOIR/OS, in consultation with BIA's Executive Officer. The BIA personnel requiring the security clearance must not submit a request for the security clearance on their own behalf. EOIR/OS will notify the individual requiring the clearance if/when the clearance (Top Secret, Secret, or Confidential) has been granted.

4. EOIR/OS will provide each BIA personnel member who is granted a security clearance with (a) a set of guidance/training materials concerning the proper handling and protection of classified information in accordance with these procedures, and (b) a security briefing regarding such procedures. The recipient of the security clearance must receive this briefing from EOIR/OS prior to accessing classified information and

on an annual basis thereafter. The briefing may be conducted by EOIR/OS personnel. Contact EOIR/OS if additional copies of any information in the security clearance packet are needed.

B. Responsibilities to Ensure the Safeguarding of Classified Information

1. Disclosure to BIA Personnel

a. All BIA personnel are obligated to protect classified information in accordance with these procedures.

b. BIA's Security Coordinator, Classified Case Coordinator(s), designated SLA(s), and other appropriately cleared BIA personnel with access to classified information used in a particular case may disclose such information to other BIA personnel only if such personnel have a security clearance at the requisite level, an executed non-disclosure agreement on file with EOIR/OS, and a need-to-know the information. *See supra* Section IV.A, Requirements for Access to Classified Information. Confirmation that BIA personnel have the requisite security clearance and non-disclosure agreement can be requested from EOIR/OS by the BIA's Chief Clerk, Classified Case Coordinator(s), or designated SLA(s). Because appropriately cleared BIA personnel are considered authorized clearance holders, further certification or authorization is not required, after consultation with the Central Security Coordinator, prior to disclosing classified information to BIA personnel so long as the personnel meet the requirements specified above.

2. Disclosure to Persons Outside BIA

a. BIA personnel are authorized, subject to and in accordance with these procedures, to receive and handle classified information in connection with their case responsibilities.

b. BIA personnel *do not* have the authority to disclose any such classified information, including the existence thereof, to any person except for other BIA personnel pursuant to Section IV.B.1, above. However, transmitting records including classified information to the immigration court, Department of Homeland Security (DHS) or a federal court, or as otherwise specified in these procedures, is permitted. *See infra* Sections VIII, Transmittal of Classified Information, and XII.A, Return of Classified Materials. The ability to authorize any disclosure of such classified information to persons outside BIA rests with the originating agency.

3. Unauthorized Disclosure

a. Contact EOIR/OS immediately if there has been a possible unauthorized disclosure of classified information and/or any potential violation of these procedures.

b. The unauthorized disclosure of classified information (whether to an individual, online, or otherwise) does not affect the 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 unless and until it has been declassified by the originating agency. As set forth above, BIA personnel who disclose classified information without authorization may be subject to administrative, civil, or criminal penalties.

c. Unless authorized to handle classified information pursuant to these procedures, BIA personnel are not permitted to access information marked or labeled classified, including any such information from publicly available sources. BIA personnel who believe that they may have downloaded classified information to non-classified government systems (including laptop computers not specifically approved for processing classified information, as specified below in Section VI.K.3, Security Procedures, Media) must immediately contact EOIR/OIT and provide notification to EOIR/OS.

V. Custody and Storage of Classified Materials

A. Materials Covered

The security procedures set forth below for storing classified information are media neutral and apply to all papers, documents, and other materials—whether in hard copy or electronic form—that contain classified information and that are in the custody of the BIA (*e.g.*, motions, pleadings, briefs, notes, transcripts, and audio recordings of *in camera* proceedings, among other materials containing classified information, must never be saved in any electronic record materials).

B. Safeguarding Classified Information

1. Classified information transmitted or submitted to the BIA shall be handled only by BIA personnel with the appropriate security clearance who are working on the particular matter, possess a need-to-know the information, and have executed a non-disclosure agreement on file with EOIR/OS. The classified information must be controlled, maintained, and stored in a manner designed to minimize the possibility of unauthorized disclosure, removal, and/or access including specifically set forth below. The Chief Clerk, as the BIA's Security Coordinator, should consult with EOIR/OS regarding the proper storage of materials in any case involving classified information.

2. Documents or other materials containing classified information must never be uploaded into the EOIR Courts and Appeals System (ECAS), *i.e.*, materials containing classified information must never be saved in any electronic Record of Proceeding (eROP). Instead, a paper Record of Proceedings (ROP) must be created. For more information on converting an eROP to a paper ROP, *see infra* Section VI.B, Unclassified ROPs or eROPs.

3. All classified materials[3] in the custody of the BIA shall be stored in a GSA-approved security container (i.e., safe) or open storage area (*i.e.*, Restricted Access Room, *see infra* Section V.F, Restricted Access Room). The combinations to 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 Chief Clerk or EOIR/OS to convert the factory pre-set combination if and when the combination has been subject to possible compromise or an individual knowing the combination no longer requires access to the security container. After consultation with the Central Security Coordinator, the Chief Clerk may provide the combination for a security container to other BIA personnel who possess the requisite security clearance, has signed a non-disclosure agreement, has a need-to-know, and requires access to the container. The Chief Clerk must inform the Central Security Coordinator whenever there is a change in BIA personnel and an individual no longer requires access to a particular security container combination. The Chief Clerk must also inform EOIR/OS whenever there is a change in combination to a security container.

4. Classified materials relating to different cases maintained in the same security container shall be segregated by placing the materials in separate envelopes or folders that are appropriately labeled with the applicable classification level and are identified by the registration number or A number for the respondent[4] involved in the case. Unclassified materials must not be stored in these security containers.

5. Classified material must be kept in secure facilities as set forth above and must never be taken out of such facilities unless the material is being returned to the filing party, originating agency, or immigration court, or certified and transported for further litigation, or being archived. *See also infra* Sections VIII, Transmittal of Classified Information, and Section IX, Certification of Records. Classified material must be reviewed in an area that affords sufficient protection against unauthorized disclosure of the information—*i.e.*, an area to which access can be limited and where processing can be accomplished without being observed or monitored by persons not authorized to access the classified information. *See infra* Section V.F, Restricted Access Room.

6. Classified material must never be taken to a person's home under any circumstances. This is true even if a person has a security clearance or has been approved for telework, remote work or work from an alternative worksite. If any part of an ROP is classified, the entire ROP must be reviewed and maintained at the BIA or other designated secure facility at all times.

---

[3] Separate procedures apply to the treatment of SCI, which must be stored and discussed in a SCIF. *See supra* Section II.

[4] The term "respondent" is used in this memorandum to encompass individuals who appear before the BIA, including respondents, applicants, petitioners (who may be a US citizen), self-petitioners, beneficiaries, carriers, and individuals (who may be US citizens) in fine proceedings.

7. Access to classified information by BIA personnel shall be limited to the minimum number of cleared personnel necessary to effectively carry out the administration of the case. Access includes reviewing classified information or being present at an *in camera* hearing or any other proceeding during which classified information may be disclosed.

8. All material containing classified information must be properly accounted for each time such material is taken out of the security container or secure room. The Security Container Check Sheet, Form SF-702, must be affixed to the outside of the security container or secure room to track who had access to the space and the date and time of each such access. Additionally, an unclassified document register, to be kept in the security container or secure room and updated by the Chief Clerk, Classified Case Coordinator(s), or designated SLA(s), must be used to track who had access to the security container or secure room, who took classified material from the space, and when the material was removed and then returned.

C. Advance Notice That Classified Information is Being Sent to the BIA

1. Whan an entity – the immigration court or DHS – transmits classified information to the BIA, the entity should provide the BIA and EOIR/OS with advance notice that classified material is being forwarded.[5]

2. Any BIA personnel who are contacted by the immigration court or DHS regarding the transmission of classified information to the BIA must immediately contact the Chief Clerk (as the BIA's Security Coordinator) and/or the Classified Case Coordinator(s) at the Office of the Clerk (Clerk's Office).

D. Instructions for Receipt of Classified Materials from OCIJ at the BIA Clerk's Office

1. The immigration courts must follow specific Office of the Chief Immigration Judge (OCIJ) issued procedures for the sending and receiving of classified information.[6] An immigration court must not send classified information directly to the mail room of the BIA's Clerk's Office, nor should an immigration court send classified information electronically. Rather, the materials must be addressed to an individual at the BIA who has been identified by EOIR/OS.

2. When an immigration court sends classified information at the Confidential or Secret level to the BIA, the mailing will be sent through the U.S. Postal Service (USPS) via Registered Mail, Return Receipt Requested; USPS Express Mail, Return Receipt

---

[5] The Office of the Principal Legal Advisor (OPLA) within the U.S. Immigration and Customs Enforcement (ICE) of DHS is usually the U.S. Government's representative in immigration proceedings before the immigration court and the BIA, if an appeal is filed. Also, attorneys within DHS from the U.S. Citizenship and Immigration Services in visa petition proceedings or attorneys from U.S. Customs and Border Protections in fine proceedings or advance permission proceedings may appear before the BIA.

[6] OCIJ has issued an OPPM for Classified Information in Immigration Court Proceedings (OPPM 24-01). That memorandum is available on the EOIR website at www.justice.gov/eoir.

Requested; or through Federal Express (FedEx). The immigration court should provide the tracking number of the package to the BIA in advance of its arrival, so that the Chief Clerk, Classified Case Coordinator(s) or other designated BIA personnel can monitor the package.

3. After arrival at the BIA's Clerk's Office, the package will be picked up by designated and cleared BIA personnel, and that person shall immediately hand-carry the package to the Chief Clerk, Classified Case Coordinator(s) or other designated BIA personnel. The package may never be left on a desk or otherwise unattended.

4. The BIA's Classified Case Coordinator(s) or other designated BIA personnel will then place the classified information, except for SCI, in a GSA-approved security container (*i.e.*, safe) in the Restricted Access Room (*see infra* Section V.F) or temporarily in an authorized designated safe in the Clerk's Office.

5. Material containing Top Secret information must always be hand-carried to the destination by an individual cleared at the Top Secret level and designated as a classified courier. EOIR/OS shall coordinate arrangements for the transport of any material containing SCI to a SCIF with the appropriate DOJ security officials prior to the issuance of any decision in immigration court, in order for the information to be properly received at the BIA.

6. When not in use, classified materials shall be stored in the safe in the Restricted Access Room. Classified materials relating to different cases maintained in the same security container shall be segregated by placing the materials in separate envelopes or folders that are appropriately labeled with the applicable classification level and that are identified by the registration number or A number for the respondent involved in the case. Unclassified materials must not be stored in these security containers.

7. Once the classified materials arrive at the BIA, CASE must be updated by the Chief Clerk, Classified Case Coordinator(s) or other designated personnel to reflect its arrival, through completion of the following steps:

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

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

    c. The CASE identifier "Secure Access Case" must also be added to CASE under the Comments Tab to (1) reflect receipt of the classified information, and (2) advise that inquiries and correspondence in the case must be directed to the Classified Case Coordinator(s). Notes added to CASE under the Comments Tab may reflect the receipt date of any classified information, but the notes must not describe the substance or source of any classified information.

E. Secure Access Report

The Classified Case Coordinator(s) or other Clerk's Office designated personnel will maintain a monthly report that monitors and tracks all cases with classified material from the time the material is received at the BIA until it is archived. The monthly report shall be made part of the BIA's permanent record keeping, but it will not include any classified information. The report will also be made available to EOIR/OS upon its request.

F. Restricted Access Room

1. Classified information in immigration cases received at the BIA must be kept in the designated Restricted Access Room.

2. EOIR/OS staff, the Chief Clerk, the Classified Case Coordinator(s), the designated SLA(s), and other designated and cleared BIA personnel are authorized to access the Restricted Access Room.

3. The Restricted Access Room contains the necessary equipment to store, destroy, transmit, and reproduce classified information. EOIR-issued laptops and computers are not certified to process classified information and should not be used to process classified information. Computers used to process classified information must be specifically accredited and approved for the processing of classified information. Prior to the initiation of any such processing, contact EOIR's Chief IT Security Officer to ensure that a particular computer is accredited and approved.

4. Protocols consistent with the procedures set forth herein for handling classified information materials must be posted inside the Restricted Access Room.

5. An employee's office, position, rank, or security clearance does not automatically allow them access to the Restricted Access Room. Access to the Restricted Access Room shall be made by appointment with the Chief Clerk, Classified Case Coordinator(s), the designated SLA(s), or EOIR/OS. Any admittance into the Restricted Access Room by designated individuals from the Clerk's Office or the designated SLA(s) shall be recorded in the BIA's Restricted Access Room logbook. This logbook, which is maintained in the BIA's safe, shall reflect who was admitted into the room, the time and date of admission, and the time of departure. Also, the BIA's Restricted Access Room logbook shall be used to record who accessed the safe in that room that is assigned to the BIA, what material was reviewed, and what material was added to or removed from the safe. No classified information shall be recorded in this logbook.

6. All material containing classified information must be properly accounted for each time such material is taken out of the security container or secure room. The Security Container Check Sheet, Form SF-702, must be affixed to the outside of the security container or secure room to track who had access to the space and the date and time of each such access. Additionally, an unclassified document register, to be kept in the security container or secure room and updated by the Chief Clerk, Classified Case Coordinator(s), or designated SLA(s), must be used to track who had access to the

security container or secure room, who took classified material from the space, and when the material was removed and then returned.

7. EOIR/OS maintains the master combination for the GSA-approved security container (*i.e.*, safe) assigned to the BIA for storage of classified information when not in use. The Chief Clerk, Classified Case Coordinator(s), or designated SLA(s) are required to inform EOIR/OS whenever there is a need for a change in combination (*e.g.*, change in personnel). Dissemination of the combination to the assigned BIA safe is limited to a minimum number of cleared BIA personnel to minimize the possibility of unauthorized disclosure, removal, and/or access.

8. Use of any computer equipment assigned to the BIA that is accredited and approved for the processing of classified information shall be recorded in the EOIR Classified Computer Usage log. This log, which is maintained in the safe assigned to the BIA, shall reflect who used the approved laptop assigned to the BIA as well as the time and date of usage. The log shall not include any classified information.

9. Portable electronic devices (*e.g.*, smart watches, fitness trackers, laptops, mobile devices, and removable media CD-R for music) are not permitted in the Restricted Access Room.

VI. Security Procedures

A. Receipt of Notice of Appeal, Interlocutory Appeal, or Motion

1. The BIA may receive a case that involved classified information before the immigration court or receive an appeal, interlocutory appeal, motion to reopen, or motion to remand in which DHS advises the BIA of its intention to present classified information that was not previously provided to the immigration court. The Notice of Appeal or motion will initially be received by the Clerk's Office.

2. DHS must comply with the procedures set forth in Section VII.A, Notice That Case May Involve Classified Information, if DHS intends to present classified information to the BIA that was not previously provided to the immigration court.

3. If DHS files a notice or otherwise indicates that classified information may be submitted to the BIA that was not submitted to the immigration court, the Chief Clerk, Classified Case Coordinator(s) or other designated cleared BIA personnel will immediately take over the processing of the case once the case is entered into CASE.

4. Documents or materials containing classified information should never be uploaded into ECAS or saved in any eROP. Cases involving classified materials should always be handled on an expedited basis.

B. Unclassified ROPs or eROPs

1. Pursuant to governing OCIJ procedures, upon receipt of classified information at the immigration court, appropriately cleared court personnel will convert an eROP to a

paper ROP, deactivate the eROP in ECAS, and notify the parties that the case is no longer eligible for electronic filing.[7] *See* OCIJ OPPM 24-01.

2. Upon receipt of classified information at the BIA that was not previously submitted before the immigration court, the Chief Clerk, Classified Case Coordinator(s), or other appropriately cleared BIA personnel shall convert the case from an eROP into a paper ROP, *i.e.*, the case file must be converted from electronic to hard copy. Any existing unclassified documents contained in the eROP must be printed, a paper ROP must be constructed, and the eROP must be deactivated. The parties must be notified through a BIA-issued notice that the case is no longer eligible for electronic filing or processing, and that all future filings must be submitted in paper. That notice must be sent outside of ECAS and all subsequent filings must be made in hard copy outside of ECAS, given the conversion of the electronic record into a paper record. Only cleared BIA personnel may assist in the conversion of the eROP into a paper ROP. Following conversion of the case file into paper form, the classified portions of the paper ROP must be marked and then stored and safeguarded according to the procedures set forth herein. Unclassified portions of the paper ROP may be maintained separately.[8]

C. Classified ROPs

If the entire record of proceedings is classified, all ROP documents will be contained in BIA's safe in the Restricted Access Room at all times while at the BIA. All processing by the Chief Clerk, Classified Case Coordinator(s), or designated SLA(s) will be conducted in the Restricted Access Room. Review of the classified information by the designated and cleared AIJ(s) and/or Attorney Advisor assigned to prepare the BIA's decision will also be conducted in the Restricted Access Room.

D. Transcription of Hearing Involving Classified Information

1. Transcription of hearings involving classified information must only be performed by persons with the proper clearance and must be performed in the Restricted Access Room. Before such a hearing may be transcribed, EOIR/OS must confirm the clearance level of the person preparing the transcript.

2. Completed transcripts of hearings involving classified information must contain the appropriate classification markings before they are sent for review by the originating agency. It is the responsibility of EOIR/OS to forward a copy of the marked and labeled transcript to DOJ's National Security Division for facilitating such

[7] Where a case involving classified information includes a rider respondent, pursuant to the OCIJ procedures, the rider's eROP will also have been converted to a paper ROP and deactivated and will no longer be eligible for electronic filing.

[8] The same process must take place for any rider respondent's ROPs that are traveling with the lead respondent's ROP.

classification review. EOIR/OS will contact the BIA when the review of the transcript has been completed and the transcripts returned to EOIR.

E. Completion of Briefing Schedule/Case Assignment

1. Upon completion of the briefing schedule in a case, the Classified Case Coordinator(s) or other designated Clerk's Office personnel will advise the designated SLA(s) that the matter is ready for adjudication. The designated SLA(s) will then contact the Chief Appellate Immigration Judge and/or Deputy Chief Appellate Immigration Judges regarding the assignment of the case to a Panel comprised of AIJs with the requisite security clearance. The designated SLA(s) also will contact the Director of Operations and the Senior Panel Attorneys for assignment of the case to an SLA or Attorney Advisor with the requisite security clearance.

2. The designated Senior Panel Attorney and/or Supervisory Attorney Advisor (Team Leader) is responsible for advising the Attorney Advisor 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 the Attorney Advisor must first contact the Classified Case Coordinator(s) or other designated BIA personnel for admission to the Restricted Access Room.

F. Review of the Non-Classified Portion of the ROP

If any part of an ROP is classified, the entire ROP must be reviewed and remain on-site at the BIA all times. The non-classified portion of the ROP may be reviewed on-site in an attorney's office but shall be stored in the Restricted Access Room. Additionally, BIA Judicial Tools (BIA JT) may not be used to process the BIA's decision (e.g., draft, circulate, vote, or issue). Rather, the laptop and printer in the Restricted Access Room designated for the BIA's use for processing classified information must be used for preparation of the BIA's decision. *See infra* Section VII.F.2, Decisions by the BIA, Preparation and Circulation of Proposed BIA Decision.

G. Review of Classified Information

Where review of classified information is necessary to adjudicate a case, the assigned AIJ(s) and/or Attorney Advisor must contact the Chief Clerk, Classified Case Coordinator(s), or designated SLA(s) for admission to the Restricted Access Room. Classified information must *not* be removed from the Restricted Access Room by either the designated AIJ(s) or the Attorney Advisor. *See also infra* Section VI.L, Note-Taking.

H. Oral Discussions

Any discussions regarding classified information must be conducted in an area or room that affords sufficient security against unauthorized disclosure. Windows should be equipped with blinds, drapes, or other coverings to prevent observation by unauthorized persons. In addition, appropriate measures should be taken to minimize sound leaving the area (*e.g.*, sound insulation, white noise systems, etc.). The classified information must not be able to be overheard or seen by any person not authorized to access the information. Portable electronic devices (*e.g.*, smart watches, fitness trackers, laptops, mobile devices, and removable media CD-R for music) are

not permitted in any room where classified information may be discussed. *See supra* Section V.F.9, Restricted Access Room. Contact EOIR/OS for additional guidance if discussions need to be held outside the Restricted Access Room. SCI may only be discussed in a SCIF.

I. Telephone and Electronic Communications Security

Classified information must not be discussed, communicated, or processed using any non-secure communication device or system, including standard telephone instruments, office intercommunication systems, cellular devices, computers, or other electronic or internet-based communication services, such as email. Classified information may only be discussed, communicated, and processed on devices or systems approved by the Central Security Coordinator and cleared for the level of classification of the information at issue.

J. Reproduction Security

Copying or other reproduction of classified material is permitted only to the minimum extent required for the BIA's operational needs. Reproduction of classified information may only be performed by persons authorized to access the classified information in accordance with these procedures. Copies of classified information are subject to the same controls as the original information. Before making copies, such authorized personnel shall ensure that any persons not authorized to access the classified information cannot view or otherwise access the information during reproduction. Where copying is necessary, reproduce only the minimum number of copies needed and ensure that all copies of all pages are retrieved, that no pages remain inside the copier, and that all classified waste is removed and disposed of properly. Only an approved copier by EOIR's Chief IT Security Officer in consultation with EOIR/OS may be used, and an approved copier has been designated for the BIA's use in the Restricted Access Room. Network copiers must *not* be used to copy classified information. *See also infra* Section VII.F.4.b, Decisions by the BIA, Final Disposition, Destruction of Reproductions.

K. Computer Security

1. Generally

All computers, printers, and copiers used to process classified information must be certified, accredited, and approved by EOIR's Chief IT Security Officer, in consultation with EOIR/OS, for the processing of classified information prior to initiation of any such processing.

2. Approved Laptop Computers Must be Used.

a. Any document prepared by BIA personnel containing classified information must only be processed using a laptop computer specifically approved by EOIR/OS for classified processing in connection with a specified case(s) involving classified information. The approved laptop must *not* be connected to any network or email system and shall be used only to create or process classified documents related to the case(s) involving classified information for which the laptop was approved. The computer must be stored in a GSA-approved security container or the Restricted

Access Room compliant with the requisite standards corresponding to the classification level of the information processed on the approved laptop.

b. Only the approved BIA 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 BIA's decision or any other document containing classified information from that case (e.g., notes). The approved laptop may be connected to the local printer cleared for handling classified information.

c. The authorized BIA personnel using the approved laptop may save documents or work product onto the hard drive of the approved laptop or separately onto a classified storage device that must be approved by EOIR/OS and stored pursuant to the same security procedures set forth herein applicable to the approved laptop. *See also infra* Section VI.K.3, Security Procedures, Media.

d. The approved laptop must be kept within the authorized user's control at all times, must never be taken outside of the Restricted Access Room or other designated secure facility, and must be stored as set forth above. The approved laptop must never be taken home by the authorized user.

3. Media

a. Classified information may be stored, in addition to hard copy form, on portable media such as CDs and mobile drives (*e.g.*, thumb drives, flash drives, and portable hard drives). Any such portable storage media must either be (i) provided directly by the filing party already containing the classified information or (ii) obtained by the BIA from and approved by EOIR/OS and EOIR/OIT for the storage of classified information. The exterior of any such media must be clearly labeled with the appropriate classification markings according to the highest level of classified information contained on the media. Any such portable media approved for use by EOIR must be used to store classified information only up to the classification level for which the device is approved. Any such media containing classified information must be stored according to the security procedures set forth above.

b. Approved portable storage media may be used to transfer classified information to an approved laptop computer or other approved electronic equipment. The portable media must be transported in compliance with the security procedures set forth below for the transmittal of classified information. *See infra* Section VIII, Transmittal of Classified Information.

4. Printers

An approved printer has been designated for the BIA's use in the Restricted Access Room. Any document containing classified information must be printed, to the extent necessary for the BIA's operations, only on the designated printer that has been approved by EOIR's Chief IT Security Officer, in consultation with EOIR/OS, for the printing of classified information. If/when BIA personnel believes that the printing of classified information is required, please contact the Central Security Coordinator, who

will provide instructions regarding the marking, storage, and any transmittal of such printed materials.

L. Note-Taking

1. BIA employees should avoid taking notes (including extracting information from classified documentary evidence or oral testimony) of classified information, unless doing so is necessary to fulfill their case responsibilities. Notes include paraphrasing or restating classified information. If it becomes necessary to take notes, 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 are not part of the record of the case available to the parties, and must be:

   (a) dated to reflect when they were created,

   (b) marked with the highest classification level that applies to any of the information therein,

   (c) maintained in a GSA-approved security container (*i.e.*, the safe in the Restricted Access Room) in accordance with the applicable classification level and security procedures set forth herein, and

   (d) destroyed in accordance with the applicable classification level and security procedures set forth herein when no longer needed by the BIA (*e.g.*, the shredder in the Restricted Access Room).

2. For information regarding marking or labeling, *see* Section VII.F.3.a, Marking or Labeling Classified Attachment of the BIA's Decision.

VII. Procedures for Cases Involving Classified Information

A. Notice That Case May Involve Classified Information

1. The DHS may seek to use classified information in any matter within the jurisdiction of EOIR, including but not limited to removal, bond, deportation, exclusion, rescission, visa petition, credible fear review, and fine proceedings.

2. When DHS anticipates using classified information for the first time in a particular case before the BIA, DHS shall file a notice with the BIA, and serve a copy of the notice on the respondent, informing the BIA and the respondent that DHS may seek to use classified information in the case. The notice should contain, to the extent feasible, a brief description of the general form (not the substance) of the classified information that DHS may seek to use—*e.g.*, documentary evidence or witness testimony—in order to facilitate the court's preparation for the receipt and proper handling of any such classified evidence.

3. Upon receipt of such a notice, BIA personnel shall promptly notify the Chief Clerk and/or the Classified Case Coordinator(s) that the case in question may involve classified information.

4. If DHS, in consultation with the originating agency and any other relevant agency, determines that notifying a respondent that a case may involve classified information would be reasonably likely to cause a risk to public safety or national security, DHS may delay serving such notice on the respondent for a period of 14 days after the notice has been filed with the BIA or until the risk is no longer present, whichever is shorter. DHS may request that the BIA extend the period of delay, which request shall be granted upon a showing by DHS that the delayed notice remains reasonably necessary to avoid causing such risk.

B. Protective Orders

Upon a motion by DHS, the BIA shall issue an order to (1) protect against the unauthorized disclosure of any classified information submitted or presented in a particular case, and/or (2) protect against the unauthorized disclosure of any unclassified summary of classified information submitted or presented in a particular case.

C. *In Camera*, *Ex Parte* Review of Classified Information[9]

1. The respondent and their representative are not permitted to access classified information presented to the BIA, which must be safeguarded from such unauthorized disclosure. *See, e.g.*, 8 C.F.R. §§ 1240.11(a)(3), 1240.49(a) (decision on application for adjustment of status may be based on classified information not made available to respondent), 1240.49(c)(3), 1240.49(c)(4)(iv) (asylum applicant not entitled to access classified information submitted by DHS).

2. As set forth above, BIA personnel do not have the authority to (a) acknowledge the existence of classified information to individuals other than appropriately authorized BIA personnel, except when providing notice of the use of classified information to a respondent as specifically provided for in these procedures pursuant to Sections VII.D.3-5, Notice of the Use of Classified Information and Provision of Unclassified Summaries; or (b) disclose classified information used in a case to individuals other than appropriately authorized BIA personnel. *See supra* Section IV.B, Responsibilities to Ensure the Safeguarding of Classified Information. The authority to permit any such disclosure of the existence or substance of classified information to other parties, including the respondent and their representative, rests with the originating agency, and no such disclosure shall be made without the written authorization of the originating agency.

[9] As used herein, "ex parte" refers to communications involving only the BIA and the government.

3. BIA personnel do not have the authority to declassify information. The authority to declassify information rests with the originating agency.

4. Consistent with the foregoing, the BIA's review of all classified information submitted by DHS shall be *in camera* and *ex parte*, and the BIA may not order or compel the disclosure of classified information to a respondent or their representative. *See generally* 8 U.S.C. § 1229a(b)(4)(B) (respondent in removal proceedings has rights including to be represented by counsel, examine the evidence against the respondent, and present evidence on the respondent's behalf, "but these rights shall not entitle the alien to examine such national security information as the Government may proffer in opposition to the alien's admission to the United States or to an application by the alien for discretionary relief under this chapter"). In the event that the originating agency authorizes any further disclosure of classified information, the originating agency's written certification (in redacted form as necessary) must be made part of the record of the case prior to the disclosure of any classified information to any respondent or their representative.

5. Any classified document or unclassified summary of classified information submitted by DHS that bears the seal letterhead, or other official markings of any U.S. Government department or agency will be considered self-authenticating evidence and not require any further extrinsic evidence of authenticity to be admitted by the BIA.

D. Notice of the Use of Classified Information and Provision of Unclassified Summaries

1. This subsection applies when DHS submits classified information for the first time to the BIA (*e.g.*, when such information has not already been provided to the immigration court).

2. While a respondent is not entitled to access classified information submitted by DHS, the respondent must be provided notice of the use of classified information in the proceedings.

3. Prior to submitting or presenting classified evidence, DHS shall notify the respondent that classified information will be provided to the BIA. When feasible, DHS may provide the respondent with an unclassified summary of the classified information, but DHS is not required to do so. The BIA shall not order DHS or the originating agency to provide an unclassified summary to the respondent, or to provide the BIA, the respondent, or the respondent's counsel with the basis for any decision not to supply such an unclassified summary.

4. When a respondent is requesting asylum or withholding of removal and the BIA receives classified information that it determines is relevant to the proceeding, the BIA shall inform the respondent that classified information has been received. *See* 8 C.F.R. §§ 1240.11(c)(3)(iv) (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 BIA may notify the respondent on the record at OA, or send written notification to the respondent, informing the respondent

that classified information is being received into evidence. DHS, in coordination with the originating agency and EOIR/OS, may provide the respondent with an unclassified summary of the classified information, but is not required to do so. The BIA shall not order DHS or the originating agency to provide an unclassified summary to the respondent, or to provide the BIA, the respondent, or the respondent's representative with the basis for any decision not to supply such an unclassified summary.

5. When DHS submits classified information in adjustment of status cases, in addition to notifying the respondent of the receipt of classified evidence consistent with the preceding paragraph, the BIA should—whenever the BIA believes that the BIA can do so while safeguarding both the classified information and its source—inform the respondent of the general nature of the information so that the respondent may have an opportunity to offer opposing evidence. *See* 8 C.F.R. §§ 1240.11(a)(3) (adjustment of status in removal proceedings), 1240.49(a) (adjustment of status in deportation proceedings). However, prior to informing the respondent of the general nature of the information, the BIA must consult with DHS, in coordination with the originating agency and EOIR/OS, to ensure that the general summary to be provided to the respondent does not contain or risk revealing classified information. Any proposed draft summary must be treated as presumptively classified until it undergoes review and clearance by the originating agency. If DHS, the originating agency, or EOIR/OS determines that a general summary cannot be provided without containing or risking the disclosure of classified information, the BIA shall not provide any such summary to the respondent. The BIA must defer to the determinations of DHS, the originating agency, and EOIR/OS on these issues.

6. If DHS, in consultation with the originating agency and any other relevant agency, determines that notifying a respondent of the use of classified information would be reasonably likely to cause a risk to public safety or national security, DHS may submit classified information to the BIA and inform the BIA of the need to delay notice, which shall not be provided by the BIA or DHS to the respondent. When classified information is submitted without notice to the respondent pursuant to this provision, notice subsequently must be provided to the respondent as soon as the risk is no longer present and no later than 14 days after the classified information has been submitted. DHS may request that the BIA extend the period of delay, which request shall be granted upon a showing by DHS that the delayed notice remains reasonably necessary to avoid causing such risk.

E. Oral Argument

1. *In Camera, Ex Parte* Proceeding

a. Any hearing involving classified information shall be held *in camera* and *ex parte*. *See Jay v. Boyd,* 351 U.S. 345 (1956) (upholding denial of suspension of deportation based on confidential information undisclosed to the petitioner).

b. Consistent with the notice provisions set forth above, the BIA must notify a respondent of any such *in camera, ex parte* hearing or conference, and DHS must notify the respondent that classified information will be presented to the BIA.

c. The BIA should schedule the *in camera*, *ex parte* hearing involving classified information for a different time or date than the remainder of the OA in the case, to ensure that the respondent is able to be present for all but the portion of the proceeding involving classified information.

d. When conducting an *in camera*, *ex parte* hearing involving classified information, the BIA must ensure that only persons authorized to access that specific classified information are allowed to be present. Portable electronic devices (*e.g.*, smart watches, fitness trackers, laptops, mobile devices, and removable media CD-R for music) are not permitted in any room where classified information may be discussed. The BIA must consult with EOIR/OS as to whether any other safeguards should be implemented to ensure that the classified information is adequately protected, such as pulling down shades on curtains, locking doors (when compliant with fire and safety codes), posting guards outside the OA room, and clearing adjacent rooms if walls are not soundproof.

e. Both prior to and following any such *in camera*, *ex parte* hearing, the respondent and the respondent's representative should be allowed to present any evidence that they believe may be relevant to the hearing before the BIA.

f. At the close of an *in camera*, *ex parte* hearing involving classified information, the recording, transcript, and any other record of the hearing must be labeled with the proper classification level, sealed, and stored by the BIA pursuant to the security procedures for the storage of classified materials set forth herein. The recording, transcript, and any other record of such an *in camera, ex parte* proceeding involving classified information must be maintained in the classified portion of the case's paper ROP and stored in an approved storage device in the Restricted Access Room, never uploaded to an eROP, and shall not be disclosed or otherwise made available publicly.

2. Recording

a. The BIA will not use Digital Audio Recording (DAR) technology that is connected to EOIR's network to record hearings involving classified information. Rather, a laptop computer equipped with DAR technology, which has been approved by EOIR/OS and EOIR/OIT for processing classified information, shall be used to record any hearing involving classified information. Whenever an OA involving classified information is recorded, the recording must be saved on the approved laptop's hard drive or a portable storage device that has been approved for use by EOIR/OS and EOIR/OIT. The recording on the approved laptop and/or storage device used during this portion of the OA must be labeled with the appropriate security classification (*i.e.*, CONFIDENTIAL, SECRET, or TOP SECRET). The

approved laptop and/or storage device shall be stored in the BIA's safe in the Restricted Access Room.[10]

b. When DHS anticipates offering classified information or otherwise discussing classified information at an OA, DHS must inform the BIA of that possibility in DHS's notice that classified information may be used in the case or otherwise in advance of the OA, so that the BIA and EOIR can ensure proper technology is present at the hearing.

3. Other Evidence

If classified materials are placed in the record of a case, BIA personnel must follow appropriate procedures, as specified herein, to ensure that the classified information is not accessed by unauthorized persons. The classified evidence must be placed in an envelope separate from any unclassified information in the case and labeled with the applicable classification level on the outside of the envelope. The information must then be stored pursuant to the security procedures set forth herein.

4. Transcriptions

If OA audio recordings need to be transcribed, the transcription procedures are the same as specified above in Section VI.D, Transcription of Hearing Involving Classified Information.

5. Classification/Marking and Review

The procedures for marking and review of the transcripts of the OA by the originating agency are the same as specified above in Section VI.D, Transcription of Hearing Involving Classified Information.

6. Note-Taking

BIA personnel should avoid taking notes that contain classified information, unless necessary to fulfill their case responsibilities. *See supra* Section VI.L, Note-Taking, for specific guidance on note-taking.

F. Decisions by the BIA

1. Generally

All BIA personnel must avoid causing the disclosure of any classified information in the rendering of any BIA decision.

[10] SCI must be stored in a SCIF.

2. Preparation and Circulation of Proposed BIA Decision

a. A laptop and printer in the Restricted Access Room have been designated for the BIA's use for preparation of the BIA's decisions. Only the approved laptop and printer located in the Restricted Access Room may be used to prepare the BIA's decisions. *See also supra* Section VI.K, Computer Security. BIA JT may not be used to prepare, circulate, vote, or issue the BIA's decisions. In each case involving classified information, the BIA's decision, separate classified attachment (if any), and any related notes may not be removed from the Restricted Access Room.

b. When the proposed BIA decision is ready to be reviewed by the designated AIJ(s), a paper circulation sheet should be prepared and placed on top of the proposed decision. Also, the Attorney Advisor should advise the designated AIJ(s) that the BIA's decision has been prepared and is ready for review in the Restricted Access Room. The designated AIJ(s) must contact the Classified Case Coordinator(s) or designated SLA(s) for admission into the Restricted Access Room to review the decision. If oral discussions regarding classified information are necessary, they should take place in the Restricted Access Room. *See also supra*, Section VI.H, Oral Discussions.

3. Marking or Labeling Classified Attachment of the BIA's Decision

a. If the BIA determines that it is necessary to include classified information in a decision, the portion of the decision containing classified information must be prepared as a separate attachment so that the remainder of the decision may be released to the respondent and their representative. The BIA must confine any classified information to the classified attachment and not include any classified information in the rest of the decision. The decision should state, in sum and substance, whether the classified information contained in the attachment was material to the decision, without disclosing the substance or source of the classified information. Additionally, the following procedures must be followed in marking the classified attachment:

i. A cover sheet showing the classification level must be attached to the document.

ii. 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.

iii. 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; (C) for Confidential; and (U) for Unclassified.

iv. "Derived from" Line: The information on this line is obtained from the source document used in the proceedings.

v. "Declassify on" Line: The information on this line is obtained from the source document used in the proceedings.

b. Prior to releasing the decision, the decision and the classified attachment shall be sent to EOIR/OS using the transmittal procedures set forth in Section VIII, Transmittal of Classified Information, below. EOIR/OS will then forward the documents to DOJ's National Security Division, which will in turn transmit the documents to the originating agency for purposes of conducting a classification review in order to ensure that no classified information is disclosed in the decision and that all classified information in the attachment has been marked correctly. The entire decision, including the classified attachment, must be treated as presumptively classified, at the highest level of the classified information involved in the case, until the decision and attachment have been reviewed and cleared by the originating agency. The BIA's decision shall not be affected by the originating agency review. Rather, the role of the originating agency is strictly to ensure that the classified information is correctly marked and to provide a redacted version of the BIA's decision.

4. Final Disposition

a. Issuance of BIA Decision

EOIR/OS shall notify the BIA's Chief Clerk, Classified Case Coordinator(s), or other designated BIA personnel when the originating agency has completed the classification review of the BIA's decision and classified attachment, if any. Designated BIA personnel will issue a hard copy of *only* the unclassified BIA decision and serve it on the parties. However, a copy of the BIA's unclassified decision will not be available via BIA Decisions or in EOIR's Reading Room. Instead, a coversheet referring interested persons, who are authorized to access the BIA Decision, to contact the Chief Clerk or Deputy Chief Clerk, will be scanned and uploaded to BIA Decisions by the Classified Case Coordinator(s) or other BIA designated personnel.

b. Destruction of Reproductions

Copies of classified information (*e.g.*, drafts, working papers, notes, waste from reproduction, extra copies, and discs) that 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. Return of Classified Materials

Classified documents filed in a case may be returned to the filing party upon request and after consultation with the Central Security Coordinator. This must occur no later than 30 days after all proceedings in the case have concluded,

including the resolution of any appeals and federal court challenges or the expiration of the period for filing any such appeals or challenges. Classified materials that are part of the ROPs will remain with the case file and will be retained in appropriate storage in accordance with the procedures set forth herein until returned to the immigration court (or DHS, if the case is in visa petition, advance permission, or fine proceedings). However, the unclassified portion of the ROPs may be returned to the immigration court or DHS if the case is in visa petition, advance permission, or fine proceedings using routine mail handling. All classified portions of an ROP must be returned under the guidelines below in Section VIII, Transmittal of Classified Information.

d. Archiving

Archiving ROPs will be the responsibility of the immigration court or DHS if the case is in visa petition, advance permission, or fine proceedings.[11]

VIII. Transmittal of Classified Information

The following transmittal procedures must be followed any time classified information must be sent to another location. In all of these situations, the portion of the record that contains classified information—including the audio of any classified hearing, which should be placed on an approved portable storage device—shall be transmitted in the following manner, to protect the information against unauthorized access:

A. Confidential or Secret Information

1. The BIA's Security Coordinator, Classified Case Coordinator(s), or other designated BIA personnel shall notify EOIR/OS in advance that classified information will be transmitted to the immigration court and obtain from EOIR/OS the contact information of the appropriate individual(s) at the immigration court or federal court to receive the information. The BIA's Security Coordinator, Classified Case Coordinator(s), or other designated BIA personnel shall then notify the court, in advance, that the classified information will be transmitted.

2. All Secret or Confidential classified information physically transmitted shall be enclosed in two opaque layers. The inner enclosure shall clearly identify the name and address of both the sender and the intended recipient, the highest classification level of the contents, marked on the top and bottom, front and back, and any appropriate warning notices. The outer enclosure shall be the same, except that there should be no markings to indicate that the contents are classified.

3. This double-wrapped package must be transmitted by USPS via Registered Mail, Return Receipt Requested, or by USPS Express Mail, Return Receipt Requested, or

[11] DHS creates and maintains the record in visa petition, advance permission, and fine proceedings and is in charge of archiving these ROPs.

through FedEx. Packages must be hand-carried to the Post Office or to the FedEx location by the BIA's Security Coordinator, Classified Case Coordinator(s), or other designated BIA personnel. Do not use a street-side mail or FedEx collection box. The Waiver of Signature and Indemnity Block on the USPS Express Mail Label shall not be completed. The unclassified and classified portions of the ROP must be mailed separately, not within the same shipment, to the immigration court.

4. When a package containing classified information is sent to the immigration court, notify the individual to whom it is addressed of the estimated date of arrival and include the tracking number.

B. Top Secret Information and SCI

Any record containing Top Secret information or SCI cannot be mailed or sent by commercial carrier and must be hand-carried in an approved courier pouch. This package then must be hand-carried from the BIA to its destination by an individual cleared at the Top Secret level (and specific SCI compartment, if applicable) and designated as a classified courier. The BIA must contact EOIR/OS for assistance in making special arrangements for the transport of any material containing Top Secret information or SCI to an immigration court or federal court.[12]

IX. Certification of Records

1. The BIA may be requested to certify a case record containing classified information. If the BIA does not have the ROPs, the ROPs will need to be obtained from the immigration court, and the procedures for receipt of classified materials in Section V.D, Instructions for Receipt of Classified Materials from OCIJ at the BIA Clerk's Office, must be followed.

2. Requests to certify a record including classified information are generally the result of the respondent filing a petition for review with a United States Court of Appeals or a case in federal district court involving proceedings other than removal proceedings (*e.g.*, bond proceedings and reasonable fear proceedings). In those cases, the BIA processes a certification request in conjunction with DOJ's Office of Immigration Litigation (OIL) and/or the U.S. Attorney's Office handling the case. The procedures below address certification requests from OIL in connections with petitions for review. If the certification request comes from another federal agency, the BIA's Security Coordinator, Classified Case Coordinator(s), or other designated BIA personnel will work with EOIR/OS in order to fulfill the request and ensure proper safeguarding of classified information.

A. Verification of Certification Request

1. The certification request will initially be received by the BIA's Clerk's Office. Thereafter, the Classified Case Coordinator(s) or other designated BIA personnel will

[12] SCI must be stored in a SCIF.

take responsibility over processing the certification request.

2. Prior to processing a certification request from OIL, the Classified Case Coordinator(s) or other designated BIA personnel must obtain the following: (i) docket number of the respondent's federal court proceedings; (ii) number of certified copies requested; (iii) date certified copies are due to OIL, and (iv) the name(s) and telephone number(s) of the individual(s) at OIL to whom the certified classified copies are to be transmitted. Also, 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 supra* Section VI. J, Reproduction Security.

C. Transmittal of Certified Copies

1. The same wrapping procedures addressed in Section VIII, Transmittal of Classified Information, above shall be followed, except that the certified copy of the classified document or case will not be mailed or sent by FedEx. The certified classified copy or copies must be hand-carried to OIL by an individual with the appropriate security clearance. EOIR/OS or other designated DOJ personnel must be contacted for assistance in making the arrangements for the transport of the certified copies by a designated classified courier.

2. OIL is responsible for filing the certified copy of the classified document or case with the appropriate federal court. The BIA is responsible for uploading unclassified portions of the certified record with the appropriate federal court.

D. Notify Receiver

The Classified Case Coordinator(s) or other designated BIA personnel will notify OIL that the certified classified copy(ies) is/are en route to ensure that the package is received.

X. Processing Formerly Classified Case No Longer Involving Classified Information

The BIA may receive a case from an immigration court or DHS that involved classified information, but the case no longer involves such information (*e.g.*, classified information returned to the originating agency and is no longer provided or needed for adjudication). Although such a case may no longer involve classified information, the BIA will nonetheless employ heightened procedural safeguards when handling such a case.

A. Post-BIA Decision Case Monitoring

Even though the BIA is unlikely to receive advance notice that a case previously contained classified information but no longer does, the Classified Case Coordinator(s) shall maintain a

report to monitor the activity on cases that were previously processed at the BIA. The Classified Case Coordinator(s) is responsible for reporting findings to the BIA's Security Coordinator, and the designated SLA. This report shall be part of the BIA'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 or other designated BIA personnel will take responsibility over processing the case through the Clerk's Office.

1. Verification of Non-Classified Status of Case

The Classified Case Coordinator(s) shall verify with the immigration court or DHS that the case no longer involves or contains classified information. The Classified Case Coordinator(s) will also consult with EOIR/OS as needed regarding any classified material relating to the case in EOIR's possession. If the pending matter before the BIA 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(s) will advise BIA's Security Coordinator immediately, and the case will be processed according to the appropriate procedures set forth herein.

2. Non-Classified Status Verified

The Classified Case Coordinator(s) 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(s) will advise the designated SLA(s), who will contact the Chief Appellate Immigration Judge and/or Deputy Chief Appellate Immigration Judges regarding the assignment of the case to a BIA Panel. The SLA(s) also will contact the Director of Operations and Senior Panel Attorneys for assignment of the case to an Attorney Advisor.

XI. Processing a Case Upon Discovery of Possible Information Obtained From A Source Other Than an Originating Agency

1. The BIA may receive a case that has classified information obtained by the respondent, possibly through publicly available sources.

2. Classified information obtained from a source other than an originating agency can appear in the ROP or eROP in any number of ways. There may be a reproduction of a page or a reference in a document that the information came from a publicly available source. There also may be a transcript reference to a document as coming from a publicly available source, or there may be testimony that repeats or summarizes information obtained through a publicly available source. Also, it is possible that this information may have been submitted at the immigration court level but was not discovered at that level and may not come to light until on review before the BIA.

3. As noted above in Section V.B, Safeguarding Classified Information, all BIA personnel are obligated to protect classified information. The fact that classified information may have been disclosed to the public or was not properly identified before the immigration court does not change the fact that the information is still classified. The public availability of classified information does not relieve BIA personnel from their obligation to treat the information as classified when it comes into the custody of the BIA.

A. Steps to Take if Information Is Found or Suspected

1. If BIA personnel discover, or even believe, that they have encountered classified information, the following steps should be taken immediately to ensure that information is handled properly.

    a. Secure the information immediately.

    b. Do not attempt to verify whether the information is classified.

    c. Notify a supervisor immediately, who will then notify the BIA's Security Coordinator, Classified Case Coordinator(s), and/or designated SLA(s) of the receipt and the case involved. If your supervisor or another supervisor is not available, contact the BIA's Security Coordinator, Classified Case Coordinator(s), and/or designated SLA(s) directly. EOIR/OS should be contacted if the BIA's Security Coordinator, Classified Case Coordinator(s), and/or designated SLA(s) are not available.

    d. Keep a written record of the handling of the material since it came into your custody (e.g., how you came upon it, what steps you took to secure and notify, the appropriate personnel and the time and date of each step). Do not forward the material via email, including to a supervisor, the BIA's Security Coordinator, Classified Case Coordinator(s), and/or designated SLA(s).

2. EOIR-issued laptops and computers are not certified to process classified information and should not be used to process classified information, including potentially classified information discovered as described above. *See supra* Section IV.B.3, Unauthorized Disclosure.

B. Steps to Take if Working at Home

The process is the same. If BIA personnel are working on a case at home and discovers, or believes that they have discovered, classified information obtained through a publicly available source or other source, follow the steps listed above.

C. Classification Markings: Indicator of Classified Information

1. In general, classified information is marked or labeled by the agency. *See supra* Section VII.F.3, Marking or Labeling Classified Attachment of the BIA's Decision.

2. 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. If any portion of a document has markings at the Top Secret, Secret, or Confidential level, then the entire document is treated as classified. The following classification levels and/or symbols for information that is classified may be seen in the document:

   Top Secret "(TS)"

   Secret "(S)"

   Confidential "(C)"

3. A document may have a non-classified markings and/or symbols that reflect that information is not classified. The following non-classified markings and/or symbols may be seen in the document:

   Unclassified "(U)"

   Sensitive but Unclassified "(SBU)"

   Controlled Unclassified Information "(CUI)"

   For Official Use Only "(FOUO)"

   Limited Official Use "(LOU)"

4. Be aware that, just because a document may contain unclassified information, that does not change the overall classification of the document if it also contains classified information. The entire document is still considered classified at the highest level as listed above in Section II, Definitions.

XII. Post-Decision Handling of Classified Materials

A. Return of Classified Materials

At the conclusion of the proceedings before the BIA, the BIA's Security Coordinator will arrange for the ROP to be returned to the immigration court (or DHS if the case is in visa petition, advance permission, or fine proceedings) for archiving and return of any classified information to the originating agency. This must occur no later than 30 days after all proceedings in the case have concluded, including the resolution of any appeals and federal court challenges or the expiration of the period for filing any such appeals or challenges. Classified decisions or attachments will not be released to the parties, but will remain with EOIR consistent with procedures consistent with this section. Classified decisions or filings should be retained in appropriate storage in a security container or secure room until archived. Audio of classified hearings should likewise be stored pursuant to the procedures set forth herein until archived. *See supra* Section VII.E.2.a, Recording. The BIA Security

Coordinator must consult with EOIR/OS and the EOIR Agency Records Officer prior to destroying any audio of classified hearings.

B. Storage, Retention, and Destruction of Classified Information

Documents and other material, such as attorney and AIJ notes, which are identified for destruction must continue to be stored pursuant to the procedures specified herein until and unless EOIR/OS and the Agency Records Officer determine destruction is appropriate. The Agency Records Officer and EOIR/OS must be consulted prior to the destruction of any classified information.

C. Archiving Classified Evidence

1. The form used by the immigration court to archive records, SF-135, must indicate the classification level of the classified records being archived and the relevant Federal Records Center must be notified that a cleared driver will be required to transport the materials. The Central Security Coordinator must maintain a record of archived classified filings in EOIR proceedings.

2. Records containing Top Secret information must be transported from the court to the Federal Records Center by the Defense Courier Service.

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

XIII. Implementation and Training

A. Implementation

Within 30 days of the issuance of this OPPM, the BIA shall undertake a review of the existing practices and physical infrastructure at the BIA, and shall consult with the Central Security Coordinator regarding any adjustments to the BIA's practices and infrastructure that will be necessary to ensure that the procedures set forth herein are properly implemented and followed.

B. Training

Within 30 days of the issuance of this OPPM, the BIA will work with the Central Security Coordinator to conduct training(s) for all cleared BIA personnel on the procedures set forth herein. Going forward, the Central Security Coordinator shall conduct such trainings for all cleared BIA personnel on an annual basis.