OOD
PM 25-37 (Amended)
Effective: September 23, 2025

To: All of EOIR
From: Roman Chaban, Acting Deputy Director
Date: September 23, 2025

ROMAN CHABAN
Digitally signed by ROMAN CHABAN
Date: 2025.09.23 12:45:11 -04'00'

CLASSIFIED INFORMATION IN EOIR PROCEEDINGS

PURPOSE:	Consolidate and update EOIR policies regarding the handling of classified information in EOIR adjudicatory proceedings
OWNER:	Office of the Director
AUTHORITY:	8 C.F.R. § 1003.0(b)
CANCELLATION:	OCIJ Operating Policies and Procedures Memorandum (OPPM) 24-01, *Classified Information in Immigration Court Proceedings*, and BIA OPPM 24-01, *Classified Information at the Board of Immigration Appeals*

Table of Contents

I. Introduction and Scope

This Policy Memorandum (PM) updates EOIR guidance on the proper handling of classified information in most adjudicatory proceedings, including those before the Office of the Chief Immigration Judge (OCIJ), Board of Immigration Appeals (BIA), and the Office of the Chief Administrative Hearing Officer (OCAHO).[1] To consolidate guidance in one location, particularly for cases involving classified information adjudicated by OCIJ and then appealed to the BIA, this PM rescinds, cancels, and supersedes two prior Operating Policies and Procedures Memoranda (OPPM), OCIJ 24-01*, Classified Information in Immigration Court Proceedings* and BIA 24-01, *Classified Information at the Board of Immigration Appeals*, but incorporates most of the information in those OPPM herein. For the first time, it also provides guidance for the handling of classified information before OCAHO.

The handling of classified information at EOIR 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 policy includes all relevant regulations under Titles 8 and 28 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. To the extent there is any conflict between this PM and any statute, regulation, Executive Order, DOJ policy, or other applicable source of law, the other authority shall control.

[1] EOIR operates other adjudicatory proceedings in which classified information is unlikely to be at issue. *See*, *e.g.*, 8 C.F.R. §§ 1292.11-1292.20 (detailing EOIR's recognition and accreditation program which includes provisions for adjudicatory review of certain decisions). Nevertheless, should classified information be involved in such proceedings, EOIR will follow all applicable laws and policies and use the instant PM as a guide to handling that information.

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 memorandum, EOIR personnel shall request assistance and guidance from the EOIR Office of Security (EOIR/OS). At OCIJ, this is coordinated through each court's Court Administrator or Assistant Chief Immigration Judge (ACIJ). At the BIA, this is coordinated through the BIA Security Coordinator. At OCAHO, this is coordinated through the Chief Administrative Hearing Officer (CAHO) or Chief Administrative Law Judge (Chief ALJ).

EOIR personnel must protect classified information and prevent its unlawful or unauthorized disclosure. EOIR 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 position, and/or criminal prosecution.

If you have any questions regarding the procedures set forth in this memorandum, please contact your supervisor or EOIR/OS.

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," E.O. 13526 § 6.1(gg), 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;" or

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, EOIR personnel must contact the Central Security Coordinator (*see infra* Section III.A.) immediately if a party[2] notices the intent to use SCI or if EOIR 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 and/or process the material. The Central Security Coordinator will also work with the agency submitting the SCI to ensure that EOIR personnel receiving the material are cleared to receive it.

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 EOIR, 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. At OCIJ, a Court Administrator serves as the Security Coordinator at his or her assigned court(s) and reports to and receives guidance from the Central Security

[2] The term "party" is used in this memorandum to encompass any individuals or entities who may appear before the immigration courts, the BIA, or OCAHO.

Coordinator related to these procedures and handling of classified information.[3] *See infra* Section III.B. At the BIA, the BIA Security Coordinator reports to and receives guidance from the Central Security Coordinator related to these procedures and handling of classified information. At OCAHO, the Deputy Chief Administrative Hearing Officer (Deputy CAHO) serves as the Security Coordinator.

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 resources are 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. Security Coordinator at Each Immigration Court

1. The Court Administrator for each court is designated as the Security Coordinator for all cases at that court involving classified information.

2. The Court Administrator and the ACIJ with responsibility for the Court Administrator's court(s) must obtain and maintain TS/SCI clearance.

3. The Court Administrator, as the Security Coordinator, is responsible for ensuring that these procedures are properly implemented at the Court Administrator's assigned court(s), and that all OCIJ personnel at the assigned court(s) are aware of these procedures and their obligation to follow them.

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

5. The Court Administrator must notify the ACIJ with responsibility for the Court Administrator's court(s), as well as the Central Security Coordinator, immediately upon learning that a case may involve the use of classified information. OCIJ personnel who learn that a case may involve the use of classified information must immediately notify the Court Administrator.

6. In a case involving classified information, the Court Administrator (as the Security Coordinator) is responsible for physically taking possession of any classified materials directly from the filing party and immediately securing the materials in a

[3] Court Administrators are within OCIJ; the Central Security Coordinator is within EOIR/OS.

security container approved by the General Services Administration (GSA)[4] as set forth below in Section V.B, Safeguarding Classified Information.

C. BIA Security Coordinator

1. The 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(s), and the designated Senior Legal Advisor(s) (SLA(s)), 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, inter alia, 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 security container approved by GSA, as set forth below in Section V.B, Safeguarding Classified Information.

D. OCAHO Security Coordinator

1. The Deputy CAHO is designated as the Security Coordinator for all cases at OCAHO involving classified information.

2. In the event that a party seeks to introduce classified information in an OCAHO proceeding, the following individuals within OCAHO may be required to obtain a TS/SCI clearance: the Chief Administrative Hearing Officer; the Deputy CAHO; the Chief ALJ; and a paralegal or other appropriate support person.

[4] In this memorandum, except for the limited discussion of SCI (which is stored in a SCIF), EOIR focuses on the use of "secure containers." Should EOIR require the use of a "secure room" (space that is authorized under regulation, and approved by the Department Security Officer at SEPS, as an open storage area for classified information), EOIR's Central Security Coordinator will coordinate with DOJ to obtain appropriate access to such a location.

3. The Deputy CAHO is responsible for ensuring that these procedures are properly implemented at OCAHO, and that all OCAHO personnel are aware of these procedures and their obligation to follow them.

4. The Deputy CAHO's responsibilities as OCAHO's Security Coordinator include, inter alia, overseeing the transmission, handling, and storage of classified information, and ensuring that all OCAHO personnel authorized to access such information follow these procedures so that the unauthorized disclosure of classified information does not occur.

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

6. In a case involving classified information, the Deputy CAHO (as OCAHO's Security Coordinator) is responsible for physically taking possession of any classified materials directly from the filing party and immediately securing the materials in a security container approved by GSA, as set forth below in Section V.B, Safeguarding Classified Information.

E. Other Cleared EOIR Personnel

1. EOIR/OIT coordinates all required security procedures for the agency in conjunction with DOJ's Office of the Chief Information Officer (DOJ/OCIO) and in consultation with EOIR/OS and the relevant EOIR stakeholder(s). EOIR/OIT is responsible for obtaining the needed expertise and technology from DOJ/OCIO in any and all situations where IT is required (*e.g.*, processing, incident response, etc.). EOIR/OIT will provide DOJ/OCIO with the necessary guidance on EOIR networks and systems in order for DOJ/OCIO to execute on the requirements (*e.g.*, hardware, software, etc.) in a given scenario.

2. The Court Administrator may designate appropriately cleared OCIJ personnel, *see infra* Section IV, to assist with ensuring that the security safeguarding procedures set forth herein are followed in a particular case, or in all cases, at the Court Administrator's assigned court(s), including to assist with entering the proper "Secure Access Status" identifier in Case Access System for EOIR (CASE). This is necessary in part so that if a particular Court Administrator is unable to be present at a hearing site where classified information will be used, or if there are several cases involving classified information under the purview of the Court Administrator at a given time, additional designated OCIJ personnel are available to assist in implementing the appropriate security procedures.

3. The BIA's Security Coordinator, who is the Chief Clerk, may designate appropriately cleared BIA personnel per Section IV, *infra*, to assist with ensuring that the procedures set forth herein are followed. This is necessary, in part, so that 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, additional

designated BIA personnel are available to assist in implementing the appropriate security procedures.

4. The BIA's Chief Clerk and Classified Case Coordinator(s) work in conjunction with one or more designated SLA(s), who assist them in fulfilling their responsibilities. The designated SLA(s) also work with the Central Security 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.

5. OCAHO's Security Coordinator may designate other appropriately cleared OCAHO personnel to assist with ensuring that the security safeguarding procedures set forth herein are followed in a particular case, or in all cases, at OCAHO. This is necessary in part so that if the OCAHO Security Coordinator is unable to be present at a particular hearing, pre-hearing conference, or other event where classified information will be used in an OCAHO proceeding, additional designated OCAHO personnel are available to assist in implementing the appropriate security procedures.

IV. Access to Classified Information

In addition to obtaining TS/SCI clearances for designated personnel at EOIR/OS and the Security Coordinators at each adjudicating component, the adjudicating components must additionally obtain and maintain clearances for the following personnel. At OCIJ, all supervisory judges (Chief Immigration Judge (CIJ), Regional Deputy Chief Immigration Judges (RDCIJs), and ACIJs) and Court Administrators must have TS/SCI clearances. Immigration Judges may be required to obtain TS/SCI clearances as needed. At the BIA, all Appellate Immigration Judges (AIJs) must have TS or TS/SCI clearances. Certain Attorney Advisors and designated Support Staff in the Clerk's Office may also have TS or TS/SCI clearances.

Senior leaders in the adjudicating components or their designees, in coordination with EOIR/OS, regularly review which, and how many, EOIR personnel have clearances to ensure, among other reasons, that there are sufficient personnel to process cases that involve classified information. When EOIR personnel have a need to access classified information in connection with their duties, EOIR/OS must confirm that the applicable EOIR personnel possess the requisite clearance level for accessing the information. EOIR/OS, as opposed to EOIR personnel, is responsible for assessing and determining whether any particular EOIR personnel are authorized to access classified information, before the EOIR personnel are permitted to access the information.

A. Requirements for Access to Classified Information

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

   a. Possess the requisite level of security clearance;

   b. Have demonstrated a need to know the information; and

c. Have 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. EOIR personnel must possess the requisite security clearance before accessing classified information. Requests for security clearances for EOIR personnel must be made by EOIR/OS, in consultation with the relevant ACIJ, RDCIJ, and the CIJ, in the case of OCIJ; the BIA's Executive Officer, in the case of the BIA; or the Chief Administrative Hearing Officer (CAHO) and Deputy CAHO, in the case of OCAHO. EOIR personnel requiring security clearance must not submit a request for the security clearance on their own behalf. EOIR/OS will notify individuals requiring a clearance if/when the clearance (Top Secret, Secret, or Confidential) has been granted.

4. EOIR/OS will provide each EOIR personnel member who is granted 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. The recipient may contact EOIR/OS if additional copies of any information in the security clearance packet are needed.

5. If a security clearance cannot be promptly obtained for OCIJ personnel at a particular court handling a case involving classified information, the relevant Court Administrator, ACIJ, or RDCIJ may temporarily assign OCIJ personnel from another court location, with the requisite clearance, to assist with the handling of that case.

B. Responsibilities to Ensure the Safeguarding of Classified Information

1. Disclosure to EOIR Personnel

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

   b. Court Administrators, ACIJs, the BIA's Security Coordinator, Classified Case Coordinator(s), designated SLA(s), the Deputy CAHO, and other appropriately cleared EOIR personnel with access to classified information used in a particular case may disclose such information to other appropriately cleared EOIR 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.

c. Confirmation that EOIR personnel have the requisite security clearance and non-disclosure agreement can be requested from EOIR/OS by the Court Administrator or ACIJ (at OCIJ) or the BIA's Chief Clerk, Classified Case Coordinator(s), or designated SLA(s) (at the BIA).

d. Because appropriately cleared EOIR 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 EOIR personnel, so long as the personnel meet the requirements specified above.

2. Disclosure to Persons Outside EOIR

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

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

c. In accordance with 28 C.F.R. § 68.42(b)(2), an Administrative Law Judge (ALJ) presiding over an OCAHO case involving classified information may direct the party seeking to introduce classified information to permit the opposing party or parties to have access to such information, provided that those parties have obtained the appropriate security clearances. However, the ALJ shall not personally disclose any such classified information, or the existence thereof, to any other party or person outside of EOIR.

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, EOIR 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, EOIR personnel are not permitted to access information marked or labeled classified, including any such information from publicly available sources. EOIR 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.E.3., Computer Security, Media) must immediately contact the Central Security Coordinator and provide notification to EOIR/OIT.

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 EOIR (*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 an adjudicating component shall be handled only by OCIJ, BIA, or OCAHO 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 for reasons specifically set forth below. The designated Security Coordinators for each adjudicating component 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) or OCAHO's electronic case management system or electronic case files.

    a. At OCIJ, materials containing classified information must never be saved in any electronic Record of Proceeding (eROP) in ECAS. Instead, a paper Record of Proceedings (ROP) must be created. Upon receipt of classified information in a particular case, the Court Administrator or appropriately cleared OCIJ personnel shall convert the court's file for that case from an eROP into a paper ROP (*i.e.*, the case file must be converted from electronic form into a 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 court-issued notice that the case is no longer eligible for electronic filing or processing and that all future filings must be submitted in paper format. 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 OCIJ 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 stored and safeguarded according to the procedures below. Unclassified portions of the paper ROP may be maintained separately.[5]

b. At the BIA, upon receipt of classified information 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 form into a 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 format. 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.

c. At OCAHO, materials containing classified information must never be saved in an electronic case file or any electronic case management system. If classified information is introduced in an OCAHO proceeding, the OCAHO case file for that case must be converted into a paper case file and maintained exclusively as a paper case file for the remainder of the proceedings. For cases involving classified information, any existing unclassified documents contained in the OCAHO electronic case file must be printed, a paper OCAHO case file must be constructed, and the electronic case file must be deactivated. If the case is enrolled in electronic filing, the parties must be notified through an OCAHO-issued notice that the case is no longer eligible for electronic filing or processing, and that all future filings must be submitted in paper format. Such notice must be sent in hard copy only, and all subsequent filings must be made (and all subsequent orders must be issued) in hard copy. Only cleared OCAHO personnel may assist in the conversion of the OCAHO electronic case file into a paper case file. Following conversion of the case file into a paper form, the classified portions of the paper OCAHO case file must be stored and safeguarded according to the procedures below. Unclassified portions of the paper OCAHO case file may be maintained separately.

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

3. All classified materials[6] in the custody of adjudicating components shall be stored in a GSA-approved security container (*i.e.*, safe). The combinations for security containers are classified at the same level as the highest level of classified material stored within the container. Combinations of security containers shall be changed by the designated Security Coordinators for each adjudicating component or EOIR/OS when the container is first placed in service, when the combination has been subject to possible compromise, when an individual knowing the combination no longer requires access to the security container, and when the container is taken out of service. After consultation with the Central Security Coordinator, the designated Security Coordinators for each adjudicating component may provide the combination for a security container to other personnel who possess the requisite security clearance, have signed a non-disclosure agreement, have a need to know, and require access to the container. The designated Security Coordinators for each adjudicating component must inform the Central Security Coordinator whenever there is a change in personnel and an individual no longer requires access to a particular security container combination. The designated Security Coordinators for each adjudicating component 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 appropriate case identifiers (*i.e.,* for OCIJ and BIA by the alien registration number (A number) and for OCAHO by the case number). Unclassified materials must not be stored in these security containers.

5. Classified material must be kept in security containers as set forth above and must not be taken out of such containers unless the material is being reviewed by authorized personnel, returned to the filing party or originating agency, sent to an adjudicating component, certified and transported for further litigation, or being archived. *See also infra* Sections VII.M., Transmittal of Classified Information, and X.A., Return of Classified Materials. 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 VI, Security Procedures; V.E., Restricted Access Room – BIA.

6. Classified material must never be taken to any person's home under any circumstances. If any part of an ROP is classified, the entire ROP must be reviewed and maintained either at the adjudicating component's location or at a designated secure facility.

7. Access to classified information by EOIR personnel shall be limited to the minimum number of cleared personnel necessary to effectively carry out the administration of

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

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 properly be accounted for on each occasion that such material is taken out of the security container. The Security Container Check Sheet, Form SF-702, must be affixed to the outside of the security container to track who had access to the security container and the date and time of each such access. Only those individuals authorized to open security containers must annotate the Form SF-702. By contrast, any authorized personnel covered in Section III that remove classified information from the safe must document such removal in an unclassified register document. An unclassified register document tracks who had access to the security container, the classified material they used, and when the material was removed and then returned.

C. Receipt of Classified Materials from OCIJ at the BIA Clerk's Office

1. 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 immigration courts must follow the specific procedures for the sending and receiving of classified information. *See infra* Section VII.M., Transmittal of Classified Information.

2. After arrival at the BIA's Clerk's Office, the package with classified information will be picked up by designated and cleared BIA personnel, and the personnel shall immediately hand-carry the unopened 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.

3. 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.E.).

4. Material containing Top Secret information must always be hand-carried to the destination by an individual cleared at the TS 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, for the information to be properly received at the BIA.

5. When not in use, classified materials shall be stored in the GSA-approved security container (*i.e.*, 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 alien involved in the case. Unclassified materials must not be stored in the security container.

6. Once the classified materials arrive at the BIA, the Chief Clerk, Classified Case Coordinator(s) or other designated personnel must update CASE to reflect the arrival of the classified materials, 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.

D. Secure Access Report – BIA

The Classified Case Coordinator(s) or other designated personnel must 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 must not include any classified information. The report will also be made available to EOIR/OS at its request.

E. Restricted Access Room – BIA

1. Classified information in immigration cases received at the BIA must be kept in the security container 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. Unless labeled as such, EOIR-issued laptops and computers are not approved[7] to process classified information and should not be used to process classified information. Computers used to process classified information must be specifically 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 approved for processing classified information.

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

[7] In this memorandum, the term "approved" is used to describe laptops, computers, and copiers that are "certified, accredited, and approved" for classified processing, as described *infra*, in Section VI.E., Media.

5. An employee's office, position, rank, or security clearance do 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, in accordance with Section V.B.8., Safeguarding Classified Information.

7. EOIR/OS maintains the master combination for the security container 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, as described in Section V.B.3., *supra*. 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 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. Oral Discussions

Any discussion 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.). Authorized personnel shall ensure that unauthorized persons cannot overhear discussions or see 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. BIA personnel must 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.

B. 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.

C. Reproduction Security

1. Generally

   a. Reproduction of classified information may only be performed by persons authorized to access classified information in accordance with these procedures.

   b. Copies of classified information are subject to the same controls as the original information. Only an approved copier by EOIR's Chief IT Security Officer in consultation with EOIR/OS may be used.

   c. Before making copies, such authorized personnel shall ensure that any person not authorized to access the classified information cannot view or otherwise access the information during reproduction. As such, copiers used for the reproduction of classified information must be located in a private space to reduce the possibility of unauthorized disclosure.

   d. 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. Under no circumstances may network copiers be used to reproduce classified information.

2. Immigration Court

   If an immigration court must reproduce or copy any document involving classified information, the Court Administrator must contact the Central Security Coordinator for specific instructions.

3. BIA

   An approved copier has been designated for the BIA's use in the Restricted Access Room. *See supra* Section V.E., Restricted Access Room – BIA.

4. OCAHO

   If OCAHO must reproduce or copy any document involving classified information, the Deputy CAHO must contact the Central Security Coordinator for specific instructions.

D. Note Taking

1. EOIR 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.*, for the BIA, 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 adjudicating component.

2. For information regarding marking or labeling, *see* Section VII.J.3., EOIR Decisions, Marking or Labeling the Classified Attachment of an EOIR Decision.

E. Computer Security

1. Generally

    All IT resources used to access and process classified information must be certified, accredited, and approved by DOJ/OCIO in consultation with EOIR/OIT and EOIR/OS.

2. Approved Laptop Computers Must be Used.

    a. Any document prepared by adjudicating component personnel containing classified information must only be processed using a laptop computer specifically approved by DOJ/OCIO for classified processing in connection with specified cases 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.

    b. The approved laptop must always be kept within the authorized user's control, must never be taken outside of the adjudicating component's premises 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.

c. Computer equipment approved for processing classified information must be used in a space where the access can be limited, and the processing can be accomplished without observation or monitoring by unauthorized persons. While using an approved laptop or other computer equipment authorized for processing classified information, the authorized user must be mindful of his or her surroundings to guard against unauthorized disclosure.

d. Depending on the type of facility where the adjudicating component is located and the classification level of any classified materials, additional safeguards may be required. Whenever a laptop or other electronic equipment is approved by DOJ/OCIO for use at an adjudicating component for processing classified information, the Central Security Coordinator must consult with the designated Security Coordinators for each adjudicating component regarding the potential need for, and implementation of, any such additional safeguards.

e. Below are procedures that must be followed by the specific adjudicating component.

i. Immigration Court

1. When an immigration court anticipates that it will be required to take notes or create a written document containing classified information (including drafting a decision), the Court Administrator, as the Security Coordinator for that immigration court, will notify the ACIJ as well as EOIR/OS and request an approved laptop computer from DOJ/OCIO via EOIR/OIT for use in connection with the specified case(s) involving classified information. The authorized OCIJ personnel using the 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 DOJ/OCIO and stored pursuant to the same security procedures set forth herein applicable to the laptop. *See also infra* Section VI.E.3., Computer Security, Media.

2. Once the immigration court no longer requires use of the approved laptop computer for the designated case(s), the Court Administrator must ensure that EOIR/OS is notified, and the computer is returned to EOIR/OIT. The procedures set forth below, applicable to the transmission of classified information, must be used for returning the laptop, depending on whether the computer was used for Top Secret, Secret, or Confidential information processing. *See infra* Section VII.M., Transmittal of Classified Information.

ii. BIA

1. 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.

2. 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 DOJ/OCIO and stored pursuant to the same security procedures set forth herein applicable to the approved laptop. *See also infra* Section VI.E.3., Computer Security, Media.

3. The approved laptop must always be kept within the authorized user's control, 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.

iii. OCAHO

1. When OCAHO anticipates that it will be required to take notes or create a written document containing classified information, including drafting a decision or order, the Deputy CAHO, as the OCAHO Security Coordinator, should request an approved laptop computer from DOJ/OCIO for use in that case. The authorized OCAHO personnel using the 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 DOJ/OCIO and stored pursuant to the same security procedures set forth herein applicable to the laptop.

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 an adjudicating component from and approved by EOIR/OS and DOJ/OCIO 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 media 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 VII.M., Transmittal of Classified Information.

4. Printers

Any document containing classified information must be printed, to the extent necessary for the adjudicating component's operations, only on a printer that has been approved by DOJ/OCIO in consultation with EOIR/OIT and EOIR/OS, for the

printing of classified information. If the adjudicating component's personnel believes that the printing of classified information is required, they should contact the Central Security Coordinator, who will coordinate the provision of an approved printer[8] if necessary and provide instructions regarding the marking, storage, and any transmittal of such printed materials.

VII. Procedures for Cases Involving Classified Information

A. Protective Orders

Upon a motion by a party, the adjudicating component 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.

B. Notice That a Case May Involve Classified Information – Generally

1. Parties may seek to use classified information in any matter within the jurisdiction of an adjudicating component.

2. When a party anticipates using classified information for the first time in a particular case before an adjudicating component, the party shall file a notice with the adjudicating component and serve a copy of the notice on the other party. The notice shall inform the adjudicating component and the other party that the introducing party 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 the party may seek to use—*e.g.*, documentary evidence or witness testimony—in order to facilitate the adjudicating component's preparation for the receipt and proper handling of any such classified evidence.

3. Upon receipt of such notice, EOIR personnel shall promptly notify EOIR/OS, as well as the following employees, that the case in question may involve classified information.[9]

    a. If the matter is before the immigration courts, EOIR personnel must notify the relevant ACIJ and Court Administrator at the immigration court. Although any Immigration Judge with the appropriate clearance may hear the case, the matter will generally be assigned to an ACIJ. Any ACIJ or management Immigration Judge with the appropriate clearance may be assigned (or re-assigned) the case. DHS, through the Interactive Scheduling System, may also schedule such a

[8] An approved printer has been designated for the BIA's use in the Restricted Access Room.

[9] For additional procedures specific to cases involving an application for asylum and withholding of removal, *see* 8 C.F.R. §§ 1240.11(c)(2), (c)(3)(iv) (applications for asylum and withholding of removal in removal proceedings), 1240.33(b),(c)(4) (applications for asylum and withholding of deportation in exclusion proceedings), 1240.49(c)(3), (c)(4)(iv) (applications for asylum and withholding of deportation in deportation proceedings).

matter directly to an ACIJ's docket, though the case may be subsequently re-assigned as appropriate. Matters docketed with an ACIJ must generally be resolved by the ACIJ within 60 days where possible, consistent with due process.

b. If the matter is before the BIA, EOIR personnel must notify the Chief Clerk and/or the Classified Case Coordinator(s) at the Office of the Clerk (Clerk's Office). 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 or the Classified Case Coordinator(s) at the Clerk's Office.

c. If the matter is before OCAHO, EOIR personnel must notify the Deputy CAHO and the Chief ALJ. Although any ALJ with the appropriate clearance may hear the case, in general such cases will be assigned (or reassigned) to the Chief ALJ.

4. If the party seeking to introduce classified information, in consultation with the originating agency and any other relevant agency, determines that notifying the alien of the potential use of classified information would be reasonably likely to cause a risk to public safety or national security, the introducing party may delay serving such notice on the alien for a period of 14 days after the notice has been filed with the adjudicating component or until the risk is no longer present, whichever is shorter. The introducing party may request that the adjudicating component 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.[10]

5. EOIR personnel do not have the authority to acknowledge the existence of classified information to individuals, other than appropriately authorized EOIR personnel, except when providing notice of the use of classified information to a party, as specifically provided for in this PM. The authority to permit any such disclosure of the existence or substance of classified information to other parties, including aliens and their representatives, rests with the originating agency, and no such disclosure shall be made without the written authorization of the originating agency.

6. EOIR personnel do not have the authority to declassify information. The authority to declassify information rests with the originating agency.

C. Specific Notice Considerations in the Immigration Courts and BIA

1. The immigration courts or the BIA may notify the alien on the record at a hearing, or send written notification to the alien, informing him or her that classified information is being received into evidence. The introducing party, in coordination with the originating agency and EOIR/OS, may provide him or her with an unclassified summary of the classified information, but is not required to do so. The

[10] This provision does not apply to parties seeking to introduce classified information in OCAHO proceedings. Parties seeking to introduce classified information in OCAHO proceedings must follow the procedures set forth in 28 C.F.R. part 68, including 28 C.F.R. § 68.42(b) (governing the use and introduction of classified or sensitive matter) and 28 C.F.R. § 68.36 (prohibiting *ex parte* communications).

adjudicating component, in this case, the immigration court or the BIA, shall not order the introducing party or the originating agency to provide an unclassified summary to the alien, or to provide EOIR, the alien, or his or her counsel with the basis for any decision not to supply the unclassified summary.

2. When a party submits classified information in adjustment of status cases, in addition to notifying the alien of the receipt of classified evidence consistent with the preceding paragraph, the adjudicating component should—whenever it believes that it can do so while safeguarding both the classified information and its source—inform the alien of the general nature of the information so that he or she 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 alien of the general nature of the information, the adjudicating component must consult with the introducing party, in coordination with the originating agency and EOIR/OS, to ensure that the general summary provided 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 the introducing party, the originating agency, or EOIR/OS determines that a general summary cannot be provided without containing or risking the disclosure of classified information, the adjudicating component shall not provide any such summary to the alien. The adjudicating component must defer to the determinations of DHS, the originating agency, and EOIR/OS on these issues.

D. Specific Notice Provisions before OCAHO

1. Prior to submitting or presenting classified evidence, the introducing party shall notify OCAHO and the opposing party that classified information will be provided to OCAHO.

2. If OCAHO receives notification from a party that it intends to introduce classified information into the record, and the presiding ALJ determines that such information should form part of the record, the ALJ may direct the producing party to prepare an unclassified or nonsensitive summary or extract of the original. 28 C.F.R. § 68.42(b)(1). That unclassified or nonsensitive summary or extract may be admitted as evidence in the record.

3. If the ALJ ultimately determines that use of the unclassified or nonsensitive summary or extract is inadequate and that classified information must form part of the record, the ALJ should immediately notify the Deputy CAHO of that determination so that appropriate provisions can be made for OCAHO's receipt and handling of classified information, in accordance with the provisions of this memorandum.

E. Custody and Bond Proceedings before the Immigration Courts

1. A custody or bond proceeding before the immigration courts involving the use of classified information must be conducted *ex parte* and *in camera* consistent with the procedures set forth herein. Courts are encouraged to record audio of custody and bond proceedings where DHS has noticed an intent to present classified information.

If recorded, the proceeding must be recorded on a laptop equipped with Digital Audio Recording (DAR) technology and approved by DOJ/OCIO for classified processing. The recording of the proceeding must not be uploaded to any online system, including but not limited to CASE. The approved laptop and any mobile storage media containing the recording of a proceeding involving classified information must be stored pursuant to the security procedures set forth above for laptops and other equipment containing classified information.

2. Pursuant to 8 C.F.R. § 1003.19(d), "[t]he determination of the Immigration Judge as to custody status or bond may be based upon any information that is available to the Immigration Judge." This includes classified information presented by DHS.

F. Hearings

1. Pre-Hearing Conferences before the Immigration Courts

   a. Any party before the immigration courts may move for a pre-hearing conference to consider matters relating to classified information that may arise in connection with the proceedings. Following such motion by a party, or *sua sponte*, the Immigration Judge shall hold a pre-hearing conference to consider any matters that relate to classified information or otherwise promote a fair and expeditious hearing. *See* 8 C.F.R. § 1003.21.

   b. DHS may request that the Immigration Judge conduct an *in camera*, *ex parte* pre-hearing proceeding to make determinations concerning the use, relevance, or admissibility of classified information. *See* 8 C.F.R. §§ 1240.9, 1240.47. Upon such a request, the Immigration Judge shall conduct an *in camera*, *ex parte* hearing to address such issues relating to the potential presentation of classified information.

2. *In Camera, Ex Parte* Proceedings before the Immigration Courts and the BIA[11]

   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. OCIJ and the BIA may not order or compel the disclosure of classified information to aliens or their representatives. *See generally* 8 U.S.C. § 1229a(b)(4)(B) (aliens in removal proceedings have the privilege of representation, a reasonable opportunity to examine the evidence against them and to present evidence on their behalf, but they are not entitled to examine "such national security information as the Government may proffer in opposition to [their] admission to the United States or to an application … for discretionary relief under this chapter"). If 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

[11] As used herein, "*ex parte*" refers to communications involving only the adjudicating component and the Government.

the case prior to the disclosure of any classified information to aliens or their representatives.[12]

c. Consistent with the notice provisions set forth above, the adjudicating component must notify the alien of any such *in camera, ex parte* hearing or conference, and the introducing party must notify the alien that classified information will be presented to the adjudicating component.

d. The adjudicating component should schedule the *in camera*, *ex parte* hearing involving classified information for a different time or date than the remainder of the hearing before the immigration court, or OA before the BIA, to ensure the alien's presence for the entirety of the proceedings apart from the portion of the proceedings involving classified information. The immigration court or BIA may schedule the *in camera*, *ex parte* hearing to a different date, rather than different time, if doing so is necessary to ensure the alien's presence.

e. When conducting an *in camera*, *ex parte* hearing involving classified information, the immigration court or 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 court or 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 courtroom or OA room, and clearing adjacent rooms if the walls are not soundproof.

f. Any classified document or unclassified summary of classified information submitted by any party to OCAHO bearing the seal, letterhead, or other official markings of any U.S. Government department or agency will be considered self-authenticating evidence, and the authenticity of such documents shall be deemed admitted.

g. Both prior to and following any such *in camera*, *ex parte* hearing, the alien and his or her representative should be allowed to present any evidence that they believe may be relevant to the hearing before the immigration court or the BIA.

h. 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 adjudicating component pursuant to the security procedures for the storage of classified materials set forth herein. The recording, transcript, and any other record of such

[12] Aliens and their representatives are not permitted to access certain classified information presented to the immigration court or the BIA, which must be safeguarded from such unauthorized disclosure. *See, e.g.*, 8 C.F.R. §§ 1240.11(a)(3), 1240.49(a) (a decision on an application for adjustment of status may be based on classified information, which is not made available to the alien), 1240.49(c)(3), 1240.49(c)(4)(iv) (an asylum applicant is not entitled to access classified information submitted by DHS).

an *in camera, ex parte* proceeding involving classified information must be maintained in the classified portion of the case's paper ROP (for the courts and the BIA) and stored in an approved storage device in a safe, never uploaded to an eROP, or DAR, and shall not be disclosed or otherwise made available publicly.

3. Hearings and Pre-Hearing Conferences before OCAHO[13]

   a. Any party before OCAHO may move for a pre-hearing conference to consider matters relating to classified information that may arise in connection with the proceedings. *See* 28 C.F.R. § 68.13(a). Following such a motion, or in the ALJ's own discretion, the ALJ may hold a pre-hearing conference to consider any matters that relate to classified information (including the possibility of the use of unclassified summaries or extracts, 28 C.F.R. § 68.42(b)(1)), or such other matters that may expedite or aid in the disposition of the OCAHO proceeding. 28 C.F.R. § 68.13(a)(2)(ix).

   b. If an OCAHO ALJ determines that classified information must form part of the record, the ALJ shall inform the parties of that determination and provide an opportunity for the parties to arrange for a party or its representative to have access to such information. Those arrangements may include allowing time for the parties to obtain appropriate security clearances. *See* 28 C.F.R. § 68.42(b)(2). A party seeking to introduce classified information in an OCAHO proceeding may request that the ALJ conduct an *in camera* pre-hearing proceeding to make determinations concerning the use, relevance, or inadmissibility of classified information. *See* 28 C.F.R. §§ 68.13(a), 68.42(b).

   c. When conducting an *in camera* hearing involving classified information, OCAHO must ensure that only parties and/or their representatives who are authorized to access the specific classified information are allowed to be present. Portable electronic devices (*e.g.*, smart watches, fitness trackers, laptops, mobile devices, and removable CD-R for music) are not permitted in any room where classified information may be discussed. OCAHO 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 courtroom or office, and clearing adjacent rooms if the walls are not soundproof.

   d. Any classified document or unclassified summary of classified information submitted by any party to OCAHO that bears the seal, letterhead, or other official markings of any U.S. Government department or agency will be considered self-authenticating evidence, and the authenticity of such documents shall be deemed

[13] OCAHO's regulations generally prohibit *ex parte* communications, *see* 28 C.F.R. § 68.36, and similarly contemplate that any classified information introduced in an OCAHO proceeding be made available to appropriately cleared parties and/or their representatives, *see* 28 C.F.R. § 68.42(b)(2). Accordingly, absent extraordinary and compelling circumstances supported by other legal authority, OCAHO review of classified information introduced in a particular case should not be *ex parte*.

admitted unless a party files a written objection to the authenticity of such documents prior to the hearing. *See* 28 C.F.R. § 68.46.

e. To the extent practicable, OCAHO should schedule the *in camera* hearing involving classified information for a different time or date than the remainder of the hearing to ensure that all parties and representatives involved in the case can be present for all but the portion of the proceedings involving classified information.

f. Both prior to and following such *in camera* hearing, all parties to the proceeding should be allowed to present all material and reliable evidence that they believe may be relevant to the hearing before OCAHO. *See* 28 C.F.R. § 68.40(b).

g. OCAHO's rules require that a verbatim written record be kept of all OCAHO hearings. For cases not involving classified information, this is typically done through use of an official court reporter. In cases involving classified information, if the use of traditional court reports is not feasible due to lack of necessary clearances or security procedures from the relevant court reporting company, OCAHO may elect to generate a verbatim written record of the classified portions of the hearing through other means (such as use of appropriate recording devices and subsequent transcription of those recordings).

h. At the close of an *in camera* 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 OCAHO 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* proceeding involving classified information must be maintained in the classified portion of the case's paper case file and stored on an approved storage device within a safe. Such recording, transcript, or any other record of the *in camera* proceeding involving classified information, must not be uploaded to an electronic case file or electronic case management system and must not be disclosed or otherwise made available publicly.

i. OCAHO personnel do not have the authority to declassify information. The authority to declassify information rests with the originating agency.

j. OCAHO procedures for handling and safeguarding classified information shall continue to apply if the case is subject to administrative review by the CAHO, including in cases in which the CAHO permits oral argument. *See* 28 C.F.R. § 68.54(b)(2).

4. Recording

a. EOIR will not use DAR technology that is connected to EOIR's network to record immigration court hearings, OA hearings, or OCAHO hearings involving classified information. Instead, a laptop computer equipped with DAR technology, which has been approved by EOIR/OS and DOJ/OCIO for processing classified information, shall be used to record any hearing involving classified information. Whenever a hearing or 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 DOJ/OCIO. The recording on the approved laptop and/or portable storage device used during this portion of the immigration court hearing, OA, or OCAHO hearing 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 one of EOIR's safes.[14]

b. When a party anticipates offering classified information or otherwise discussing classified information at an immigration court hearing, an OA, or an OCAHO hearing, the introducing party must inform the adjudicating component of that possibility in the party's notice that classified information may be used in the case. This must occur in advance of the immigration court hearing, OA, or OCAHO hearing for EOIR to ensure proper technology is present at the hearing.

5. Other Evidence

If classified materials are placed in the record of a case, EOIR 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.

6. Note Taking

If note taking is deemed necessary to fulfill case responsibilities in adjudicatory proceedings, *see supra*, Section VI.D., Note Taking, for specific guidance.

G. 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 Clerk's Office initially receives the Notice of Appeal.

2. DHS must comply with the procedures set forth in Section VII.B, 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

[14] SCI must be stored in a SCIF.

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 nor saved in any eROP. Cases involving classified materials should always be handled on an expedited basis.

H. Transcription of Hearing Involving Classified Information

1. Transcription of hearings involving classified information by the BIA 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 before a court or OA before the BIA 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 classification review. EOIR/OS will contact the BIA when the review of the transcript has been completed, and the transcripts returned to EOIR.

I. Completion of Briefing Schedule/Case Assignment – BIA

1. Upon completion of the BIA 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 Judge(s) 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 a SLA or an 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.

3. If any part of an ROP is classified, the entire ROP must be reviewed, and remain on-site, at the BIA at all times. The non-classified portion of the ROP may be reviewed on site in an attorney's office but must be stored in the Restricted Access Room. Additionally, BIA Judicial Tools (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.J.2, Preparation and Circulation of Proposed BIA Decision.

4. 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.D., Note Taking.

J. EOIR Decisions

1. Generally

   a. When an Immigration Judge renders a decision referencing classified information, the Immigration Judge must issue a written decision (not oral).

   b. BIA personnel must avoid the disclosure of any classified information in the rendering of any BIA decision. For specific information regarding the preparation and circulation of a proposed BIA decision, *see* Section VII.J.2., Preparation and Circulation of Proposed BIA Decision.

   c. In OCAHO cases, when an ALJ renders a decision referencing classified information, the ALJ must issue the decision in written (not oral) form.

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.E., 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.A, Oral Discussions. For cases involving classified information that are discussed or decided *en banc*, the BIA shall follow the same protocols for handling and safeguarding classified information as it does for regular cases involving classified information.

3. Marking or Labeling the Classified Attachment of an EOIR Decision

   If an EOIR adjudicator 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 all parties and representatives in the case. The adjudicating component 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:

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

b. Overall Classification Marking: The overall classification is the highest classification level of information contained in the document. The overall classification marking must be conspicuously placed at the top and bottom of the page. When using a computer, these markings can be entered as headers and footers.

c. Portion Marking: Subjects, titles, and paragraphs shall be marked to show the level of classified information contained in that portion. Classification level must be indicated immediately preceding or following the portion to which it applies: (TS) for Top Secret; (S) for Secret; (C) for Confidential; and (U) for Unclassified.

d. "Derived from" Line: The information on this line, which should appear on the first page of the document, is obtained from the source document used in the proceedings.

e. "Declassify on" Line: The information on this line, which should appear on the first page of the document, is obtained from the source document used in the proceedings.

4. Prior to releasing the EOIR adjudicating component's decision, the decision and the classified attachment shall be sent to EOIR/OS using the transmittal procedures set forth in Section VII.M., Transmittal of Classified Information, *infra*. 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 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 originating agency review shall not affect the substance of the EOIR adjudicating component's decision. 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 EOIR adjudicating component's decision.

5. Issuance of Adjudicating Component Decisions

a. Generally

Prior to release, the decision and any classified attachment shall be sent to EOIR/OS, as discussed in Section VII.J.4., *supra*, using the transmittal procedures set forth in Section VII.M., Transmittal of Classified Information, *infra*.

b. Specific Guidance for Issuance of Immigration Court Decisions

EOIR/OS shall notify the Security Coordinator at the corresponding immigration court as well as the ACIJ, when the originating agency has completed the classification review of the ACIJ's decision and classified attachment, if any. The Security Coordinator at the corresponding immigration court or the ACIJ will issue a hard copy of only the unclassified ACIJ's decision and serve it on the parties. The decision will be kept in the immigration court's safe.

c. Specific Guidance for Issuance of BIA Decisions

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 will refer interested persons who are authorized to access the BIA Decision, to contact the Chief Clerk or Deputy Chief Clerk. That cover sheet will be scanned and uploaded to BIA Decisions by the Classified Case Coordinator(s) or other BIA designated personnel.

d. Specific Guidance for Issuance of OCAHO Decisions

EOIR/OS shall notify the OCAHO Security Coordinator when the originating agency has completed the classification review of the ALJ's decision and classified attachment, if any. The Security Coordinator or other cleared OCAHO personnel will issue a hard copy of only the unclassified ALJ's decision and serve it on the parties. The decision will be kept in a security container, consistent with storage of similarly classified materials in that case. The presiding ALJ may direct that the classified attachment be placed in the restricted access portion of the record, in accordance with 28 C.F.R. § 68.51.

Section X on Post-decision handling of classified materials covers storage, retention, and destruction of classified information and reproductions, return of classified materials, and archiving classified materials.

K. Interlocutory Appeals before the BIA

1. As detailed in Part III of the EOIR Policy Manual, the BIA entertains interlocutory appeals only in limited circumstances and generally involving important jurisdictional questions regarding the administration of the immigration laws or recurring questions in the handling of cases by Immigration Judges. In the event that a party seeks to file an interlocutory appeal challenging the Immigration Judge's

application of these procedures with respect to classified information, any such request for an interlocutory appeal should be limited to challenging a decision by the Immigration Judge as to whether to accept classified information or require an unclassified summary or other form of disclosure in the particular case.

2. Any challenge to the immigration court's factual findings, ultimate rulings, or consideration and/or weight of the evidence must be raised in the normal course of the administrative appeal process.

3. The filing of an interlocutory appeal will not automatically stay proceedings in immigration court.

L. Review of ALJ Interlocutory Orders before OCAHO

1. The CAHO only entertains review of interlocutory orders issued by OCAHO ALJs in limited circumstances—specifically, only where "the order concerns an important question of law on which there is a substantial difference of opinion" *and* "an immediate appeal will advance the ultimate termination of the proceeding or . . . subsequent review will be an inadequate remedy." 28 C.F.R. § 68.53(a). If a party seeks CAHO review of an interlocutory order challenging the ALJ's application of OCAHO procedures with respect to classified information, any such request for interlocutory review should explain why the review meets the regulatory criteria outlined above.

2. A party must file notice of any such request for review of an interlocutory order relating to classified information with the CAHO within 10 days of the date of entry of the interlocutory order. 28 C.F.R. § 68.53(a)(2).

3. Filing a request for review of an interlocutory order will not automatically stay the proceeding before the ALJ unless the ALJ or the CAHO determines that the circumstances require a stay. 28 C.F.R. § 68.53(b).

M. Transmittal of Classified Information

The following transmittal procedures in subsections N and O must be followed any time classified information must be sent to another location. In each 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.

N. Confidential or Secret Information

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

court to receive the information.[15] The adjudicating component's Security Coordinator, Classified Case Coordinator(s), or other designated personnel shall then notify the receiving component or entity, in advance, that the classified information will be transmitted.

2. Classified information categorized as Secret or Confidential shall be enclosed in two opaque layers before physical transmission. 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 the United States Postal Service (USPS) via Registered Mail, Return Receipt Requested, or by USPS Express Mail, Return Receipt Requested, or through FedEx. Packages must be hand-carried to the Post Office or to the FedEx location by the adjudicating component's Security Coordinator, Classified Case Coordinator(s), or other designated EOIR 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 intended destination.

4. When a package containing classified information is sent between adjudicating components, the adjudicating component's Security Coordinator, Classified Case Coordinator(s), or other designated personnel shall notify the individual to whom it is addressed of the estimated date of arrival and include the tracking number.

O. 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 adjudicating component 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 sending adjudicating component must contact EOIR/OS for assistance in making special arrangements for the transport of any material containing Top Secret information or SCI to the intended recipient.[16]

P. Certification of Records

1. The BIA may be requested to certify a case record originating from the immigration court containing classified information. If the BIA does not have the ROPs, the ROPs will need to be obtained from the immigration court, and

[15] In the case of an appeal to the BIA, the Court Administrator shall then notify the BIA's Security Coordinator or Classified Case Coordinator at the Office of the Clerk, in advance that the classified information will be transmitted.

[16] SCI must be stored in a SCIF.

the procedures for receipt of classified materials in Section V.C., 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 alien 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 connection 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

      i. The certification request is initially received by the BIA's Clerk's Office. Thereafter, the Classified Case Coordinator(s) or other designated BIA personnel takes responsibility over processing the certification request.

      ii. 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 alien'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 classified information are subject to the same controls as the original information. *See supra* Section VI.C., Reproduction Security.

   c. Transmittal of Certified Copies

      i. The same wrapping procedures addressed in Section VII.M., 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.

ii. 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 must notify OIL that the certified classified copy is, or copies are, en route to ensure that the package is received.

Q. Certification of Records by OCAHO

1. OCAHO may be requested to provide a certified copy of a case record for a case that involves classified information. Requests to provide a certified copy of a case record are generally the result of a party filing a petition for review with a United States Circuit Court of Appeals. In those cases, OCAHO processes a request for a certified copy of the case record in cooperation with either OIL or the Appellate Staff of the Civil Division of the Department of Justice.

2. The request for a certified copy of the record is typically received by either the Court Clerk or the Chief Case Management Staff. If the request is for a certified copy of the record for a case involving classified information, the Deputy CAHO or other designated OCAHO personnel takes responsibility over processing the request.

3. Prior to processing a request for a certified copy of the record, the Deputy CAHO or other designated OCAHO personnel must obtain the following: (i) the docket number of the federal court proceedings; (ii) number of certified copies requested; (iii) date certified copies are due to OIL, the Civil Division, or the Court of Appeals; and (iv) the name(s) and telephone number(s) of the individual(s) at OIL or the Civil Division to whom the certified copy of the record is to be transmitted. EOIR/OS should be contacted to verify that the individual(s) at OIL or the Civil Division have the appropriate security clearance.

4. Review and preparation of a certified copy of the record for a case containing classified information must take place in a private room. Copies of classified information are subject to the same controls as the original information.

5. When transmitting certified copies of a record containing classified information, the same wrapping procedures addressed in Section VII.M., Transmittal of Classified Information, *supra*, 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 or the Civil Division (as appropriate) 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 copy by a designated classified courier.

6. The Deputy CAHO or other designated OCAHO personnel must notify OIL or the Civil Division (as appropriate) that the certified classified copy is en route to ensure that the package is received.

VIII. Processing Formerly Classified Cases No Longer Involving Classified Information - BIA

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 must 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(s). This report shall be part of the BIA's permanent record keeping but must not include any classified information.

B. Receipt of Notice of Appeal or Motion

The Notice of Appeal or motion on a formerly classified case is initially received by the Clerk's Office. Thereafter, the Classified Case Coordinator or other designated BIA personnel takes 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) shall 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 is 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) advises the BIA's Security Coordinator(s) immediately, and the case is 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 Judge(s) 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.

IX. Classified Information From a Source Other Than an Originating Agency

The adjudicating components may receive a case that has classified information obtained by the alien (or, in OCAHO cases, any party), possibly through publicly available sources.

Classified information obtained from a source other than an originating agency can appear in the ROP, eROP, or OCAHO case file 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.

As noted above in Section V.B., Safeguarding Classified Information, all EOIR 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 EOIR personnel from their obligation to treat the information as classified when it comes into the custody of EOIR.

A. Steps to Take if Information is Found or Suspected

1. If EOIR 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 Security Coordinator, Classified Case Coordinator(s), or other designated personnel. EOIR/OS should be contacted if the Security Coordinator, Classified Case Coordinator(s), or other designated personnel are not available.

    d. Keep a written record of the handling of the material since it came into EOIR personnel custody (*e.g.*, how EOIR personnel came upon it, what steps were taken to secure and notify, the appropriate personnel, and the time and date of each step). The material must not be forwarded via email, including to a supervisor, the Security Coordinator, Classified Case Coordinator(s), and/or designated SLA(s).

2. Unless labelled as such, EOIR-issued laptops and computers are not approved 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

If EOIR personnel who are permissibly working on a case at home discover, or believe 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.J.3., Marking or Labeling the Classified Attachment of an EOIR 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 respective 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 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.

X. Post-Decision Handling of Classified Materials

A. Return of Classified Materials

At the conclusion of the proceedings before the immigration courts and the BIA, its corresponding Security Coordinator, will arrange for the ROP to be returned to the immigration court (or DHS if the case is a 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 must not be released to the parties but must remain with EOIR, consistent with the procedures outlined with this section. Classified decisions or filings should be retained in appropriate storage in a security container until archived. Audio of classified hearings should likewise be stored pursuant to the procedures set forth herein until archived. *See supra* Section V.B., Safeguarding Classified Information. The designated Security Personnel, as described *supra* in Section III, 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 adjudicator 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. Archiving ROPs before the immigration court and the BIA is the responsibility of the immigration court, or DHS if the case is in visa petition, advance permission, or fine proceedings.[17] Archiving OCAHO case files is the responsibility of OCAHO.

2. The form used by the adjudicating component 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 is required to transport the materials. The Central Security Coordinator must maintain a record of archived classified filings in EOIR proceedings.

3. Records containing Top Secret information must be transported from the adjudicating component to the Federal Records Center by the Defense Courier Service.

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

XI. Implementation and Training

A. Implementation

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

Within 45 days of the issuance of this policy, all EOIR personnel in the adjudicating components shall certify to component leadership that they have received and familiarized themselves with this memorandum.

On an ongoing basis thereafter, all newly onboarded personnel in the adjudicating components will certify receipt and familiarization with this memorandum within 45 days of onboarding.

Within 90 days of the issuance of this policy, EOIR's Security Coordinator(s), shall certify to adjudicating component leadership that they have undertaken a review of the existing practices and physical infrastructure within their purview and shall consult with the Central Security Coordinator to resolve questions regarding processes or adjustments that will be necessary to ensure that the procedures set forth herein are properly implemented and followed.

B. Training

Within 90 days of the issuance of this policy, the adjudicating components will work with the Central Security Coordinator to conduct training(s), and certify attendance, for all cleared EOIR personnel on the procedures set forth herein. Going forward, the Central Security Coordinator shall conduct such training(s) for all cleared EOIR personnel on an annual basis.

XII. Conclusion

This PM is not intended to, does not, and may not be relied upon 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. Nothing herein should be construed as mandating a particular outcome in any specific case. Nothing in this PM limits an adjudicator's independent judgment and discretion in adjudicating cases or an adjudicator's authority under applicable law.

Please contact your supervisor or EOIR/OS if you have any questions.