Operating Policies and Procedures Memorandum 24-01: Classified Information in Immigration Court Proceedings

U.S. Department of Justice

Executive Office for Immigration Review

Office of the Chief Immigration Judge

MEMORANDUM

TO:

All Assistant Chief Immigration Judges

All Immigration Judges

All Court Administrators

All Attorney Advisors and Judicial Law Clerks

All Immigration Court Staff

FROM:

Sheila McNulty

Chief Immigration Judge

DATE:

June 18, 2024

RECISSION:

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

SUBJECT:

Operating Policies and Procedures Memorandum 24-01: *Classified Information in Immigration Court Proceedings*

I. Introduction and Scope

This Operating Policies and Procedures Memorandum (OPPM) provides directives on the proper handling of classified information in immigration court proceedings and within the immigration courts. This OPPM supersedes OPPM 09-01, Classified Information in Immigration Court Proceedings, dated February 5, 2009, which is hereby rescinded.

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

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

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

II. Definitions

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

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

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

2. Secret: The unauthorized disclosure of the information "reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe"; and

3. Confidential: The unauthorized disclosure of the information "reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe."

E.O. 13526 § 1.2 (emphasis added).

Sensitive Compartmented Information (SCI) refers to a subset of classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled pursuant to formal access control systems established by the Director of National Intelligence. See Intelligence Community Directive 703 (2013). Because of the procedures that apply to the handling of SCI, OCIJ personnel must contact the Central Security Coordinator (see infra Section III.A) immediately if a party notices the intent to use SCI or if OCIJ personnel otherwise learn that a proceeding may involve SCI. The Central Security Coordinator is responsible for coordinating with DOJ Security and Emergency Planning Staff (SEPS) to ensure that SCI is properly handled, including with respect to transport and storage in a Sensitive Compartmented Information Facility (SCIF), in accordance with the relevant access control procedures applicable to the particular SCI and in consultation with the agency from which the SCI originated. Upon notification that SCI will be introduced for a case or hearing, the Central Security Coordinator will work with SEPS to ensure that all personnel required for the case are properly cleared and read into the appropriate SCI compartment, and to designate a SCIF location for those personnel to review/process the material. The Central Security Coordinator will also work with the agency submitting the SCI to ensure that the court personnel receiving the material is cleared to do so.

III. Security Personnel

A. Central Security Coordinator

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

2. Each Court Administrator, who serves as the Security Coordinator at their particular court (see infra Section III.B), will report to and receive guidance from the Central Security Coordinator.

3. The Central Security Coordinator must maintain Top Secret//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 OCIJ 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 that necessary equipment and technology are allotted and provided to EOIR personnel to properly process and safeguard classified information; and (5) coordinating annual trainings for all EOIR personnel on these procedures.

B. Security Coordinator

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 for each court 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 that court 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, 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 secure container approved by the General Services Administration (GSA) or in a secure open storage area (also called a "secure room"), as set forth below in Section V.B, Safeguarding Classified Information.

7. 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 court, including to assist with ensuring that the proper "Secure Access Status" identifier is entered into the Case Access System for EOIR (CASE). This is necessary in part 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, designated additional OCIJ personnel are available to assist in implementing the appropriate security procedures.

IV. Access to Classified Information

All supervisory judges (Chief Immigration Judge, Deputy Chief Immigration Judges, and ACIJs) and Court Administrators must have TS//SCI clearances. When OCIJ personnel have a need to access classified information in connection with their duties, EOIR/OS must confirm that the OCIJ personnel possesses the requisite clearance level for accessing the information. EOIR/OS, and not OCIJ personnel, is responsible for assessing and determining whether any particular OCIJ personnel is authorized to access classified information, before the OCIJ personnel is permitted to access the information.

A. Requirements for Access to Classified Information

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

a. Possesses the requisite level of security clearance;

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

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

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

3. OCIJ personnel must possess the requisite security clearance before accessing classified information. Requests for security clearances for OCIJ personnel must be made by EOIR/OS, in consultation with the relevant ACIJ, Regional Deputy Chief Immigration Judge, and the Chief Immigration Judge. The OCIJ personnel requiring the security clearance must not submit a request for the security clearance on their own behalf. EOIR/OS will notify the individual requiring the clearance if/when the clearance (Top Secret, Secret, or Confidential) has been granted.

4. EOIR/OS will provide each OCIJ personnel member who is granted a security clearance with (a) a set of guidance/training materials concerning the proper handling and protection of classified information in accordance with these procedures, and (b) a security briefing regarding such procedures. The recipient of the security clearance must receive this briefing from EOIR/OS prior to accessing classified information and on an annual basis thereafter. The briefing may be conducted by EOIR/OS personnel. Contact EOIR/OS if you need additional copies of any information in the security clearance packet.

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 Regional Deputy Chief Immigration Judge may temporarily reassign OCIJ personnel with the requisite clearance from another court location to assist with the handling of that case.

B. Responsibilities to Ensure the Safeguarding of Classified Information

1. Disclosure to OCIJ Personnel

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

b. Court Administrators, ACIJs, and appropriately cleared OCIJ personnel with access to classified information used in a particular case may disclose such information to other OCIJ 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. Confirmation that OCIJ personnel have the requisite security clearance and non-disclosure agreement can be requested from EOIR/OS by the Court Administrator or ACIJ. Because appropriately cleared OCIJ personnel are considered authorized clearance holders, Court Administrators, after consultation with the Central Security Coordinator, are not required to obtain further certification or authorization prior to disclosing classified information to OCIJ personnel so long as the personnel meet the requirements specified above.

2. Disclosure to Persons Outside OCIJ

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

b. OCIJ personnel do not have the authority to disclose any such classified information, including the existence thereof, to any person except for other OCIJ personnel pursuant to Section IV.B.1 above. However, transmitting records including classified information to the BIA for appeal purposes is permitted. See infra Section VIII. The ability of OCIJ personnel to authorize any disclosure of such classified information to persons outside EOIR rests with the originating agency pursuant to Section VII.C.

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, OCIJ 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, OCIJ personnel are not permitted to access information marked or labeled classified, including any such information from publicly available sources. OCIJ 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.D.3, Security Procedures, Media) must immediately contact EOIR/OIT and provide notification to EOIR/OS.

V. Custody and Storage of Classified Materials

A. Materials Covered

The security procedures set forth below for storing classified information are media neutral and apply to all papers, documents, and other materials — whether in hard copy or electronic form — that contain classified information and are in the custody of the court (e.g., motions, pleadings, briefs, notes, transcripts, and audio recordings of in camera proceedings, among other materials).

B. Safeguarding Classified Information

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

2. Documents or other materials containing classified information must never be uploaded into the EOIR Courts and Appeals System (ECAS), i.e., materials containing classified information must never be saved in any electronic Record of Proceeding (eROP). 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 Record of Proceeding (ROP), i.e., the case file must be converted from electronic to hard copy. Any existing unclassified documents contained in the eROP must be printed, a paper ROP must be constructed, and the eROP must be deactivated. The parties must be notified through a 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. 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.

3. All classified materials in the custody of the court shall be stored in a GSA-approved security container (i.e., safe) or open storage area (i.e., secure room). The combinations to security containers are classified at the same level as the highest level of classified material stored within the container. Combinations to security containers shall be changed by the Court Administrator to convert the factory pre-set combination if and when the combination has been subject to possible compromise or an individual knowing the combination no longer requires access to the security container. After consultation with the Central Security Coordinator, the Court Administrator may provide the combination for a security container to other OCIJ personnel who possess the requisite security clearance, has signed a non-disclosure agreement, has a need-to-know, and requires access to the container. The Court Administrator must inform the Central Security Coordinator whenever there is a change in OCIJ personnel and an individual no longer requires access to a particular security container combination. The Court Administrator must also inform EOIR/OS whenever there is a change in combination.

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 alien or A number for the noncitizen involved in the case. Unclassified materials must not be stored in these security containers.

5. Classified material must be kept in secure facilities as set forth above and must never be taken out of such facilities unless the material is being returned to the filing party or originating agency, sent to the BIA, or archived. See also infra Section VIII, Transmittal of Classified Information. 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.

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

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

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

VI. Security Procedures

A. Oral Discussions

Any discussions regarding classified information must be conducted in an area or room that affords sufficient security against unauthorized disclosure. Windows should be equipped with blinds, drapes, or other coverings to prevent observation by unauthorized persons. In addition, appropriate measures should be taken to minimize sound leaving the area (e.g., sound insulation, white noise systems, etc.). The classified information must not be able to be overheard or seen by any person not authorized to access the information. Portable electronic devices (e.g., smart watches, fitness trackers, laptops, mobile devices, and removable media CD-R for music) are not permitted in any room where classified information may be discussed. 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. If a Court must reproduce or copy any document involving classified information, they may only use a copier that is approved by EOIR's Chief IT Security Officer in consultation with EOIR/OS. The Court Administrator must contact the Central Security Coordinator for specific instructions. Under no circumstances may network copiers be used to reproduce classified information.

2. Copying or other reproduction of classified material is permitted only to the minimum extent required for the court's operational needs. Copies of classified information are subject to the same controls as the original information. 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. See also infra Section IX, Post-Decision Handling of Classified Documents.

3. Reproduction of classified information may only be performed by persons authorized to access the classified information in accordance with these procedures. Before making copies, such authorized personnel shall ensure that any persons not authorized to access the classified information cannot view or otherwise access the information during reproduction. As such, copiers used for the reproduction of classified information must be located in a private space or secure room to reduce the possibility of unauthorized disclosure.

D. Computer Security

1. Generally

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

2. Approved Laptop Computers Must Be Used

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

b. When a 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, should request an approved laptop computer from EOIR/OS 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 EOIR/OS and stored pursuant to the same security procedures set forth herein applicable to the laptop. See also infra Section VI.D.3, Security Procedures, Media.

c. The approved laptop must be kept within the authorized user's control at all times, must never be taken outside of the court 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.

d. Computer equipment approved for processing classified information must be used in a space in the court premises where access can be limited and processing can be accomplished without being observed or monitored by persons who are not authorized to view or otherwise access the classified information. While using an approved laptop or other computer equipment authorized for processing classified information, the authorized user must be mindful of their surroundings to guard against unauthorized disclosure.

e. Depending on the type of facility where the court 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 EOIR/OS for use at a court for processing classified information, the Central Security Coordinator must consult with the Court Administrator and/or ACIJ for that court regarding the potential need for, and implementation of, any such additional safeguards.

f. Once the court no longer requires use of the approved laptop computer for the designated case(s), the Court Administrator must ensure that the computer is returned to EOIR/OS. 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 VIII, Transmittal of Classified Information.

3. Media

a. Classified information may be stored, in addition to hard copy form, on portable media such as CDs and mobile drives (e.g., thumb drives, flash drives, and portable hard drives). Any such portable storage media must either be (i) provided directly by the

filing party already containing the classified information or (ii) obtained by the court from and approved by EOIR/OS and EOIR/OIT for the storage of classified information. The exterior of any such media must be clearly labeled with the appropriate classification markings according to the highest level of classified information contained on the media. Any such portable media approved for use by EOIR must be used to store classified information only up to the classification level for which the device is approved. Any such media containing classified information must be stored according to the security procedures set forth above.

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

4. Printers

Any document containing classified information must be printed, to the extent necessary for the court's operations, only on a printer that has been approved by EOIR's Chief IT Security Officer, in consultation with EOIR/OS, for the printing of classified information. If OCIJ personnel believes that the printing of classified information is required, please contact the Central Security Coordinator, who will coordinate the provision of an approved printer if necessary and provide instructions regarding the marking, storage, and any transmittal of such printed materials.

VII. Procedures for Cases Involving Classified Information

A. Notice That Case May Involve Classified Information

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

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

3. Upon receipt of such a notice, the Court Administrator shall promptly notify the relevant ACIJ and EOIR/OS that the case in question may involve classified information. The matter shall then be reassigned for adjudication to the ACIJ. DHS, through the Interactive Scheduling System, also may schedule such a matter directly to an ACIJ's docket. Matters docketed with the ACIJ must generally be resolved by the ACIJ within 60 days where possible consistent with due process.

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

B. Protective Orders

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

C. In Camera, Ex Parte Review of Classified Information

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

2. As set forth above, OCIJ personnel do not have the authority to (a) 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 noncitizen as specifically provided for in these procedures pursuant to Sections VII.D.3-4 below; or (b) disclose classified information used in a case to individuals other than appropriately authorized EOIR personnel. See supra Section IV.B. The authority to permit any such disclosure of the existence or substance of classified information to other parties, including the noncitizen and their representative, rests with the originating agency, and no such disclosure shall be made without the written authorization of the originating agency.

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

4. Consistent with the foregoing, the immigration court's review of all classified information submitted by DHS shall be in camera and ex parte, and the court may not order or compel the disclosure of classified information to a noncitizen or their representative. See generally 8 U.S.C. § 1229a(b)(4)(B) (noncitizen in removal proceedings has rights including to be represented

by counsel, examine the evidence against the noncitizen, and present evidence on the noncitizen's behalf, "but these rights shall not entitle the alien to examine such national security information as the Government may proffer in opposition to the alien's admission to the United States or to an application by the alien for discretionary relief under this chapter"). In the event that the originating agency authorizes any further disclosure of classified information, the originating agency's written certification (in redacted form as necessary) must be made part of the record of the case prior to the disclosure of any classified information to any noncitizen or their representative.

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

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

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

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

3. When a noncitizen is requesting asylum or withholding of removal and the court receives classified information that the court determines is relevant to the proceeding, the court shall inform the noncitizen that classified information has been received. See 8 C.F.R. §§ 1240.11(c)(3)(iv) (applications for asylum and withholding of removal in removal proceedings), 1240.33(c) (applications for asylum and withholding of deportation in exclusion proceedings), 1240.49(c) (applications for asylum and withholding of deportation in deportation proceedings). The court may notify the noncitizen on the record at a hearing or send written notification to the noncitizen, informing the noncitizen that classified information is being received into evidence. DHS, in coordination with the originating agency and EOIR/OS, may provide the noncitizen with an unclassified summary of the classified information, but is not required to do so. The court shall not order DHS or the originating agency to provide an unclassified summary to the noncitizen, or to provide the court, noncitizen, or noncitizen's representative with the basis for any decision not to supply such an unclassified summary.

4. When DHS submits classified information in adjustment of status cases, in addition to notifying the noncitizen of the receipt of classified evidence consistent with the preceding paragraph, the court should — whenever the court believes that the court can do so while safeguarding both the classified information and its source — inform the noncitizen of the general nature of the information so that the noncitizen 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 noncitizen of the general nature of the information, the court must consult with DHS in camera, ex parte, in coordination with EOIR/OS, to ensure that the general summary to be provided to the noncitizen does not contain or risk revealing classified information. Any proposed draft summary must be treated as presumptively classified until it undergoes review and clearance by the originating agency. If DHS, the originating agency, or EOIR/OS determines that a general summary cannot be provided without containing or risking the disclosure of classified information, the court shall not provide any such summary to the noncitizen. The court must defer to the determinations of DHS, the originating agency, and EOIR/OS on these issues.

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

E. Custody and Bond Proceedings

1. A custody or bond proceeding 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 audio record 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 EOIR/OS and EOIR/OIT 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 Conference

a. Any party 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, or on its own motion, the court 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 court 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 court 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 Proceeding

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

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

c. The court should schedule the in camera, ex parte hearing involving classified information for a different time or date than the remainder of the hearing in the case, to ensure that the noncitizen is able to be present for all but the portion of the proceedings involving classified information. The court may schedule the in camera, ex parte hearing to a different date, rather than different time, if doing so is necessary so that the noncitizen is able to be present for all but the portion of the proceedings involving classified information.

d. When conducting an in camera, ex parte proceeding involving classified information, the court 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, through the Court Administrator, 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, and clearing adjacent rooms if walls are not soundproof.

e. Both prior to and following any such in camera, ex parte hearing, the noncitizen and the noncitizen's representative should be allowed to present any evidence that they believe may be relevant to the hearing for the court's consideration.

f. At the close of an in camera, ex parte proceeding 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 court pursuant to the security procedures for the storage of classified materials set forth herein. The recording, transcript, and any other record of such an in camera, ex parte proceeding involving classified information must be maintained in the classified portion of the case's paper ROP or an approved laptop or storage device and never uploaded to an eROP or DAR, and shall not be disclosed or otherwise made available publicly.

3. Testimony

a. OCIJ will not use DAR technology that is connected to EOIR's network to record hearings involving classified information. Rather, a laptop computer equipped with DAR technology, which has been approved by EOIR/OS and EOIR/OIT for processing classified information, shall be used to record any hearing involving classified information. Whenever classified testimony is taken and the proceeding is recorded, the recording must be saved on the approved laptop's hard drive or a portable storage device that has been approved for use by EOIR/OS and EOIR/OIT.

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

4. Other Evidence

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

5. Note-Taking

If court personnel deem it necessary to take notes at a classified hearing, any such notes shall be considered part of the court's "working papers" — not part of the record of the case available to the parties — and the notes must be:

(a) dated to reflect when they were created;

(b) marked with the highest classification level of information discussed at the hearing;

(c) maintained in a GSA-approved security container or secure 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 court.

G. Decisions by the Immigration Court

1. When a court determines that it will render a decision referencing classified information, the court must issue the decision in written (not oral) form.

2. If the court determines that it is necessary to include classified information in a decision, the portion of the decision containing classified information must be prepared as a separate attachment so that the remainder of the decision may be released to the noncitizen and their lawyer. The court 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. Conspicuously place the overall classification at the top and bottom of each page. When using a computer, these markings can be entered as headers and footers.

c. Portion markings: Each header and paragraph shall be marked to show the highest level of classified information contained in that portion. Indicate the classification level immediately preceding the portion to which it applies: (TS) for Top Secret; (S) for Secret; (C) for Confidential; or (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 underlying classified source material.

e. "Declassify on" line: The information on this line, which should appear on the first page of the document, is obtained from the underlying classified source material.

3. Prior to releasing the decision, the decision and the classified attachment shall be sent to EOIR/OS using the transmittal procedures set forth in Section VIII below. EOIR/OS will then forward the documents to DOJ's National Security Division, which will in turn transmit the documents to the originating agency for purposes of conducting a classification review in order to ensure that no classified information is disclosed in the decision and that all classified information in the attachment has been marked correctly. The court's decision shall not be affected by the originating agency review. Rather, the role of the originating agency is strictly to ensure that the classified information is correctly marked and to provide a redacted version of the court's decision.

4. The entire decision, including the 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 pursuant to the procedures set forth above. Designated OCIJ personnel will issue a hard copy of only the non-classified decision and serve it on the parties.

H. Interlocutory Appeals

1. The BIA only entertains interlocutory appeals in limited circumstances, generally involving important jurisdictional questions regarding the administration of the immigration laws or recurring questions in the handling of cases by immigration judges. See BIA Practice Manual § 4.14(c). In the event that a party seeks to file an interlocutory appeal challenging the court'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 court as to whether to accept classified information or require an unclassified summary or other form of disclosure in the particular case.

2. A party must file notice of any such interlocutory appeal relating to classified information with the BIA within 30 days of the decision that the party seeks to appeal.

3. Any challenge to the court's consideration or weighing of the evidence, factual findings, or ultimate rulings must be raised in the normal course of the administrative appeal process.

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

VIII. Transmittal of Classified Information

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

A. Confidential or Secret Information

1. The Court Administrator, as the Security Coordinator, 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) to receive the information.

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

3. This double-wrapped package must be transmitted by 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 Court Administrator or other appropriately cleared OCIJ 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 BIA.

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

B. Top Secret Information and SCI

Any record containing Top Secret information or SCI cannot be mailed or sent by commercial carrier and must be hand-carried in an approved courier pouch. This package then must be hand-carried from the court 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 court must contact EOIR/OS for assistance in making special arrangements for the transport of any material containing Top Secret information or SCI to the BIA. Alternatively, the court storing the information, or the originating agency, may make the information available for review at their premises by the BIA.

IX. Post-Decision Handling of Classified Materials

A. Return of Classified Materials

The filed classified documents may only be returned to the filing party upon request and after consultation with the Central Security Coordinator. This must occur no later than 30 days after all proceedings in the case have concluded, including the resolution of any appeals and federal court challenges or the expiration of the period for filing any such appeals. Classified decisions or attachments will not be released to the parties but will remain with EOIR consistent with this section. Classified decisions or filings should be retained in appropriate storage in a security container or secure room until archived. Audio of classified hearings should likewise be stored pursuant to the procedures set forth herein until archived. See infra Sections IX.B-C. The Court Administrator 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 identified for destruction must continue to be stored pursuant to the procedures specified herein until and unless EOIR/OS and the Agency Records Officer determine destruction is appropriate. The Agency Records Officer and EOIR/OS must be consulted prior to the destruction of any classified information.

C. Archiving Classified Evidence

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

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

D. Implementation and Training

1. Within 30 days of the issuance of this OPPM, each Court Administrator shall, in coordination with the relevant ACIJ, undertake a review of the existing practices and physical infrastructure at their court(s), and shall consult with the Central Security Coordinator regarding any adjustments to the court's practices and infrastructure that will be necessary to ensure that the procedures set forth herein are properly implemented and followed.

2. Within 30 days of the issuance of this OPPM, the Central Security Coordinator shall conduct trainings for all OCIJ personnel on the procedures set forth herein. Going forward, the Central Security Coordinator shall conduct such trainings for all OCIJ personnel on an annual basis.

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

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

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

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

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

[5] As used herein, "ex parte" refers to proceedings involving only the court and the government.

[6] 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.

[7] This memorandum 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.

Updated June 19, 2024

Executive Office for Immigration Review
5107 Leesburg Pike
Falls Church, VA 22041

Phone: 703-305-0289