EXHIBIT
46

Privacy Impact Assessment

Immigration and Customs Enforcement Operational Use of Publicly Available Information Including Social Media Information for Law Enforcement Investigations

December 15, 2023

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) U.S. Immigration and Customs Enforcement (ICE) has a statutory mission to enforce the nation's immigration laws and combat transnational crime. To achieve its mission, ICE personnel collect information from a variety of sources, including publicly available information on the internet and on social media platforms. ICE personnel use publicly available information found on the internet, including on social media platforms, in support of ICE's law enforcement mission. ICE is conducting this Privacy Impact Assessment (PIA) because some of the publicly available information that its personnel collect, maintain, or share may include personally identifiable information (PII).[1] This Privacy Impact Assessment focuses on the collection and use of publicly available information including social media information for law enforcement investigations, leaving in-depth analysis of maintenance and sharing to the respective Privacy Impact Assessments for ICE systems in which the data is ultimately stored. These systems are listed in the Appendix to this Privacy Impact Assessment.

Introduction

To fulfill its statutory mission, ICE uses a variety of sources from which it collects information related to criminal investigations and immigration enforcement matters. Accordingly, ICE may access, collect, and use information available on the internet and social media platforms,[2] including publicly available information as one of its information assets.[3] ICE maintains compliance with DHS Directive 110-01, *Privacy Policy for Operational Use of Social Media*,[4] and

[1] DHS defines "personally identifiable information" as any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the United States, or employee of or contractor to the Department. *See* DHS INSTRUCTION MANUAL 047-01-007, REVISION 3 (2017), HANDBOOK FOR SAFEGUARDING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION (PII), *available at* https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information.

[2] DHS defines "social media" as the sphere of websites, applications, and web-based tools that connect users to engage in dialogue, share information and media, collaborate, and interact. Social media takes many different forms, including but not limited to, web-based communities and hosted services, social networking sites, video and photo sharing sites, blogs, virtual worlds, social bookmarking, and other emerging technologies. The definition of "social media" does not include internal Department intranets or applications. *See* DHS LEXICON, REVISION 2 (2017), *available at* https://www.dhs.gov/publication/dhs-lexicon.

[3] DHS defines "publicly available information" as "unclassified information that has been published or broadcasted in some manner to the general public, is available to the public by subscription or purchase, could lawfully be seen or heard by a casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public." "Open source" information is a form of publicly available information and defined as "unclassified information that has been published or broadcast in some manner to the general public, could lawfully be seen or heard by a casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public." *See* DHS LEXICON, REVISION 2 (2017), *available at* https://www.dhs.gov/publication/dhs-lexicon.

[4] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY DIRECTIVE 110-01, OPERATIONAL USE OF SOCIAL MEDIA (2012), *available at* https://www.dhs.gov/privacy-policy-guidance.

its accompanying Instruction, 110-01-001.[5] These policy documents establish privacy policy and requirements for DHS and its components for the access, collection, use, maintenance, retention, disclosure, deletion, and destruction of personally identifiable information in relation to the operational use of social media. Due to the trend toward including interactive, social media-style features on "traditional" internet sites, ICE has determined DHS's Privacy Policy governs the collection of personally identifiable information online on all internet sites,[6] not only on social media platforms.

ICE may only access information online from open source sites (e.g., blogs, news sites, public record repositories) and on social media platforms that is publicly available.[7] This includes any public messages, posts, and media (e.g., photos, documents, geolocation information).[8] The ICE offices that access publicly available social media information as part of their law enforcement activities include the following:

- Office of Homeland Security Investigations (HSI): HSI is the primary investigative arm of DHS and combats criminal organizations exploiting U.S. trade, travel, financial, and immigration systems.
- Office of Professional Responsibility: The Office of Professional Responsibility is responsible for upholding ICE's professional standards through a multi-disciplinary approach of security, inspections, and investigations. The Office accomplishes its mission by investigating allegations of employee misconduct; conducting independent reviews and audits of ICE programs, offices, and detention facilities; measuring compliance with applicable policies, regulations, and laws; and administering ICE's internal security program to protect and secure people, information, and facilities.[9]

This Privacy Impact Assessment covers the following items related to ICE employee and contractor use of publicly available and social media information in law enforcement investigations:

- ICE's operational uses of publicly available online content and social media information;
- ICE's use of technology and tools that collect and analyze publicly available information including social media information;

---

[5] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY INSTRUCTION 110-01-001, OPERATIONAL USE OF SOCIAL MEDIA (2012), *available at* https://www.dhs.gov/privacy-policy-guidance.

[6] This Privacy Impact Assessment only assesses ICE's collection and use of publicly available information including social media information for law enforcement investigations. This Privacy Impact Assessment does not cover ICE undercover operations, which are governed by separate legal and privacy guidelines.

[7] *Id.*

[8] Geographic data may come from publicly shared social media information.

[9] This Privacy Impact Assessment does not address use of publicly available and social media information by ICE Office of Professional Responsibility in support of its internal security program to protect and secure people, information, and facilities.

- ICE's use of the deep and dark webs;
- ICE's policy and Rules of Behavior (ROB) for ICE personnel use of social media information;
- First Amendment and Equal Protection restrictions placed on ICE online collections;
- Select mitigation measures for the use of tools to access, collect, and/or analyze publicly available information, including social media information; and
- identification of privacy risks and steps that ICE takes to mitigate risks to personally identifiable information.

ICE's Operational Uses of Publicly Available Information, including Social Media Information

This section details how each ICE program engages with social media and how publicly available information obtained from social media or other publicly available online content is used in furtherance of ICE's law enforcement mission.

HSI Use of Publicly Available Online Content and Social Media Information

ICE HSI investigations cover a broad range of topics, including, but not limited to, national security threats, financial and smuggling violations (including illegal arms exports), financial crimes, commercial fraud, human trafficking, narcotics smuggling, child sexual abuse/exploitation, and immigration fraud. Given HSI's vast portfolio, its agents and support personnel rely on a variety of sources of information to generate leads, including information from publicly available sources and social media. Generally, HSI searches of publicly available information will have a nexus to an existing investigation; however, if the information or social media posting is indicative of a criminal violation enforceable by ICE HSI (e.g., child sexual abuse material, an online marketplace for narcotics), that information can be used to initiate an investigation. The following examples provide a comprehensive list of the ways in which HSI personnel use publicly available content and social media information. In the future, if HSI's use of such information deviates from the list below, this Privacy Impact Assessment will be updated to provide additional transparency on the new uses as well as assess any potential privacy risks and appropriate mitigation measures.

HSI uses social media and publicly available information for tactical planning activities prior to a specific law enforcement action to ensure safety of officers and other individuals at or near the scene. Any information that HSI uses in this context is documented in the Investigative Case Management system (ICM) and in the Repository for Analytics in a Virtualized Environment (RAVEn).[10] HSI also uses publicly available information, including social media

[10] *See* U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement, Privacy Impact

information, to enhance information from various government and law enforcement databases in furtherance of its law enforcement investigations.[11]

Social media searches are conducted as needed and must be associated with a specific case, operation, or mission-related purpose, such as combatting human trafficking or money laundering.

HSI may consolidate corroborated open source and social media information with information maintained in government databases and create a report that is entered into an ICE case management or lead generation system.[12] The information may then be shared within HSI for investigative action.

HSI may also conduct open source and social media research on schools as part of the certification[13] and recertification[14] compliance process of the Student Exchange and Visitor Program (SEVP).[15] For example, HSI may use publicly available information to verify a school's petition as part of the Student Exchange and Visitor Program certification, recertification, or unannounced review (e.g., following up on tips received from federal agents or the Field Representative Units). HSI does not target[16] individuals, such as school officials or students, when researching schools to determine the institutions' compliance with SEVP certification requirements.

HSI personnel also will access and use publicly available information online to verify data contained on a school's Form I-17, "Petition for Approval of School for Attendance by Nonimmigrant Student."[17] HSI will use online content, including social media information, to verify the accuracy of the school's official name and other data listed on the Form I-17, such as

---

Assessment for the Investigative Case Management System (ICM), *available at* https://www.dhs.gov/privacy-documents-ice. Any information introduced as evidence in a prosecution would be obtained directly from the social media platform via subpoena or search warrant. *See also* U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement, Privacy Impact Assessment for the Repository for Analytics in a Virtualized Environment (RAVEn), DHS/ICE/PIA-055, *available at* https://www.dhs.gov/privacy-documents-ice.

[11] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR LEADTRAC, DHS/ICE/PIA-044, and INVESTIGATIVE CASE MANAGEMENT SYSTEM (ICM), DHS/ICE/PIA-045, *available at* www.dhs/gov/privacy-documents-ice.

[12] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR LEADTRAC, DHS/ICE/PIA-044, and INVESTIGATIVE CASE MANAGEMENT SYSTEM (ICM), DHS/ICE/PIA-045, *available at* www.dhs/gov/privacy-documents-ice.

[13] The Student and Exchange Visitor Program's (SEVP) School Certification Unit certifies schools to accept F (academic) and M (vocational) visa holder students.

[14] Designated School Officials, acting on behalf of SEVP-certified institutions, must complete recertification every two years to confirm compliance with SEVP eligibility, record keeping, and recording requirements on F and/or M visa holder students at various types of schools.

[15] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE STUDENT EXCHANGE AND VISITOR PROGRAM (SEVP), DHS/ICE/PIA-001, *available at* www.dhs/gov/privacy-documents-ice.

[16] ICE SEVP does not target individuals outside of HSI's regulatory requirements to vet and conduct routine background checks on school officials/students and refer potential visa violators for further investigation.

[17] Form I-17, Petition for Approval of School for Attendance by Nonimmigrant Student, *available at* https://studyinthestates.dhs.gov/sevis-help-hub/school-records/school-certification/form-i-17-initial-certification.

the school's county, city, state, and address.

HSI may also review the school's social media homepage and school website to verify information on the Form I-17, including program(s) of instruction information (e.g., listed courses, course descriptions, schedules, graduate requirements). If HSI finds discrepancies between the information posted on the Form I-17 and what is publicly available, HSI will generate a lead to the field for further investigation.

Additionally, HSI may use publicly available information to investigate F-1 and M-1 student visa holders who are suspected of overstaying their visas or otherwise violating the terms of their admission into the United States.[18]

Further, HSI uses publicly available information, including social media information to investigate suspected illegal activity by foreign students on college campuses,[19] or other administrative issues related to a foreign student's non-immigrant status. As described above, any HSI use of social media information must have a nexus to an authorized investigation or the social media information itself be indicative of a crime enforceable by ICE HSI.

All information HSI retrieves from social media will be documented in the appropriate ICE case management or lead generation system.[20]

HSI also assists the Department of State in conducting the initial vetting of visa applicants.

ICE Office of Professional Responsibility Use of Publicly Available Online Content and Social Media Information

The ICE Office of Professional Responsibility will complement its investigations of allegations of criminal violations or misconduct by ICE personnel with publicly available information. ICE Office of Professional Responsibility will review publicly available postings on the social media accounts associated with ICE employees under investigation to further investigate any claims of criminal or administrative misconduct submitted to the Office by the public or other ICE employees. ICE Office of Professional Responsibility collects any information relevant to the investigation, documenting it in the Office's case management system, the Joint Integrity Case

---

[18] *See* U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement, Privacy Impact Assessment for LeadTrac, DHS/ICE/PIA-044, and U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement, Privacy Impact Assessment for Student and Exchange Visitor Program (SEVP), DHS/ICE/PIA-001, *available at* www.dhs/gov/privacy-documents-ice.

[19] For example, foreign students suspected of stealing intellectual property to provide to their home countries.

[20] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE INVESTIGATIVE CASE MANAGEMENT SYSTEM (ICM), *available at* https://www.dhs.gov/privacy-documents-ice. Any information introduced as evidence in a prosecution would be obtained directly from the social media platform via subpoena or search warrant. *See also* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, PRIVACY IMPACT ASSESSMENT FOR THE REPOSITORY FOR ANALYTICS IN A VIRTUALIZED ENVIRONMENT (RAVEn), DHS/ICE/PIA-055, *available at* https://www.dhs.gov/privacy-documents-ice.

Management System (JICMS).[21]

ICE Use of Technology and Tools that Collect and Analyze Publicly Available Information Including Social Media Information

ICE uses commercial databases and analytical products to help search, monitor, and process publicly available data from online, public records data sources, and social media platforms pursuant to ongoing investigations. ICE offices and programs may use one or a combination of tools to accomplish their mission. Prior to its use of any technology or tool that accesses, collects, and/or uses personally identifiable information, an ICE program must submit a Privacy Threshold Analysis (PTA) to ICE Privacy to assess the technology or tool's impacts on individual privacy. All Privacy Threshold Analyses must be submitted to and approved by the DHS Privacy Office. All personnel who use a technology or tool must be trained on the appropriate uses of that instrument. The following is a description of the tools that ICE uses to achieve its statutory mission using publicly available information. Each tool may raise unique privacy risks, which are assessed using the Fair Information Practice Principles as discussed later in this Privacy Impact Assessment.

Analytical Search Engines and Data Aggregators

ICE also uses tools that collect and compile information from multiple publicly available sources across the internet in support of open law enforcement investigations. These aggregator tools retrieve data from credit bureaus, government public records, news sites, and other publicly available information resources. The data the aggregator retrieves is available to the public, either through internet searches or purchase. Data aggregators present data from search queries in a format that is meaningful or useful to the user. Data aggregators used by ICE are specifically designed to search public records and publicly available social media information, filter duplicate information, and present returned information in a manner that is useful to ICE personnel and directly related to an ICE investigation.[22]

ICE users will access data aggregator tools via a web portal and enter the search terms directly related to a person of interest (e.g., fugitive, suspect).[23]

Link Analysis Applications

Link analysis applications capture digital connections. ICE may use link analysis

[21] The Joint Integrity Case Management System (JICMS) is owned by U.S. Customs and Border Protection and is used by ICE. For more information, *see* U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. CUSTOMS AND BORDER PROTECTION, PRIVACY IMPACT ASSESSMENT FOR THE JOINT INTEGRITY CASE MANAGEMENT SYSTEM (JICMS), DHS/CBP/PIA-044, *available at* www.dhs.gov/privacy-documents-cbp.

[22] ICE is prohibited from using data aggregators or other tools to access, collect, or use data that ICE is otherwise prohibited from accessing, collecting, or using.

[23] Persons Of Interest (POI) may include individuals who are reasonably suspected of a crime, are the subject of investigative interest based on the individuals' association with illegal cross-border activity or another criminal network, such as terrorist groups, are wanted in connection with a crime (e.g., arrest warrant), or for whom there is investigative evidence linking the individual to criminal acts within ICE's mission to enforce (e.g., bombing).

applications in support of open investigations. These applications aggregate connected online accounts and social media data to assist investigators with identifying possible connections to an investigation. This is also known as "link analysis." Link analysis helps investigators identify and assess suspected criminal networks by detecting similarities.[24]

The data must be reviewed by an ICE investigator, who is required to assess the information and corroborate it before it can be used in an investigation.

Automated Collection Tools

ICE may use automated applications or tools that collect information from publicly available websites and chatrooms identified as relevant to ICE investigations. This process, sometimes referred to as "scraping" is an automated process that copies and collects website data that has been pre-designated by a user as related to an investigation, on a recurrent basis, then loads the copied data into a database for later analysis and use.

ICE personnel will use all available and relevant information such as witness statements, investigative reports, and other documentary evidence, to assess the accuracy and authenticity. ICE is not permitted to collect entire websites or information unrelated to an investigation. The site selection must be submitted to an ICE supervisor for approval before it can be subject to an automated collection tool.

The ICE supervisor must verify that the website or chatroom contains relevant and credible evidence of suspected violations within ICE's statutory law enforcement mission and that the parameters of collection are narrowly tailored to collect only that information directly relevant to a law enforcement investigation. As noted, collection and analysis is only permitted on subjects and information determined to be relevant to and within the scope of an investigation.

Automated collection tools do not modify data in any way. All collection by the tool is passive. These tools do not violate or circumvent privacy settings and protections placed on the information by a website or chatroom. These tools do not "friend" or "follow" social media accounts, may not post content on social media websites, and may not prompt the collection of information from other individuals or accounts. All collections are manually reviewed by ICE personnel for credibility and relevance to the open investigation. If data collected by these tools is deemed irrelevant, then ICE deletes the information, and it will not be stored or retained in the repository. Any information retained by ICE will be documented in the relevant case file, including the tools that were used to acquire the information and the source of the information. If at any point a site is determined to no longer be relevant to the ICE investigation for which its use was initiated,

[24] Link analysis tools also can sort, match, and link multiple open-source databases. The link analysis tool user interface platforms can provide further attribution to the subject of an authorized, ongoing investigation. HSI will use link analysis tools to identify the following information directly related to an open investigation: criminal suspects, witnesses, the location of at-large individuals, businesses, and assets of targets of investigations for potential arrest, seizure, and forfeiture. HSI can access link analysis tools through a web-based portal (username/password) and/or submit queries directly to the tools via Short Messaging Service (SMS) text.

the collection will be immediately discontinued. Similarly, if ICE becomes aware that a site may no longer present credible information, then automated collections will be discontinued immediately.

Recurrent Query Platforms/Tools

ICE uses web-based platforms/tools to recurrently query open source websites and publicly available social media accounts for information directly related to ICE investigations. A platform must only retrieve information that would be accessible to the public through basic internet searches (e.g., a web browser search); therefore, recurrent query platforms/tools may not be used to access information that requires an account (e.g., a social media profile). ICE uses the information gathered through use of the platforms/tools to generate investigative leads. Prior to the procurement or development of a query platform/tool, ICE Privacy, through the Privacy Threshold Analysis process, will confirm that the platform/tool does not violate any website or social media account's privacy settings on which the tool is intended to be used.

ICE personnel must review responsive information to determine whether it is accurate/corroborated and whether the information is relevant to an investigation. Users can select relevant information in the results that will then automatically be added to a report that can be exported from the web portal for later ingestion into an ICE system. Information not selected (because it is determined not to be relevant to the specific investigation) will be deleted from the portal by the vendor. By selecting information as relevant to an investigation, the platform search algorithms are enhanced for future searches. If a report is exported, the ICE user will re-initiate checks against government systems and again manually search for additional open source information for corroboration prior to entering information into any ICE system or generating a lead.

ICE Policy for Using Publicly Available Online Content and Social Media Information

In 2012, the then-ICE Director issued a memorandum to all ICE personnel titled "Use of Public and Non-Public Online Information"[25] outlining core principles for ICE law enforcement use of online information (hereinafter "Morton Memo"). The memorandum laid out key principles under which ICE personnel are allowed to use social media for operational purposes. ICE use of publicly available information for operational purposes must abide by the 2012 Morton Memo and DHS Privacy Policy 110-01. Key principles of the 2012 Morton Memo include the following:

- Obtaining Information from Unrestricted Sources: Law enforcement personnel may obtain information from publicly accessible online sources and facilities under the same conditions as those by which they may obtain information from other sources generally

[25] U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, POLICY GUIDANCE MEMORANDUM 100821.1 USE OF PUBLIC AND NON-PUBLIC ONLINE INFORMATION (2012), on file with ICE Privacy. This memorandum is also referred to as the "2012 Morton Memo." This memorandum is being reviewed and may be updated or superseded as needed.

open to the public. This principle applies to publicly accessible sources located in foreign jurisdictions as well as those in the United States.

- Obtaining Identifying Information about Users or Networks: Law enforcement personnel may use available software tools in their intended lawful manner under the same circumstances in which ICE guidelines and procedures permit them to look up similar identifying information (e.g., a telephone number) through non-electronic means. However, law enforcement personnel may not use software tools, including those which are generally available as standard operating system software, to circumvent restrictions placed on system users.
- Real-Time Communications: Law enforcement personnel may passively[26] observe and log real-time electronic communications open to the public under the same circumstances in which they may attend a public meeting.
- Accessing Restricted Sources: Law enforcement personnel may not access restricted online sources or facilities absent legal authority permitting entry into a private space.
- Online Communications Generally: Law enforcement personnel may use online services to communicate in the same manner as they may use other types of communication tools, such as the telephone and the mail. Law enforcement personnel should retain the contents of a stored electronic message if they would have retained that message had it been written on paper. The contents should be preserved in a manner authorized by ICE procedures governing the preservation of electronic communications.

Any update to these principles will necessitate a corresponding update to this Privacy Impact Assessment.

Additionally, ICE Privacy works with relevant ICE program offices to ensure that ICE guidance and policy remains current and consistent with the evolution of internet use in law enforcement operations. As new publicly available information programs or tools are used, procured, or developed by ICE, ICE Privacy may require more focused and tailored rules of behavior and other safeguards for ICE's uses of publicly available information. Rules of behavior are reviewed for compliance with DHS and ICE policy, including the 2012 Morton Memo. ICE Privacy, ICE Office of the Principle Legal Advisor, and the DHS Privacy Office must approve new and updated ICE rules of behavior.

First Amendment and Equal Protection restrictions

[26] As discussed in this Privacy Impact Assessment, passive observation includes a prohibition on communicating directly with an individual, eliciting websites to collect information, responding to an individual's posts, or posting content meant to elicit a response from an individual.

In 2019, the then-DHS Secretary reaffirmed that DHS personnel would observe and protect individuals' First Amendment rights, regardless of the medium through which those rights are exercised.[27] ICE, as a Component of DHS, will not collect information regarding an individual's religious beliefs; political and personal beliefs; lawful associations; or protest unless, consistent with the Privacy Act, the information is pertinent to and within the scope of an authorized criminal, civil, or administrative law enforcement activity (e.g., a crime within the scope of ICE law enforcement authorities). ICE use of social media information is directly related to an open investigation and often subject-focused, meaning that searches and collections are centered around targets of investigation or information that is, on its face, relevant to an open criminal, civil, or administrative investigation undertaken pursuant to ICE law enforcement authority (e.g., child sexual abuse material).

In addition, the Privacy Act of 1974[28] generally prohibits ICE from collecting records describing how an individual, defined as a U.S. citizen or Lawful Permanent Resident, exercises rights guaranteed by the First Amendment. There are exceptions, however, if the record is "pertinent to and within the scope of an authorized law enforcement activity," or if either a law or the individual about whom the record is maintained expressly authorizes such maintenance.[29] ICE personnel must successfully complete social media training, created by ICE Privacy in consultation with the ICE Office of the Principle Legal Advisor and the DHS Office for Civil Rights and Civil Liberties, on how to identify First Amendment activity, ensure there is a lawful basis to collect the information, and confirm the collection will be performed using the least intrusive means[30] possible to accomplish the authorized law enforcement action or activity.

DHS also prohibits the consideration of protected individual characteristics (i.e., race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, and disability) in investigation, screening, and law enforcement activities in all but the most exceptional instances. The Department of Justice "Guidance For Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, Gender Identity, and Disability" (DOJ Guidance)[31] is the policy of DHS as it applies to federal law enforcement

---

[27] *See* SECRETARY OF HOMELAND SECURITY MEMORANDUM, INFORMATION REGARDING FIRST AMENDMENT PROTECTED ACTIVITIES (2019), *available at* https://www.dhs.gov/sites/default/files/publications/info_regarding_first_amendment_protected_activities_as1_signed_05.17.2019.pdf.

[28] 5 U.S.C. § 552a.

[29] 5 U.S.C. § 552a(e)7.

[30] "Least-Intrusive-Means" doctrine refers to the requirement that ICE begin with a collection method that is less invasive for the individual, and only increasingly so if no other less invasive collection methods exist. For example, ICE requires its investigators to use information available via public internet searches.

[31] *See* U.S. Department of Homeland Security Policy Guidance Memorandum: Guidelines for Enforcement Actions In Or Near Protected Areas (2021); The Department of Homeland Security's Commitment to Nondiscriminatory Law Enforcement and Screening Activities (2013), *available at* 21_1027_opa_guidelines-enforcement-actions-in-near-protected-areas.pdf (dhs.gov). *See also* U.S. DEPARTMENT OF JUSTICE, GUIDANCE FOR FEDERAL LAW ENFORCEMENT AGENCIES REGARDING THE USE OF RACE, ETHNICITY, GENDER, NATIONAL ORIGIN, RELIGION,

personnel and federal non-law enforcement personnel engaged in or supporting federal law enforcement activity and intelligence activity conducted by Federal law enforcement agencies.[32] Consideration of race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, and disability in DHS law enforcement activities occurs only in strict accordance with DOJ Guidance.[33]

DHS personnel may use protected individual characteristics only when a compelling governmental interest is present, and only in a manner narrowly tailored to meet the compelling interest. The Department of Justice Guidance does not apply to (1) interdiction activities at the border or its functional equivalent (such as airports, seaports, and other ports of entry) and related traveler and cargo vetting activities, as well as protective and inspection activities; (2) non-law enforcement screening activities; and (3) all activities that use country of birth or nationality as a security screening, enforcement, or investigative criterion.[34] These activities remain subject to Department of Homeland Security's 2013 policy.[35]

Further, information collection supporting HSI administrative immigration enforcement activities is governed by the DHS policy "Guidelines for Enforcement Actions in or Near Protected Areas," that superseded previous ICE policy.[36] The policy discourages actions that may detrimentally affect the willingness of an individual to seek essential services, including the monitoring of social media accounts associated with protected areas. Protected areas include churches, schools, and healthcare facilities. The policy specifically constrains "immigration enforcement surveillance" at these locations. ICE personnel are required by policy to conduct enforcement actions and information gathering activities in support of an enforcement action, in such a manner as to avoid targeting these protected areas.[37]

Select Mitigation Measures for the Use of Tools to Access, Collect, and/or Analyze Publicly

---

SEXUAL ORIENTATION, GENDER IDENTITY AND DISABILITY (May 25, 2023), *available at* https://www.dhs.gov/publication/guidance-federal-law-enforcement-agencies-regarding-use-race-ethnicity-gender-national.

[32] *See* U.S. Department of Homeland Security Policy Statement 500-02 Reaffirming the Commitment to Nondiscrimination in Department of Homeland Security Activities (May 25, 2023), *available at* https://www.dhs.gov/publication/department-homeland-security-commitment-nondiscriminatory-law-enforcement-and-screening.

[33] *Id.*

[34] *Id.*

[35] *See* U.S. Department of Homeland Security Memorandum For Component Heads, the Department of Homeland Security's Commitment to Nondiscriminatory Law Enforcement and Screening Activities (April 26, 2013), *available at* https://www.dhs.gov/sites/default/files/publications/secretary-memo-race-neutrality-2013_0_1.pdf

[36] *See* U.S. DEPARTMENT OF HOMELAND SECURITY POLICY GUIDANCE MEMORANDUM: GUIDELINES FOR ENFORCEMENT ACTIONS IN OR NEAR PROTECTED AREAS (2021), *available at* https://www.dhs.gov/sites/default/files/publications/21_1027_opa_guidelines-enforcement-actions-in-near-protected-areas.pdf.

[37] *See* U.S. HOMELAND SECURITY POLICY MEMORANDUM: GUIDELINES FOR ENFORCEMENT ACTIONS IN OR NEAR PROTECTED AREAS (2021), *available at* https://www.dhs.gov/sites/default/files/publications/21_1027_opa_guidelines-enforcement-actions-in-near-protected-areas.pdf.

Available Information, Including Social Media Information

The following are additional safeguards applicable to the use of tools, known at the time of this Privacy Impact Assessment, to facilitate ICE's use of publicly available and social media information. If ICE proposes to use additional services/platforms/tools/applications in the future, it will complete required Privacy Threshold Analyses and update this Privacy Impact Assessment as appropriate.

Use of Application Programming Interfaces/"Scraping"

The use of application programming interfaces (APIs) and/or scraping can be inconsistent with a website or social media platform's terms of service. Therefore, ICE's use of tools/applications that facilitate their use could impact personal privacy. Accordingly, some mitigation measures are in place, as discussed above, for the use of these tools/applications.

The use of APIs that facilitate scraping is akin to the use of automated collection tools. Therefore, the use of scraping tools/applications must satisfy the requirements for use of automated collection tools as discussed above.

For example, users must first assess the accuracy and authenticity of the information sought for collection and then receive supervisory approval to use this tool/application. The supervisor must verify that the site or platform targeted for collection contains relevant and credible information of suspected violations related to an open investigation and that the parameters of collection only collect information directly relevant to the investigation.

ICE is not permitted to collect entire websites or information unrelated to the investigation. Further, use of these tools/applications will be in a manner that respects all privacy settings. And, if at any point a site or platform is determined to no longer be relevant to the ICE investigation for which its use was initiated, or it may no longer present credible information, the collection by the tool/application will be immediately discontinued.

Network Analysis

Network analysis tools/applications are the same as link analysis applications discussed above. Therefore, use of these tools/applications will be in a manner consistent with the parameters outlined above. Additionally, there is a privacy risk associated with analyzing a person's network, including that the individuals who are a part of that network may have no connection to the suspected individual and/or illegal activity. For example, simply liking a post, tagging or being included in a photo, or having a relationship with a suspected individual does not indicate a connection to criminal activity under investigation. To mitigate this risk, establishing parameters around perceived relationships is critical, such as limiting collection on the number of connections out from the suspected individual (i.e., "hops") and ensuring a direct connection to the person under investigation and criminal activity by the connected individual.

Supervisors will review and confirm the user's written justification. Also, supervisors will verify ICE personnel compliance with agency-wide and tool-specific training and adherence to the applicable rules of behavior. Supervisors may require additional safeguards if they identify inconsistencies or other concerns.

Keyword Queries:

Use of keyword queries by a tool/application is the same as use of recurrent query platforms/tools discussed above. Therefore, use of keyword queries in tools/applications will be in a manner consistent with the parameters outlined previously. For example, information sought through keyword queries must be directly related to an ICE investigation. Only information accessible to the public through basic internet searches can be retrieved; therefore, the keyword queries tool/application cannot be used to access information that requires an account (e.g., social media profile). Users must review responsive information to assess its accuracy and direct relevance to an open investigation. Further, users must corroborate the information before it may be used. If information is retrieved that is not directly relevant to an open investigation, then it must be deleted and the collection discontinued.

Additionally, there is a risk that using certain keywords to search an individual's publicly available information may implicate the "purpose specification" principle. Accordingly, any keywords used to query publicly available information will be designed in such a way as to not profile, target, or discriminate against any individual for lawfully exercising their First Amendment rights. Keywords will be directly relevant to the suspected criminal actions of the person of interest, specific events, or specific locations directly related to the investigation. To ensure that keyword searches are conducted in an authorized manner, keywords used to query publicly available information will be documented and subject to periodic review by the Office of the General Counsel, ICE Privacy, DHS Privacy, and the DHS Office for Civil Rights and Civil Liberties. Additionally, ICE Privacy will meet monthly with the program to assess how keywords are being used.

Vendor Limitations

There is a risk that ICE's use of vendors or contractors could implicate the "purpose specification" principle. As noted previously, ICE may not use a vendor-provided tool or application, nor may a contractor perform work on behalf of ICE, in a manner inconsistent with governing law and policy. Contractors and vendors should not collect, use, maintain, or disseminate personally identifiable information that ICE does not have the authority to collect, use, maintain, or disseminate. For example, while contractors may collect personally identifiable information related to First Amendment protected activity when operating independent of any government involvement, contractors may not collect such personally identifiable information to fulfill any obligations to the government.

Additionally, there is a risk that a vendor could have access to personally identifiable information ICE users input into the tools/applications and ICE sensitive law enforcement activities. Accordingly, while vendors will retain administrative functions within a tool/application, ICE will maintain control of all use restriction and auditing capabilities, unless any additional functions assigned to the vendor are detailed in the contract or agreement and are performed under general ICE direction. Additionally, the vendor may not use personally identifiable information input into the tool/application by an ICE user to further refine and/or train the tool or its model(s).

Other tools/applications

The platforms or tools that ICE uses on publicly available information, including social media information, for investigations may include other applications or functions that are not permitted for use at this time. For example, ICE may not use emotional or sentiment analysis tools/applications, "risk profile," facial recognition, or reverse image searching tools in this context. If in the future ICE wishes to reevaluate the tools it uses in this context, it will coordinate with the DHS Privacy Office and the Office for Civil Rights and Civil Liberties to assess the proposed tool's efficacy and assess any related potential privacy, civil rights, and civil liberties risks.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[38] articulates concepts of how the Federal government should treat individuals and their information and imposes duties upon Federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.[39]

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.[40] The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002 Section 208 and the Homeland Security Act of 2002 Section 222.[41] Because ICE use of publicly available and social media information is not

[38] 5 U.S.C. § 552a.
[39] 6 U.S.C. § 142(a)(2).
[40] U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY GUIDANCE MEMORANDUM 2008-01/PRIVACY POLICY DIRECTIVE 140-06, THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (2008), *available at* https://www.dhs.gov/privacy-policy-guidance.
[41] 6 U.S.C. § 142.

an information technology system, this Privacy Impact Assessment is conducted as it relates to the DHS construct of the Fair Information Practice Principles. This Privacy Impact Assessment examines the potential privacy impact of ICE use of publicly available and social media information.

1. Principle of Transparency

Notice of ICE operational use of publicly available information including social media information for law enforcement investigations is provided by the publication of this Privacy Impact Assessment and relevant system of records notices governing systems in which social media information collections are maintained.[42] ICE also includes notice of other instances of its use and maintenance of publicly available information including social media information in an ICE system via that system's Privacy Impact Assessment.[43] Since ICE collection and use of publicly available and social media information collections are law enforcement activities related to law enforcement investigations, it may not be feasible to provide direct notice to individuals at the time their information is collected from publicly available sources because to do so could provide notice of sensitive, ongoing law enforcement investigations.

Privacy Risk: There is a risk that individuals who use publicly available platforms, including social media platforms, may not know that the information they publicly share on the platform may be collected by ICE to support an open law enforcement investigation.

Mitigation: The risk is partially mitigated. To the extent information in this Privacy Impact Assessment is made publicly available, this Privacy Impact Assessment provides notice of ICE's collection, use, and maintenance of publicly available information, including social media information, to support law enforcement investigations.

While publicly available sources, including social media platforms, may provide notice of the potential use of information posted to the sites for law enforcement investigations pursuant to lawful process, notice of ICE's use of publicly available information as discussed in this Privacy Impact Assessment often is not provided by the platform. Further, as noted previously, ICE cannot notify an individual when their information is collected by ICE from publicly available sources because doing so could risk informing a target of an active law enforcement activity of an open investigation.

To mitigate this risk, ICE personnel may only view information that is available to the public (e.g., not behind added privacy walls). ICE assumes the individual is on notice that their information, not subject to additional privacy restrictions, is viewable by anyone that has access to the publicly available source/social media platform. In other words, ICE will only access publicly available sources to collect and analyze data that is available (either for free or for

[42] For a list of all ICE system Privacy Impact Assessments, *see* www.dhs.gov/privacy-documents-ice. For a list of Systems of Records Notices published by ICE, *see* https://www.dhs.gov/system-records-notices-sorns.
[43] *See* the Appendix to this Privacy Impact Assessment for a list of ICE systems that contain publicly available and social media information.

purchase) to the public and directly relevant to an open law enforcement investigation.

Privacy Risk: There is a risk that a third party may post an individual's information to a website or social media platform without the individual's consent and that information is then used by ICE in a law enforcement investigation.

Mitigation: This risk cannot be mitigated. At the time of collection, ICE cannot determine whether an individual provided a third party with consent to publicly post their information to a website or social media platform. Similarly, ICE cannot determine whether an individual understands the privacy policies and settings of a social media platform before they posted the information to a publicly available source.

Privacy Risk: There is a risk that individuals will not know that their information was obtained by ICE to support an open law enforcement investigation.

Mitigation: This risk is partially mitigated.

Targets of investigations and their associates who are directly related to the law enforcement matter being investigated may not be aware ICE is actively collecting their information from publicly available sources/social media platforms. Providing notice to these individuals could inform them that they are the target of an actual or potential law enforcement activity or reveal ICE's investigative interest in them.

All individuals present in the United States, however, have constitutional protections in criminal proceedings entitling them to discovery production.[44] The discovery obligations of federal criminal prosecutors established by the Federal Rules of Criminal Procedure include Rule 16, and Rule 26.2. Additionally, the requirements of 18 U.S.C. § 3500 (the Jencks Act), *Brady v. Maryland*,[45] and *Giglio v. United States* apply.[46] In court, each party is responsible for producing evidence upon which it seeks to rely in the litigation. Therefore, if ICE seeks to use publicly available information or evidence derived from such information to sustain any charge or otherwise use as evidence, it would be required to produce that information to the defendant.

Further, as noted previously, ICE may not collect information that is not directly relevant to an open law enforcement investigation, which helps mitigate the number of individuals potentially impacted by ICE's use of publicly available information to support law enforcement investigations.

2. Principle of Individual Participation

As with notice, ICE cannot involve the individual in the process of using their personally

[44] Discovery is the pre-trial process parties use to gather information in preparation for trial. Parties may obtain discovery regarding any nonprivileged matter in the form of records, testimony, and other information, that is relevant to any party's claim or defense. *See* Fed. R. Civ. P. 26-37, and Fed. R. Crim. P. 16 and 26.2, *available at* https://www.uscourts.gov/rules-policies/current-rules-practice-procedure.
[45] 373 U.S. 83 (1963).
[46] 405 U.S. 150 (1972).

identifiable information to support open investigations. To seek consent for the collection, use, dissemination, and maintenance of their personally identifiable information could risk exposing an ongoing law enforcement investigation. To mitigate this risk, ICE is not permitted to access and use information from publicly available sources that is subject to additional privacy safeguards. For instance, social media platforms may allow individual users to set privacy restrictions on who may access and see their content. If these restrictions are in place, ICE may not access that information. Additionally, individuals may edit, correct, or update information shared in their own posts or in comments they made to the posts of others.

An individual's ability to access or amend information in ICE law enforcement information systems is limited by law and policy due to the need to protect the integrity of national security or law enforcement sensitive information.[47] Access to ICE records might also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, harm victims, or avoid detection or apprehension. Individuals may submit requests for information access and correction as permitted by the Privacy Act, and the requests will be reviewed on a case-by case basis. Individuals seeking to correct records, or seeking to contest their content, may submit a request in writing to the ICE Office of Information Governance and Privacy by mail:

U.S. Immigration and Customs Enforcement Office of Information Governance and Privacy
Attn: Privacy Unit
500 12th Street SW, Stop 5004
Washington, D.C. 20536-5004
http://www.ice.gov/management-administration/privacy

Privacy Risk: There is a risk that individuals cannot access and amend inaccuracies in ICE systems that maintain publicly available information, including social media information.

Mitigation: The risk is partially mitigated. For example, vendors of commercial data should endeavor to ensure their information collections contain near real-time data for the efficacy of the product that ICE would utilize. However, if a vendor collects data from publicly available sources, any edit, correction, or update the individual makes to the information in the data sources might be delayed before it is reflected in the vendor database. Moreover, vendors may not notify ICE when an edit, update, or correction occurs within its own proprietary database. Likewise, information ICE accesses from other publicly available sources, including social media information, may be amended without notice to ICE.

In accordance with ICE policy, ICE users will research and corroborate the source data to ensure that the information is as accurate, timely, and complete prior to using the data to generate an investigative lead or pursuing a law enforcement action. Likewise, as noted above, users will

[47] *See* DHS/ICE-009 External Investigations, 85 FR 74362, (November 20, 2020), Final Rule for Privacy Act Exemptions, 74 FR 4508 (August 31, 2009), *available at* https://www.dhs.gov/system-records-notices-sorns.

document the source(s) of information, including whether a vendor was used to obtain the information, in the relevant investigative case file.

3. Principle of Purpose Specification

ICE is authorized to collect information under Section 701 of the USA PATRIOT Act; 6 U.S.C. § 112; 8 U.S.C. §§ 1105, 1103(a)(4), 1357(a) and (b); and Executive Order 13388. Pursuant to the Homeland Security Act of 2002 (HSA), as amended, Pub. L. 107-296, 116 Stat. 2135 §§ 102, 403, 441 (Nov. 25, 2002), the U.S. Secretary of Homeland Security has the authority to enforce numerous federal criminal and civil laws. These include laws contained in Titles 8, 18, 19, 21, 22, 31, and 50 of the U.S. Code. The Secretary delegated this enforcement authority to the Director of ICE in DHS Delegation Order No. 7030.2, Delegation of Authority to the Assistant Secretary for U.S. Immigration and Customs Enforcement (Nov. 13, 2004), and the Reorganization Plan Modification for the Department of Homeland Security (January 30, 2003). Through these statutes and orders, ICE has broad legal authority to enforce an array of federal statutes including responsibility for enforcing customs authorities and federal criminal authorities.

As noted previously, this Privacy Impact Assessment addresses ICE's operational use of publicly available information, including social media information to identify, investigate, locate, arrest, and support prosecution of individuals suspected of violations of laws.

Privacy Risk: There is a risk that ICE may use publicly available information including social media information for purposes beyond what is described in this Privacy Impact Assessment.

Mitigation: This risk is mitigated. ICE mitigates this risk through training, privacy compliance processes (e.g., Privacy Threshold Analysis), auditing, and oversight. ICE Privacy has created mandatory training and rules of behaviors for ICE personnel that detail the restraints and safeguards outlined in this Privacy Impact Assessment. Additionally, new tools used to collect and use publicly available and social media information must be submitted to ICE Privacy and the DHS Privacy Office for review to ensure that the proposed use and function comply with DHS social media policy and this Privacy Impact Assessment. Prior to adoption of a new tool to access, collect, use, and maintain publicly available information, including social media information to support ICE law enforcement investigations, an ICE program or office must document the purpose of the tool's use through the Privacy Threshold Analysis process. At that time, any restrictions on its use to safeguard privacy may be set by ICE Privacy or DHS Privacy. Further, ICE supervisors audit ICE case files to ensure that the source of data and the use of publicly available and social media information in law enforcement investigations complies with the principles stated in this Privacy Impact Assessment. ICE personnel who operate in contravention to the relevant rules of behavior and this Privacy Impact Assessment may have their access to tools used on publicly available information, including social media information, revoked and could potentially face disciplinary action.

Privacy Risk: There is a risk that the use of certain keywords or recurrent query tools to collect and use publicly available and social media information may be inconsistent with ICE's authority to collect such information.

Mitigation: This risk is partially mitigated. Any information sought through keyword queries must have a direct nexus to an authorized law enforcement investigation or activity. Further, any keywords used to query publicly available information will be designed in such a way as to not profile, target, or discriminate against any individual for lawfully exercising their First Amendment rights. To ensure that keyword searches are conducted in an authorized manner, keywords used to query publicly available information, including social media information, will be documented and may be periodically reviewed by the Office of the General Counsel, ICE Privacy, the DHS Privacy Office, and the DHS Office for Civil Rights and Civil Liberties. Additionally, ICE Privacy will meet monthly with the respective program to assess how keywords are being used to ensure compliance with this Privacy Impact Assessment and DHS and ICE policies.

Privacy Risk: There is a risk that ICE will use a third-party vendor or contractor to collect publicly available information that it otherwise would not be authorized to collect.

Mitigation: This risk is mitigated. ICE may not use a vendor or contractor to collect, use, maintain, or disseminate personally identifiable information that ICE does not have the authority to collect, use, maintain, or disseminate. Prior to collection, ICE ensures vendors do not collect First Amendment protected information on their behalf by providing to the vendor guidelines on permissible and prohibited collection activities. After collection, ICE personnel routinely conduct oversight of any information collected by an ICE vendor or tool to ensure the information has a direct nexus to an open investigation, is accurate, and does not run afoul of any First Amendment protections.

4. Principle of Data Minimization

ICE will collect only the minimum amount of personally identifiable information necessary and relevant to an ICE law enforcement investigation and safeguard that personally identifiable information as required by law, regulation, and/or Department or ICE policy. Further, information found on a publicly available website or social media platform that is used in an investigation will be saved in appropriate case files and ICE systems, including information about which vendor the information was first identified (if applicable). The data will be maintained in accordance with the relevant Systems of Records Notice(s) and Privacy Impact Assessment(s), as well as the NARA-approved retention schedule(s). Relevant case files and case systems are periodically audited by supervisors and the ICE Records and Information Management Unit to ensure proper record retention and disposition.

Privacy Risk: There is a risk that ICE will collect and retain more publicly available information, including social media information, than necessary or relevant to support an open law enforcement investigation.

Mitigation: This risk is mitigated. Pursuant to ICE policy, ICE may only collect information relevant to an authorized law enforcement investigation. Because collection of publicly available information, including social media information, may implicate First Amendment protected activities, ICE personnel would not collect information about how an individual exercises their First Amendment rights "unless expressly authorized by statute, or by the individual about whom the record is maintained, or unless pertinent to and within the scope of an authorized law enforcement activity" as prescribed by the Privacy Act. As previously discussed, ICE personnel document how information relates to an investigation or specific violation of law investigated and enforced by ICE prior to its collection.

Further, if ICE personnel discover that collected information is irrelevant to an open law enforcement investigation, they will not use or maintain it. Similarly, if information discovered not to be relevant was previously added to a case file, responsible ICE personnel will remove such information. Additionally, as noted previously, there are safeguards in place to ensure that targeted collection of publicly available information, including social media information, is directly relevant to an open law enforcement investigation. Supervisory approval is required before ICE users may automatically collect information from websites. And ongoing collection must be continually evaluated to ensure that only information directly related to an investigation is being collected. If the information is determined to be inaccurate, no longer credible, and/or no longer relevant, collection must end immediately, and such information may not be used or retained.

Privacy Risk: There is a risk that ICE will collect First Amendment-protected information.

Mitigation: This risk is partially mitigated. The Privacy Act generally prohibits the collection of records describing how an individual exercises rights guaranteed by the First Amendment.[48] There are exceptions, however, including if the record is "pertinent to and within the scope of an authorized law enforcement activity." ICE personnel receive social media training created by ICE Privacy, ICE Office of the Principle Legal Advisor, and the DHS Office for Civil Rights and Civil Liberties on how to identify protected First Amendment activity and determine if publicly available content is pertinent to and within the scope of an authorized ICE law enforcement investigation. If the information does not meet this standard, then ICE may not collect or use it. Additionally, ICE personnel manually review publicly available information, including social media information, to assess its accuracy, credibility and timeliness and corroborate it by, for example, comparing it to other information maintained in government databases and other credible sources. ICE personnel will also determine and document the relevance of the information collected to the authorized law enforcement activity and whether it contains protected speech. ICE

[48] 5 U.S.C. § 552a(e)(7).

personnel may contact ICE Privacy and the Office of the Principle Legal Advisor to aid in this determination.

This determination will be periodically reviewed by the supervisory investigative agent to ensure ICE personnel adhere to the Privacy Act and do not collect First Amendment-protected information. Protected speech that is either not pertinent to or outside the scope of an ICE law enforcement activity must not be collected, used, and/or retained.

Privacy Risk: There is a risk that ICE use of automated collection and query tools (e.g., "scraping" tools) to support law enforcement investigations will collect information on or about individuals who are not suspected of violations of laws enforced by ICE.

Mitigation: This risk is partially mitigated. ICE's use of tools, such as recurrent query platforms or automated collection tools, is subject to the polices and safeguards discussed above, to minimize the risk of collecting information irrelevant to a law enforcement investigation and focus collections on information that is directly relevant to an ICE law enforcement investigation. Prior to a tool's implementation, an ICE program or office must document the purpose of the tool's use through the Privacy Threshold Analysis process. At that time, any restrictions on and privacy safeguards required for its use may be set by ICE Privacy or the DHS Privacy Office. Once in use, automated collection tools are only used for sites or chatrooms verified by ICE supervisors to contain information of suspected violations directly relevant to an authorized open investigation.

Similarly, ICE only uploads known suspect information to recurrent query platforms. Therefore, the returns created by these tools are designed and expected to be directly related to an open ICE law enforcement investigation. ICE does not use information about individuals who are not the targets of ICE law enforcement activities. Any returns are also assessed by ICE personnel to verify their accuracy and relevance to an ongoing ICE case. That verification is required before the data is loaded into an ICE case file or ICE case management system. Any data that is deemed irrelevant, inaccurate, and/or unreliable, is purged from the tool and may result in a determination to end collection on a designated site or platform.

5. Principle of Use Limitation

ICE personnel collect publicly available information, including social media information to support open law enforcement investigations. As discussed previously, search techniques and queries are governed by ICE and DHS policy, including applicable rules of behavior and this Privacy Impact Assessment.

ICE also uses tools, such as data aggregators, anonymizers, recurrent query platforms, and/or automated collection tools, to collect publicly available information directly relevant to an open law enforcement investigation. Some of these tools automate methods for detecting, summarizing, and graphically representing patterns of relationships between entities within the parameters discussed above. This allows ICE personnel to identify potentially criminal and fraudulent behavior directly related to a law enforcement investigation and assists them in

detecting crimes enforceable by ICE. ICE personnel will use these tools either alone or in combination to research and identify individuals, businesses, and business assets as targets of open law enforcement investigations. For every new tool that ICE plans to use, the relevant ICE program must submit a Privacy Threshold Analysis to ICE Privacy for review to ensure its use complies with law and policy and this Privacy Impact Assessment. At that time, ICE Privacy may recommend additional mitigation strategies to protect individual privacy. The Privacy Threshold Analysis must also be reviewed and approved by the DHS Privacy Office, which may also include additional privacy safeguards as a condition to use the tool.

In addition, ICE will not share personally identifiable information collected from publicly available information including social media information with third parties or external agencies unless directly related to an ICE law enforcement investigation. For example, after ICE has corroborated information and determined its accuracy, relevance, and timeliness, ICE may generate a shareable lead. Leads generated from publicly available information, including social media information may ultimately be shared with federal, state, tribal, local, and foreign law enforcement agencies, as well as relevant law enforcement fusion centers with which ICE has pre-existing information sharing agreements. ICE data may be shared only if the recipient agency has a need to know the information, sharing will further U.S. law enforcement and/or national security efforts, and disclosure is consistent with applicable law and agency policies. Sharing may be done manually by ICE personnel (e.g., via secure email or file transfer) or via system-to-system connections between ICE systems and a third-party system. Prior to sharing, ICE will ensure that the transfer is compatible with the original purpose of the collection (i.e., pursuant to a law enforcement investigation) and meets a routine use(s) of the applicable ICE system's System of Records Notice. ICE will share information outside the agency in accordance with the procedures and safeguards of the relevant ICE system in which the information is maintained, as described in the system's Privacy Impact Assessment and System of Records Notice[49] and consistent with information sharing agreements and applicable privacy safeguards.

Privacy Risk: There is a risk that ICE personnel without a legitimate need to know may access publicly available information, including social media information, including through access to a tool or database used by ICE in support of its law enforcement investigations.

Mitigation: This risk is mitigated. In addition to supervisors nominating and approving ICE personnel to use the tools discussed in this Privacy Impact Assessment, ICE personnel must apply to the ICE administrator of a tool or platform to be granted access to it. ICE supervisors must review every application before it is approved. Only authorized ICE personnel with a need to know and who have completed, and are current on, the prerequisite privacy and other training will be granted access to a tool or platform, including access to publicly available information accessed through the tool or platform. Lists of authorized users are reviewed periodically by ICE

[49] *See* the Appendix to this Privacy Impact Assessment for a list of ICE systems that contain publicly available and social media information and their associated Privacy Impact Assessments and System of Records Notices.

supervisory personnel to ensure a user's ongoing need to access the tool. Additionally, DHS Directive 110-01 requires that access authority be renewed annually consistent with annual training requirements. Access is contingent upon ICE personnel's successful completion of privacy and other training for operational use of publicly available information and social media information.

Privacy Risk: There is a risk that ICE may share information with parties who do not have a need to know or in a manner inconsistent with law and policy.

Mitigation: This risk is partially mitigated. If publicly available information, including social media information, is discovered in the course of an ICE law enforcement investigation and requires action by a federal, state, local, or international agency, ICE may share that information in a manner consistent with ICE policy and only for purposes permitted in the relevant System of Records Notice. ICE personnel are trained regarding whether information sharing is compatible with the purpose for which the information was originally collected. Personnel may also contact ICE Privacy for advice and guidance regarding permissible disclosures of personally identifiable information. Further, ICE personnel must document instances of information sharing in the relevant case file(s) and ICE case management systems. Instances of unauthorized disclosure are referred to the ICE Office of Professional Responsibility.

6. Principle of Data Quality and Integrity

There is a risk that information collected from publicly available sources, including social media information, may be inaccurate, incomplete, and/or irrelevant to an ICE law enforcement investigation. Accordingly, ICE must corroborate any publicly available information collected to support an open ICE law enforcement investigation to ensure that the information is accurate, relevant, timely, and complete. Additionally, if at any time ICE learns that it has received or is in possession of inaccurate information, it will correct, annotate, block or delete the incorrect information and will not use or disseminate the incorrect information. Further, ICE personnel may corroborate social media information with other data from public records data sources, information available in commercial and government databases, or information obtained from other governmental partners. ICE may not rely solely on information obtained from social media to take law enforcement action against any individual. ICE only uses this information to generate a possible lead and must corroborate the information before taking such action, including applying for a warrant or subpoena.

Finally, to ensure ICE is complying with the data quality safeguards articulated in this Privacy Impact Assessment, ICE, in coordination with ICE Privacy, will routinely review and audit all ICE offices that access publicly available information, including social media information as part of their law enforcement activities. Additionally, the DHS Chief Privacy Officer may choose to conduct a Privacy Compliance Review of ICE's use of publicly available information for law enforcement investigations.

Privacy Risk: There is a risk that information collected by ICE from publicly available sources, including social media sites, will be inaccurate and unverifiable.

Mitigation: This risk is partially mitigated. ICE uses traditional investigative methods to assess the accuracy and reliability of any publicly available information collected to support an open law enforcement investigation prior to generating a lead or entering the data into an ICE system. This includes using the totality of the information available and reviewing information from multiple sources, including public records data sources and government databases. To use publicly availability information, including social media information to support open ICE law enforcement investigations, ICE users must complete relevant training, including privacy training, to learn to analyze information and determine its reliability. ICE only considers corroborated information derived from social media to support a law enforcement investigative lead. ICE does not take any law enforcement action based solely on social media posts.

7. Principle of Security

ICE limits social media access to users who have completed annual social media training, show a need to access social media for their work, have agreed to specific rules of behavior associated with access to social media tools, and are approved to use it by a supervisor. All relevant publicly available information, including social media information, collected by ICE personnel will be stored in an ICE system(s) with built in audit controls. Users are granted access on a "need to know" basis. ICE operates its systems in compliance with the information security requirements of the Federal Information Security Modernization Act of 2014.

DHS/ICE policies and rules of behavior ensure appropriate online behavior and limit how information collected from the internet can be used for ICE operational purposes. Only ICE personnel whose official duties necessitate access to social media to support an open law enforcement investigation will be allowed to input information collected from publicly available sources, including social media platforms, into ICE systems. ICE supervisors monitor and approve which users are designated to collect publicly available information, including social media information, to support open law enforcement investigations, and that their training is current.

Supervisors must also monitor who is given access to tools and aggregators to collect publicly available information to support an open law enforcement investigation.

Access roles are assigned by a supervisor based on the user's job responsibilities and are reviewed periodically to ensure that users have the appropriate level of access. Individuals who no longer require access are removed from the access list by program managers and/or system administrators. Programs have limited numbers of accounts to access a tool, and operational needs will require a manager to transition access between and among ICE personnel needing access to a given tool. Additionally, tools are acquired on a license basis, and each instance of use must be justified each contract or option year. This is an additional opportunity for supervisors and program managers to determine which ICE personnel need access to a tool. It is incumbent upon the ICE

supervisors to maintain log files containing this information and make them available for ICE Privacy for inspection or for ICE Office of Professional Responsibility to conduct a complete audit.

ICE systems that contain publicly available information, including social media information, are restricted to personnel that have a need to know the information according to their job duties. When investigative data is imported into ICE systems, ICE personnel are required to either manually or electronically share this data with their supervisors for review.[50] ICE personnel are also required to record a description of the data being uploaded, such as source name/category and date retrieved, and the tool used to collect the information, which helps the supervisor evaluate whether the upload complies with ICE policy and helps other users better understand and evaluate the data. Supervisors are responsible for identifying any data imported into ICE systems in contravention of DHS/ICE policy. Supervisors may request that the system administrator delete any improperly uploaded data in an ICE system.

Privacy Risk: There is a risk that an unauthorized individual without a legitimate need to know may access publicly available information including social media information maintained in ICE systems.

Mitigation: This risk is mitigated. ICE system security measures are determined on a system-by-system basis, and all systems have varying degrees of access controls. Additionally, all ICE systems must abide by ICE and DHS security policies.[51] Moreover, because these systems contain law enforcement sensitive information (information that, if disclosed, could be detrimental to ICE law enforcement activities), additional scrutiny is placed upon user access restrictions in the systems to ensure that only authorized users are granted access. These systems go through security accreditations and Privacy Impact Assessments to ensure that only authorized users with a need to know will have access to data stored in the system, including social media information and publicly available data.

8. Principle of Accountability and Auditing

ICE ensures compliance with this Privacy Impact Assessment by instituting rigorous standards for training, rules of behavior, information sharing, auditing, and supervisory oversight. Additionally, rules of behaviors for ICE users of social media platforms to support open law enforcement investigations have been created in consultation with ICE Privacy and ICE Office of the Principle Legal Advisor to ensure the practices protect the privacy, civil rights, and civil liberties of individuals. ICE users who collect data from social media platforms certify annually that they have read and understand ICE policy and privacy guidance on the use of social media information.

---

[50] System specific controls are found in the system's Privacy Impact Assessment. ICE systems that contain publicly available and social media information can be found in the Appendix to this Privacy Impact Assessment, and are available at www.dhs.gov/privacy/documents-ice.

[51] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, 4300A SENSITIVE SYSTEMS HANDBOOK, VER. 13.1 (2017), *available at* https://www.dhs.gov/privacy-policy-guidance.

A mandated training program is also in place to teach ICE personnel how to properly collect information from publicly available sources, including social media platforms and to do so in accordance with ICE and DHS policies. This training is an annual requirement for ICE personnel with a need to collect personally identifiable information from publicly available sources, such as social media, for an operational purpose to support an ICE law enforcement investigation, and each user must sign a confirmation that they received and understood the training.

Most, but not all, tools used to collect publicly available information, including social media information provide auditing and accountability mechanisms, and provide a log of the date, time, user identity, and search terms that are queried. In these instances, ICE has access to the logs to ensure that the use of the systems is compliant with ICE and DHS policy. Otherwise, supervisors must create a local logging and auditing regime to mimic these requirements. ICE Privacy will work with supervisors to create appropriate logging and auditing capabilities.

ICE Privacy will develop and periodically administer an inspection mechanism to assess whether ICE's use of publicly available information, including social media information to support ICE law enforcement investigations is in compliance with the terms of this Privacy Impact Assessment. ICE Privacy will regularly evaluate the operations of program offices to ensure social media information users have completed required training and have agreed to follow the terms outlined in the corresponding rules of behavior. ICE Privacy will also assess a program's monitoring/auditing processes to ensure their efficacy and advise on best practices. Finally, ICE Privacy, in coordination with the DHS Privacy Office, through the Privacy Threshold Analysis process, will assess whether the use of publicly available information and associated tools to support ICE law enforcement investigations is consistent with this Privacy Impact Assessment and the safeguards described herein.

Additionally, ICE cybersecurity policies require personnel to use government furnished equipment for official operations. Tools that collect publicly available information, including social media information are accessed via government furnished equipment that is equipped with logging and oversight mechanisms to ensure the proper use of government IT systems. This equipment is assigned to specific ICE personnel who agree to be monitored regarding the equipment's use. Any interaction these tools may have with government furnished equipment (e.g., URL access, downloads, uploads) would therefore be logged and may be audited by ICE system administrators.

Further, audit logs are created when social media information is entered into ICE systems. Per the 2012 Morton Memorandum,[52] ICE personnel will retain any information derived from online sources in the same manner as if that content had been derived from a hard copy document or other data source (e.g., database). This includes noting the information collection or uploading the information into ICE systems prior to using the information for operational purposes.

[52] *See* U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, POLICY GUIDANCE MEMORANDUM 100821.1 USE OF PUBLIC AND NON-PUBLIC ONLINE INFORMATION (2012).

Generally, such documentation would include the date, time, and name of the user who uploaded the data into the system, the origin of the information collected, such as the date the information was collected and the site(s) accessed, as well as any tool used to access the information. Automated documentation mechanisms are system-specific and are detailed in the system's respective Privacy Impact Assessment.[53]

ICE supervisors routinely check these logs and their accompanying data to ensure that the data entered does not violate ICE policy or system requirements. The electronic records are preserved and maintained in accordance with an applicable National Archives and Records Administration (NARA) General Records Schedule (GRS) or a NARA-approved agency-specific records control schedule. If the records are subject to a litigation hold, they may not be disposed of under a records schedule until further notification.

Privacy Risk: There is a risk that ICE personnel will collect publicly available information without the appropriate training or oversight.

Mitigation: This risk is partially mitigated. While the internet allows easy access to publicly available information, ICE users must follow all policies and procedures, including as discussed in this Privacy Impact Assessment before they may use publicly available information, including social media information in an ICE law enforcement investigation. This includes completing required privacy and other training, reviewing and agreeing to follow applicable rules of behavior, obtaining required supervisory approval, and making any required relevancy determinations as discussed previously. Additionally, publicly available information must be corroborated for accuracy and reliability before it may be used in an investigation, and no law enforcement action may be based solely on information obtained from social media.

Information relevant to a law enforcement investigation must be documented in the appropriate case file. Access, collection, use, and retention of publicly available information is subject to supervisor review. These checks help ensure ICE users have a need to acquire publicly available information to support an ICE law enforcement investigation and abide by ICE and DHS policy regarding training and oversight. Any user found to be using social media platforms or tools for a purpose that is inconsistent with law, regulation, or policy will have their access revoked and could face disciplinary action, in addition to deletion of the information.

Privacy Risk: There is a risk that a third-party vendor could have access to personally identifiable information ICE users input into vendor-provided tools or applications.

Mitigation: This risk is mitigated. While vendors may need to retain some administrative functions within the tools and applications, ICE will maintain control of all use restrictions and auditing capabilities, unless any additional functions assigned to the vendor are detailed in the contract and performed under general ICE supervision. Additionally, the vendor may not use personally identifiable information input into a tool or application by an ICE user to further refine

[53] For more information see the Appendix to this Privacy Impact Assessment.

or train its tools/models.

Conclusion

ICE uses publicly available information, including social media information, in its law enforcement investigations. ICE also uses tools to assist with its collection and analysis of this information. ICE ensures that individual privacy, civil rights, and civil liberties are respected by ensuring appropriate safeguards are in place for the use of this information and maintaining compliance with DHS policy for the operational use of social media. Through proper training and oversight, ICE ensures its personnel collect, use, and maintain information collected online in a lawful and responsible manner.

Responsible Officials

Peter J. Hatch
Assistant Director
Homeland Security Investigations
U.S. Immigration and Customs Enforcement

Kenneth N. Clark, Ph.D.
Assistant Director
Management and Administration
U.S. Immigration & Customs Enforcement

Approval Signature

Original, signed version on file with the DHS Privacy Office.

_____

Mason C. Clutter
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

Appendix

ICE Systems that maintain Publicly Available Information and Social Media Information for Law Enforcement Investigations

Student and Exchange Visitor Information System (SEVIS)	DHS/ICE/PIA-001 Student and Exchange Visitor Program (SEVP)	DHS/ICE-001 Student and Exchange Visitor Program (SEVP)	DAA-0567-2016-0004-0003. Retention Period: Destroy when no longer needed for reference or 10 years after cut off, whichever is later.
Law Enforcement Intelligence Fusion System (IFS)	DHS/ICE/PIA-007 Law Enforcement Intelligence Fusion System (IFS)	DHS/ICE-006 ICE Intelligence Records (IIRS)	N1-567-09-08 Item 1A(2) Retention Period: Destroy 75 years after cutoff, and only after verification that it is no longer needed to conduct agency business.
Significant Event Notification System (SEN)	DHS/ICE/PIA-023 Significant Event Notification System (SEN)	DHS/ICE-006 - IIRS DHS/ICE-009 - External Investigations	N1-567-2011-004 Retention Period: Destroy 75 years after cutoff.
ICE Subpoena System	DHS/ICE/PIA-027 ICE Subpoena System	DHS/ICE-009 - External Investigations	N1-567-2011-011. Retention Period: Destroy 10 years after cutoff.
National Intellectual Property Rights Coordination Center	DHS-ICE-PIA-041 National Intellectual Property Rights Coordination Center	DHS/ICE-009 - External Investigations	A retention schedule is currently under development. ICE is proposing a 5 year period for unpursued claims and a period for investigations of 25 years after the case is closed
ICE SharePoint Sites	DHS/ICE/PIA-043 SharePoint Matter Tracking Systems	SORN will be dependent on the program the SharePoint site is supporting (see PIA)	Determined by the purpose for the original collection
LeadTrac System	DHS/ICE/PIA-044	DHS/ICE-009	DAA-563-2013-0001-0006.

	LeadTrac System	External Investigations DHS/ICE-015 LeadTrac System	Retention Period: Destroy 75 years after cutoff.
ICE Investigative Case Management (ICM)	DHS/ICE/PIA-045 ICE Investigative Case Management (ICM)	DHS/ICE-009 External Investigations	N1-36-86-001 Retention Period: Destroy when 20 years old.
Pre-Adjudicated Threat Recognition Intelligence Operations Team Tracking System (PATRIOT)	DHS/ICE/PIA-052 Visa Security Program Pre-Adjudicated Threat Recognition Intelligence Operations Team Tracking System	DHS/ICE-012 Visa Security Program Records	N1-567-10-005. Retention Period: Destroy 25 years after cutoff for Visa Security Reviews without a nexus to terrorism. Destroy 75 years after cutoff for Visa Security Reviews found to be a nexus to terrorism.
Repository for Analytics in a Virtualized Environment (RAVEn)	DHS/ICE/PIA-055 Repository for Analytics in a Virtualized Environment (RAVEn)	DHS/ICE-018 Analytical Records	Determined by the purpose for the original collection

Policy Number: 10082.1
FEA Number: 360-112-002b

Office of the Director

U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20536

U.S. Immigration and Customs Enforcement

JUN 28 2012

MEMORANDUM FOR: Law Enforcement Personnel

FROM: John Morton
Director

SUBJECT: Use of Public and Non-Public Online Information

Purpose

This memorandum provides U.S. Immigration and Customs Enforcement (ICE) law enforcement personnel guidance on the acceptable use of online information within the scope of their law enforcement duties.

Background

On December 8, 2010, Secretary Napolitano approved a decision memorandum titled, "Use of Public and Non-Public Online Information for Law Enforcement, Situational Awareness, and Intelligence Purposes," ("The Online Information Memorandum") that adopted a recommendation whereby the Department of Homeland Security (DHS), except members of the Intelligence Community governed by Executive Order 12333, would "follow the Department of Justice (DOJ) 1999 guidelines for online investigative and situational awareness activities." The Online Information Memorandum also suggested that DHS Components develop supplementary guidance, as necessary, for their mission-specific purposes consistent with DHS policy.

Discussion

Pursuant to the Online Information Memorandum, ICE law enforcement personnel should follow the below principles for the use of public and non-public online information, which have been adapted from the online investigative principles outlined in DOJ's 1999 Online Investigative Principles for Federal Law Enforcement Agents.[1]

[1] Law enforcement personnel are ICE employees who conduct and support criminal, civil, and administrative law enforcement investigations and operations. Examples include special agents and other law enforcement officers, law enforcement investigative support personnel, intelligence research specialists, criminal research specialists, and attorneys prosecuting criminal, civil or administrative matters.

To implement these core principles, ICE directorates and program offices may establish guidance and/or modify existing guidance, as necessary, or reference the DOJ guidance as applicable to the activities in question.

ICE Principles for Law Enforcement Use of Public and Non-Public Online Information:

1. Obtaining Information from Unrestricted Sources. Law enforcement personnel may obtain information from publicly accessible online sources and facilities under the same conditions they may obtain information from other sources generally open to the public. This principle applies to publicly accessible sources located in foreign jurisdictions as well as those in the United States.

2. Obtaining Identifying Information about Users or Networks. There are widely available software tools for obtaining publicly available identifying information about a user or a host computer network. Law enforcement personnel may use such tools in their intended lawful manner under the same circumstances in which ICE guidelines and procedures permit them to look up similar identifying information (e.g., a telephone number) through non-electronic means. However, law enforcement personnel may not use software tools, even those generally available as standard operating system software, to circumvent restrictions placed on system users.

3. Real-Time Communications. Law enforcement personnel may passively observe and log real-time electronic communications open to the public under the same circumstances in which they may attend a public meeting.

4. Accessing Restricted Sources. Law enforcement personnel may not access restricted online sources or facilities absent legal authority permitting entry into private space.

5. Online Communications Generally. Law enforcement personnel may use online services to communicate as they may use other types of communication tools, such as the telephone and the mail. Law enforcement personnel should retain the contents of a stored electronic message if they would have retained that message had it been written on paper. The contents should be preserved in a manner authorized by ICE procedures governing the preservation of electronic communications.

6. Undercover Communications. Law enforcement personnel communicating online with witnesses, subjects, or victims must disclose their affiliation with law enforcement when ICE guidelines would require such disclosure if the communication were taking place in person or over the telephone. Law enforcement personnel may communicate online under a non-identifying name or fictitious identity if ICE guidelines and procedures would authorize such communications in the physical world. For purposes of ICE undercover guidelines, each discrete conversation online constitutes a separate undercover activity or contact, but such a conversation may comprise more than one transmission between the law enforcement personnel and another person.

7. Online Undercover Activities. Just as law enforcement agencies may establish physical-world undercover entities, they also may establish online undercover facilities, such as bulletin board systems and Web sites, which covertly offer information or services to the public. Online undercover facilities, however, can raise novel and complex legal issues, especially if law enforcement personnel seek to use the system administrator's powers for criminal investigative purposes. Further, these facilities may raise unique and sensitive policy issues involving privacy, international sovereignty, and unintended harm to unknown third parties. Because of these concerns, a proposed online undercover facility, like any undercover entity, may be established only if the operation is authorized pursuant to ICE's guidelines and procedures for evaluating undercover operations.

8. Communicating Online Through the Use of the Identity of a Cooperating Witness, with Consent. Law enforcement personnel may ask a cooperating witness to communicate online with other persons in order to further an investigation if agency guidelines and procedures authorize such a consensual communication in person, over the telephone, or through other non-electronic means. Law enforcement personnel may communicate online using the identity of another person if that person consents, if the communications are within the scope of the consent, and if such activity is authorized by ICE guidelines and procedures. Personnel who communicate online through the identity of a cooperating witness are acting in an undercover capacity.

9. Appropriating Online Identity. "Appropriating online identity" occurs when law enforcement personnel electronically communicate with others by deliberately assuming the known online identity (such as the username) of a real person, without obtaining that person's consent. Appropriating identity is an intrusive law enforcement technique that should be used infrequently and only in serious criminal cases. When assuming an online identity, law enforcement personnel must follow all applicable ICE policies and guidelines.

10. Activity by Law Enforcement Personnel during Personal Time. While not on duty, law enforcement personnel are generally free to engage in personal online pursuits. If, however, the off-duty online activity directly and substantially relates to a law enforcement investigation, operation, or prosecution, law enforcement personnel are bound by the same restrictions regarding the use of online information as would apply when on duty.

11. International Issues. Unless gathering information from online facilities configured for public access, law enforcement personnel conducting investigations should use reasonable efforts to ascertain whether any pertinent computer system, data, witness, or subject is located in a foreign jurisdiction. Whenever an item or person is located abroad, law enforcement personnel should follow ICE's policies and procedures for international investigations.

Personnel who conduct and support criminal and civil law enforcement investigations and/or operations must adhere to the above principles when using information gathered online in support of an official agency criminal or civil law enforcement investigations and/or operations.

The principles that address the use of the Internet for undercover activities apply only to ICE personnel with the authority to conduct undercover investigations.

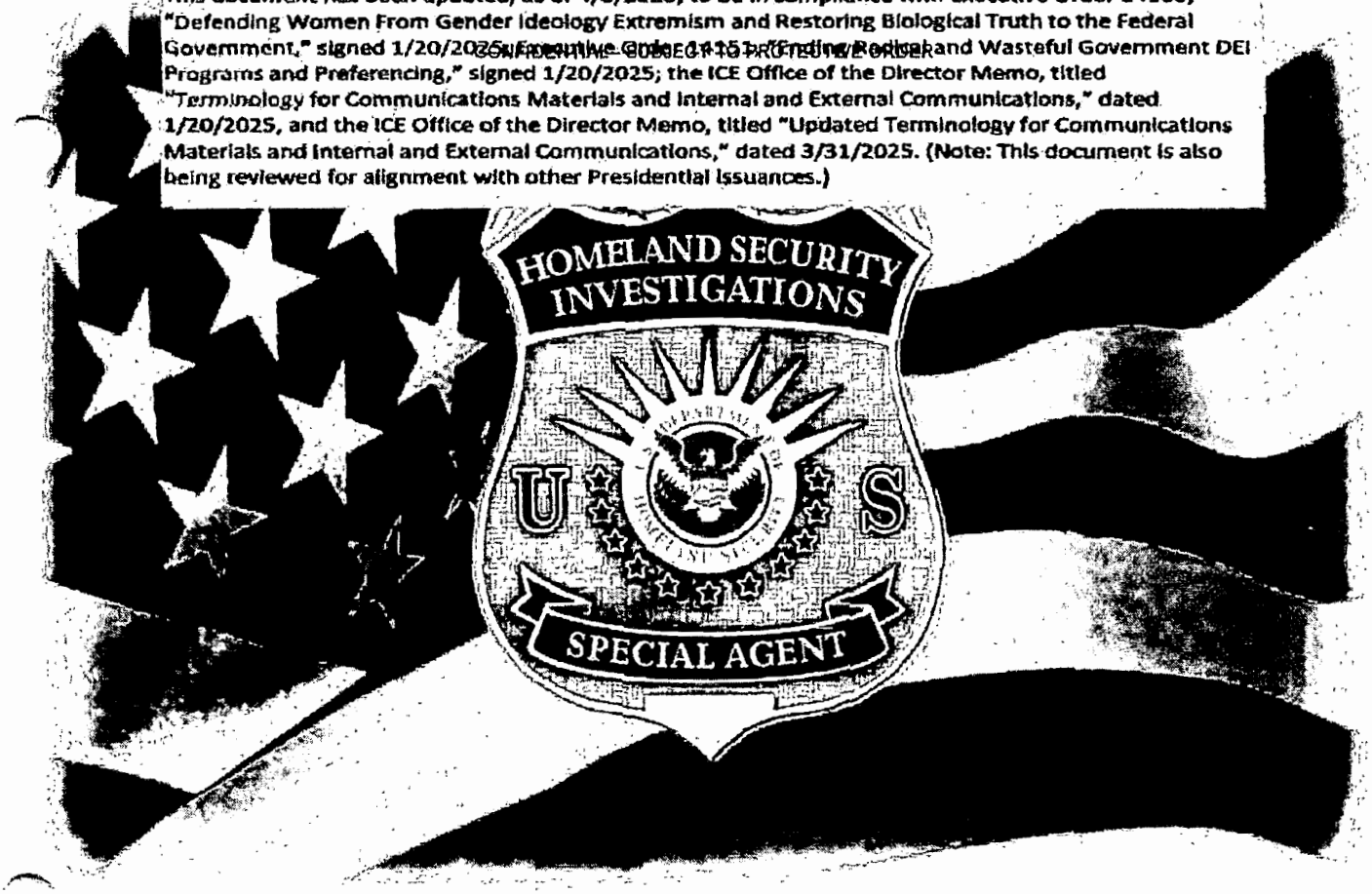
Personnel who conduct civil and criminal law enforcement activities for Enforcement and Removal Operations should also adhere to the above principles when using information gathered online in support of their law enforcement activities. Such personnel should remain mindful that the principles that address the use of the Internet for undercover activities apply only to those vested with such authority.

Attorneys with the Office of the Principal Legal Advisor should also adhere to the above principles, except those that are applicable to undercover activities, when using information gathered online in support of their handling of criminal, civil, or administrative matters.

No Private Right of Action

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 by any party in any administrative, civil, or criminal matter.

This document has been updated, as of 4/8/2025, to be in compliance with Executive Order 14168, "Defending Women From Gender Ideology Extremism and Restoring Biological Truth to the Federal Government," signed 1/20/2025; Executive Order 14151, "Ending Radical and Wasteful Government DEI Programs and Preferencing," signed 1/20/2025; the ICE Office of the Director Memo, titled "Terminology for Communications Materials and Internal and External Communications," dated 1/20/2025, and the ICE Office of the Director Memo, titled "Updated Terminology for Communications Materials and Internal and External Communications," dated 3/31/2025. (Note: This document is also being reviewed for alignment with other Presidential Issuances.)



Homeland Security Investigations

Arrest Procedures Handbook

HSI HB 15-03 / July 21, 2015

U.S. Immigration and Customs Enforcement

EXHIBIT 48

Foreword

The Arrest Procedures Handbook provides a single source of national policies, procedures, responsibilities, guidelines, and controls that should be followed by U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Special Agents when exercising the authority to detain, arrest, and transport individuals in custody in the course of conducting investigations and other enforcement-related activities within the scope of their authority. This Handbook contains instructions and guidance that will help ensure uniformity and operational consistency among all HSI field offices. (Note: HSI SAs must comply with the Department of Homeland Security's Commitment to Nondiscriminatory Law Enforcement and Screening Activities and with ICE Directive 11062.2 entitled, "Sexual Abuse and Assault Prevention and Intervention," dated May 11, 2014, or as updated.)

This Handbook supersedes Office of Investigations Handbook 07-02 entitled, "Arrest Procedures Handbook," dated October 7, 2007, and all other policies or other documents on arrest procedures issued by HSI since October 7, 2007.

The Arrest Procedures Handbook is an internal policy of HSI. It is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by any party in any administrative, civil, or criminal matter, nor are any limitations hereby placed on otherwise lawful enforcement prerogatives of ICE. This Handbook is For Official Use Only (FOUO) – Law Enforcement Sensitive. It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security policy relating to FOUO information and the ICE Directive on Safeguarding Law Enforcement Sensitive Information. This information shall not be distributed beyond the original addressees without prior authorization of the originator. If disclosure of this Handbook or any portion of it is demanded in any judicial or administrative proceeding, the HSI Records and Disclosure Unit, as well as the ICE Office of the Principal Legal Advisor and/or U.S. Attorney's Office, are to be consulted so that appropriate measures can be taken to invoke privileges against disclosure. This Handbook contains information which may be exempt from disclosure to the public under the Freedom of Information Act, Title 5, United States Code, Section 552(b), and protected from disclosure pursuant to the law enforcement privilege. Any further request for disclosure of this Handbook or information contained herein should be referred to the Records and Disclosure Unit.

The HSI Policy Unit is responsible for coordinating the development and issuance of HSI policy. All suggested changes or updates to this Handbook should be submitted to the HSI Policy Unit which will coordinate all needed revisions.

Peter T. Edge
Executive Associate Director
Homeland Security Investigations

JUL 21 2015
Date

ARREST PROCEDURES HANDBOOK

Table of Contents

ARREST PROCEDURES HANDBOOK

Chapter 1. PURPOSE AND SCOPE

The Arrest Procedures Handbook establishes policy and procedures for U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Special Agents (SAs) when they exercise the authority to detain, arrest, or transport individuals. (Note: Any force used to detain, arrest, and/or transport individuals must be used in accordance with the Interim ICE Use of Force Policy, issued July 7, 2004, or as updated.)

Chapter 2. INTRODUCTION

The scope of HSI SAs' authority is established by the United States Constitution and by statute, and SAs must know the bases for their authority as well as the limits of such authority. SAs may take an individual into custody only when acting within the scope of their legal authority.

The detention, arrest, and transport of individuals are among the most dangerous duties performed by HSI SAs. Many law enforcement officer casualties occur in the course of performing such duties. The procedures and standards set forth in this Handbook have been developed to minimize such casualties. These procedures and standards can also preclude costly and time-consuming lawsuits or trial tactics that might divert the attention of courts and juries from the substantive facts of a case to the nature of HSI's treatment of a defendant or respondent.

Compliance with the procedures and standards set forth in this Handbook, along with HSI SAs' training, will help to ensure officer safety, safeguard the rights of those individuals in the custody of SAs, and maximize the admissibility of evidence obtained by SAs.

Chapter 3. DEFINITIONS.

The following definitions are provided for the purposes of this Handbook:

3.1 Adult

Any person who is 18 years of age or older.

3.2 Arrest

An actual or constructive restraint or detention of an individual performed with the purpose of taking the individual into custody.

3.3 Booking

The act of processing an arrestee into a detention facility. This process generally includes recording the subject's personal information, photographing, fingerprinting, criminal records check, medical questionnaire, property inventory, and entrance into a detention facility. This facility may be operated by Federal, State, and/or local jurisdictions.

3.4 Detention

Restraining an individual's freedom of movement or ability to walk away during an investigative inquiry by establishing temporary control over the individual.

3.5 High Risk Prisoner

A prisoner who SAs believe poses an exceptional escape risk and/or who is charged with, or convicted of, a violent crime.

3.6 Juvenile

Any person under the age of 18.

3.7 Low Risk Prisoner

Any prisoner who has not been designated as high risk.

3.8 Medical Professional

A licensed doctor, nurse practitioner, technician, or aide trained to treat, provide care, or administer medication or services specific to the medical needs of the individual.

3.9 Weapon

Any object, item, or device that may be used to cause physical injury, incapacitate, or diminish capability, temporarily or permanently.

Chapter 4. RESPONSIBILITIES.

4.1 Executive Associate Director, Homeland Security Investigations

The Executive Associate Director of HSI has the overall responsibility for the oversight of the policies and procedures set forth in this Handbook.

4.2 Special Agents in Charge

Special Agents in Charge (SACs) are responsible for implementing the policies and procedures set forth in this Handbook within their respective areas of responsibility (AORs). SACs are also responsible for providing the appropriate restraining devices to all SAs in their AORs.

4.3 Special Agents

SAs are responsible for complying with the provisions of this Handbook.

Chapter 5. AUTHORITIES/REFERENCES

5.1 Authorities

A. Federal Authorities

HSI SAs' authority to arrest a person is based on various sections of law, including, but not limited to, the authority provided in Title 19, United States Code (U.S.C.), Section 1589a and 8 U.S.C. § 1357.

B. State Peace Officer Authority

In addition to Federal arrest authority, SAs may, in certain circumstances, exercise arrest authority as designated State peace officers or in their capacity as private citizens who witness a crime. As separate sovereigns, each State may determine who is authorized to enforce its laws. Usually, this means that arrest power is granted to State police, sheriffs, and various municipal police departments. Some States have enacted legislation designating Federal law enforcement officers as State peace officers with the power to enforce State law. (See HSI Directive 13-01 entitled, "HSI Special Agents Responding to State Crimes," dated May 30, 2013, or as updated.)

In addition to statutory authorization for SAs to serve as State peace officers, it may be possible to obtain State peace officer status by being "deputized" by a local sheriff or other State law enforcement official. SAs so deputized should confirm that the deputization is not merely honorary and actually carries with it the power of arrest.

Further, it is important for SAs to bear in mind that any State law enforcement authority they possess or receive should be used to further Federal law enforcement priorities.

C. Citizen's Arrest Authority

In addition to Federal and State arrest authority, HSI SAs have the power to arrest, search, or seize persons or things just as any private citizen would, and local law governs in such instances. SAs must therefore act in accordance with local law in any situation where they make an arrest for an offense that is not within the jurisdiction of

ICE. Generally, a private person may make an arrest when a crime (felony or misdemeanor) is committed or is attempted in his or her presence, or when the person arrested has committed a felony, even though not in the presence of the private person. However, SAs should check local law to see under what circumstances they may make arrests as private persons or as HSI SAs. (Note: For more information regarding citizen arrest authority and liabilities, see HSI Directive 13-01 entitled, "HSI Special Agents Responding to State Crimes," May 30, 2013, or as updated.)

5.2 References

A. ICE Interim Use of Force Policy, dated June 11, 2004, or as updated.

B. ICE Directive 10066.1 (former number: 7-3.), Consular Notification of Detained or Arrested Foreign Nationals, dated February 13, 2006, or as updated.

C. HSI Directive 14-01, Mandatory Booking of Arrestees Using EAGLE, dated April 23, 2014, or as updated.

D. HSI Directive 13-01, HSI Special Agents Responding to State Crimes, dated May 30, 2013, or as updated.

E. HSI Handbook (HB) 12-04, Search and Seizure Handbook, dated September 14, 2012, or as updated.

F. HSI HB 11-01, Computer Forensics Handbook, dated April 27, 2011, or as updated.

G. Office of Investigations (OI) HB 10-03, Interviewing Techniques Handbook, dated April 28, 2010, or as updated.

Chapter 6. LIABILITY

When seizing or arresting an individual, HSI SAs assume responsibility for the well-being of the individual, as well as the well-being of fellow officers and other people who may come in contact with the individual. SAs who carry out their duties in a negligent or wrongful manner may subject themselves, their supervisors, and the Federal government to civil liability.

SAs are subject to individual liability under *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics*, 403 U.S. 388 (1971) if, while enforcing Federal law, they violate an individual's clearly-established rights under the U.S. Constitution. Under 42 U.S.C. § 1983, SAs face similar liability for Federal civil rights violations committed while enforcing State or local law.

In rare cases, SAs may face criminal liability for alleged civil rights violations or other misconduct.

Chapter 7. DETENTION AND RELATED ISSUES

7.1 Border Detention

The border search exception to the warrant and probable cause requirements of the Fourth Amendment permits HSI SAs to detain people at the border, functional equivalent of the border, or extended border, with no suspicion, for the purpose of searching for merchandise, determination of alienage, and any evidence of admissibility.

19 U.S.C. §§ 482, 1581, and 1582 set forth SAs' customs statutory authority in this regard; while 8 U.S.C. §§ 1225 and 1357 set forth the primary immigration authority to temporarily detain aliens in the border environment. Customs detention is authorized to search for merchandise and for evidence related to the importation or exportation of merchandise. Immigration detention is authorized to determine the admissibility of an individual. In some cases, searches by SAs are limited by policy; for example, a search involving a pat down of an individual for merchandise requires one articulable fact that merchandise will be found on the person. In order to retrieve an item discovered during such a pat down, SAs must have a reasonable suspicion that the item is merchandise. Likewise, reasonable suspicion that a person is carrying merchandise inside his or her body is necessary in order to refer that person to an approved medical facility to have medical personnel conduct an internal examination.

7.2 Detention During Execution of Search Warrant

SAs executing a criminal search warrant have the authority to briefly detain any individuals present at the location of the enforcement site. Included in this authority are individuals attempting to leave the enforcement site in the presence of SAs arriving and individuals who arrive or attempt to obtain access to the enforcement site. An individual may be detained at the enforcement site during the execution of the criminal search warrant for as long as deemed necessary by the SAs. Restraints may be used in accordance with the procedures outlined in Section 8.4. The principles applicable to a Terry Stop (see Section 7.3 below) are fully applicable to those present during the execution of a search warrant.

7.3 Investigative Detentions (Terry Stops)

SAs may temporarily detain an individual when they have reasonable suspicion that the individual is engaged in criminal activity. If SAs fail to develop a probable cause belief that the person committed (or is committing) a crime or fail to establish a reasonable suspicion of wrongdoing distinct from the reason for the initial stop, they must release the individual. A stop must not be longer than the circumstances justifiably require and must not be more intrusive than reasonably necessary to verify or dispel the SAs' suspicions. A stop which is sufficiently long or unreasonable in duration or intrusiveness will constitute an arrest.

SAs may also perform a pat down search or frisk of an individual during the temporary detention as long as they have reasonable suspicion that the individual is armed and dangerous. For the SAs' protection (and the protection of others) during the detention, the SAs can conduct a limited search of the person to confirm or dispel that suspicion.

7.4 Limited Search for Officer Safety Concerns (Frisk)

Whenever there is reasonable suspicion that an individual is armed, SAs are justified, for officer safety concerns, in conducting a frisk for weapons during a detention. This limited search is performed pursuant to a Terry Stop. (See Section 7.3).

7.5 Time of Detention and Release

The amount of time that an individual may be detained must be determined by the totality of the circumstances involving the detention. Detained persons should be released as soon as possible, unless probable cause is developed and they are to be placed under arrest.

7.6 Need for Special Equipment or Personnel

If the need arises for special equipment or personnel in order to complete an investigative or enforcement action, for example canine (K-9) assistance, an interpreter, or contraband detection equipment, SAs must document the facts supporting the continued detention. Failure to do so may result in a court later ruling that any evidence found was the result of an unlawful arrest.

7.7 Access to Food, Water, and Restrooms

Individuals in custody for more than 6 hours must be given access to food at the expense of the investigating HSI field office. Water and restroom facilities should be made available to individuals in custody on an as-needed basis. Restroom facilities may be restricted if the detention results from a suspicion that the persons in custody are concealing merchandise or contraband in their body.

7.8 Access to Prescription Drugs and Medical Assistance

SAs shall ensure that detained individuals have access to their own legally prescribed medication or medical assistance during the time that they are in custody. In the event of a medical emergency, SAs should contact emergency services immediately.

7.9 Identification

All individuals detained by HSI SAs must be identified and the identities must subsequently be appropriately documented. Every effort should be taken to identify the detained individuals through the Integrated Automated Fingerprint Identification System, if feasible.

7.10 Detainment on Behalf of a Different Agency

If an individual has been detained on behalf of another agency, SAs must document the legal basis for the detention, the time the requesting agency made contact or was contacted, the time of arrival of officers from the requesting agency, and the identity of the officer to whom the person was released. In addition, it is important to note the physical and mental condition of the individual in custody at the time of the initial detention and at the time of the subsequent release.

7.11 Diplomats

Diplomats may be detained only as long as needed to determine their identity and status. If, after reviewing a diplomat's Diplomatic or Consular Identification Card, HSI SAs determine that the diplomat is accredited and not subject to any form of detention or arrest, the HSI SAs must immediately release the diplomat. The SAs should treat the diplomat with due respect and shall take all appropriate steps to prevent any attack on his or her person, freedom, or dignity. The diplomat's local consulate or embassy may assist in the verification of identity and status. Also, the U.S. Department of State (DOS)'s "Diplomatic List," which may change on a daily basis, covers foreign missions (embassies, interest sections) in the United States. The list contains the names of the staff of the foreign mission having diplomatic rank. These individuals enjoy full immunity under the provisions of the Vienna Convention on Diplomatic Relations except for U.S. nationals. The immunity status of the individual encountered during an enforcement action or investigation should be verified with DOS' Office of Protocol. Assistance is available through the Protocol Duty Officer on duty for the Office of Protocol or the Diplomatic Security Agent on duty. They can be contacted through the Diplomatic Security Command Center at (571) 345-3146 (open 24 hours a day). More information regarding this subject can be found at the following DOS link: http://www.state.gov/s/cpr/rls/dpl/. Valid Non-Immigrant Visas A-1, A-2, G-1, G-3, and North Atlantic Treaty Organization (NATO) 1-6 indicate possible status of immunity from criminal arrest or prosecution.

Chapter 8. ARREST PROCEDURES AND RELATED ISSUES

8.1 Arrest Defined

As stated in Section 3.2, an arrest is an actual or constructive restraint or detention of an individual performed with the purpose of taking the individual into custody. A detention may also be deemed an arrest if, based on the totality of the circumstances, a reasonable individual would believe himself or herself to be in custody. An arrest does not depend solely on whether the SA announces that the suspect has been placed under arrest. If an SA's conduct is more intrusive than an investigative stop, an arrest may take place. In determining whether an SA's conduct is tantamount to an arrest, consideration must be given to the relevant facts and circumstances, including but not limited to:

A. when and where the encounter occurred;

B. the duration of the encounter;

C. the number of SAs and other officers present;

D. what the SA(s) and the suspect said and did;

E. the use of weapons, handcuffs, a guard blocking the door, verbal commands, or other physical restraints;

F. the nature of the questioning;

G. whether SAs escorted the suspect to another location for questioning;

H. whether the SA(s) retained custody of important travel or identification documents during the encounter; and

I. whether the suspect was permitted to leave following the encounter.

HSI SAs are authorized to make arrests with or without an arrest warrant for criminal and administrative violations.

8.1.1 Criminal Arrest

A criminal arrest must be supported by probable cause to believe that the individual arrested has committed a criminal offense. Probable cause is articulable facts and circumstances that would lead a reasonably prudent person to believe that a criminal offense has been committed or is being committed by the individual to be arrested. Probable cause is more than mere suspicion, but less than absolute certainty of guilt.

In determining whether probable cause was present at the time of an arrest, courts consider the totality of the circumstances as viewed by a reasonably prudent SA, coupled with the SA's training and experience.

Pertinent factors include personal knowledge or observation by the SA; information contained in official communication to the SA; information from reliable informants, victims, or witnesses; actions and appearance of the suspect(s); criminal reputation of the suspects; inconsistent and unpersuasive answers to routine questions; and possession, disposal, or concealment of evidence.

Under certain circumstances where a suspect forcibly resists an arrest, the suspect could be arrested for a violation of 18 U.S.C. § 111 (Assaulting, resisting, or impeding certain officers), or 18 U.S.C. § 2231 (Interfering with an officer authorized to make a search).

8.1.2 Administrative Arrest

An SA has the authority to arrest an individual if the SA has reason to believe (consistently interpreted as requiring probable cause) that the individual is in violation of the Immigration and

Nationality Act (INA). An administrative arrest is initiated when the disposition of the case will be sought in civil proceedings rather than in a criminal court proceeding. This is most often associated with immigration proceedings.

8.2 Number of Officers Making an Arrest

Criminal and administrative arrests must be conducted by at least two law enforcement officers in order to ensure officer safety, except in unforeseeable, exigent circumstances. Cases where SAs respond to a duty call and there is a possibility that an arrest may be effected do not constitute an unforeseeable, exigent circumstance; therefore, SAs must adhere to the above requirement that at least two law enforcement officers conduct criminal and administrative arrests.

8.3 Foot Pursuits

SAs are authorized to engage in foot pursuits taking into consideration training and officer safety concerns. In addition, SAs should use the amount of force that is necessary and reasonable when stopping and apprehending an individual fleeing on foot, in accordance with the Interim ICE Use of Force Policy, dated July 7, 2004, or as updated.

8.4 Use of Restraints

The use of restraints on individuals in HSI custody must be conducted in a manner that is safe, secure, humane, and professional. Only the amount of restraint necessary and reasonable to ensure the safety of the SAs, the individual(s) in custody, the public, and/or to prevent escape shall be employed. Restraints shall not be used to inflict punishment or to restrict blood circulation or breathing. (Note: SAs should consult the Office of Firearms and Tactical Programs (OFTP) for questions regarding authorized restraining devices.)

8.4.1 Length of Time Restraints Are Used

All restraints are only temporary devices and should be removed when the individual in custody is placed in a secure holding facility and/or they are no longer required.

8.4.2 Method of Restraint

SAs shall handcuff (double-lock) all individuals in custody with their hands placed behind their back and the palms facing outward, unless a belly chain or transportation belt is used. If a belly chain or transportation belt is used on an individual in custody, the individual may be handcuffed in the front. Additionally, if necessary to ensure the security and safety of all, leg restraints should be used. An individual in custody who is in restraints must not be left unattended.

The SA is authorized to handcuff the individual in custody with his or her hands in the front without a belly chain, transportation belt, or other appropriate and approved restraining device(s) only if the individual in custody:

LE

Large individuals or those who are overly muscled such as weightlifters may require the use of several sets of handcuffs linked together. Flex-Cuffs or other specifically designed flexible police restraints may be used if necessary.

Individuals in custody shall not be handcuffed to an SA, officer, another person, or any object that may potentially cause an injury.

SAs may remove handcuffs from prisoners during processing only to facilitate the taking of fingerprints and to accommodate sanitation needs. Handcuffs may also be removed for medical emergencies when the circumstances dictate. Enhanced diligence is required during these times to ensure security and the safety of all.

8.4.3 Individuals to Be Restrained

Age, size, and sex are not valid reasons for failing to handcuff an individual. Juveniles may be handcuffed for officer safety.

Females shall be subject to the same handcuffing and restraint procedures used for males. (Also see Section 8.4.2(A).)

8.4.4 Aggressive Individuals

Combative individuals in custody may require the use of leg irons or other flexible restraints applied to prevent kicking by the individual.

Additional approved restraint devices may be used to secure an individual who violently resists arrest, poses a threat to officer safety, or who manifests mental disorders such that he or she presents a threat to himself or herself or to the public. (Note: SAs should contact OFTP for a list of authorized retraining devices.)

8.4.5 Transport of Individuals Using Restraints

Along with other considerations contained in this chapter, SAs should remember that, when using restraints, individuals in custody shall not be handcuffed to any moving vehicle or other conveyance. Furthermore, SAs must not transport individuals in custody who are restrained in a prone position. Individuals in custody shall never be left unsupervised in a vehicle or locked within a vehicle without supervision and appropriate ventilation. During transport, individuals in

custody are to remain restrained as described in Section 8.4.2. In circumstances where custody of an individual is turned over to other SAs for transport, the receiving SAs must search the individual regardless of any prior searches conducted by the arresting SAs or other law enforcement officers. (Note: See Chapter 9 for additional guidance on transporting individuals.)

8.5 Searches Incident to Arrest

There are two types of searches that must be conducted following each arrest: 1) an initial weapons search; and 2) a complete search.

8.5.1 Initial Weapons Search

A search for weapons should immediately follow handcuffing of any individual who may or may not be a suspect or prisoner.

Whenever possible, an SA or other officer of the same sex should conduct an initial weapons search of the individual being handcuffed and/or taken into custody. However, a frisk for weapons immediately following an arrest will not be delayed if an officer of the same sex is not available.

The discovery of a weapon or potential weapon during the search must be immediately communicated to the other officers at the scene of the encounter and/or to the members of the arrest team. The presence of one weapon suggests that other weapons might be present and calls for a heightened state of alertness by all personnel involved.

8.5.2 Complete Search

As soon as practical, a thorough search for evidence shall be conducted on the individual in custody. This search will not be limited as a result of an individual's objections, embarrassment, etc. A law enforcement officer of the same sex as the individual in custody should conduct this search if available; however, the search should not be unreasonably delayed due to the unavailability of a same-sex officer.

All property of the prisoner will be removed from him or her and secured in a plastic bag or other container. Special care should be given to document items of value. Currency should be counted in the presence of the individual in custody and another member of a law enforcement agency. If the prisoner was arrested while driving a vehicle, the vehicle will also be searched incident to arrest and detained in furtherance of the arrest. During an arrest that is made in a room or building, SAs may conduct a search of the immediate area to ensure officer safety only. Any evidence of a crime observed may be seized under the plain view doctrine. Any evidence found on the individual in custody should be kept separately from any items that do not have evidentiary value.

The prisoner will be afforded the opportunity to relinquish all personal property to a third party, either in person or by mail. This transaction will be recorded on a Department of Homeland

Security (DHS) Form 6051R, "Receipt of Property." If this cannot be accomplished, the prisoner will be afforded the opportunity to abandon his or her property. Prisoners must be informed and understand that if they abandon the property, they will have 30 days during which to recover their property, after which the property may be destroyed. This transaction will be recorded on DHS Form 4607, "Notice of Abandonment and Assent to Forfeiture of Prohibited or Seized Merchandise," and, as needed, DHS Form 4613, "Order to Destroy and Record of Destruction of Forfeited, Abandoned, or Unclaimed Merchandise."

LE

The searching officer and others present must take precautions to prevent the spread of infectious diseases from the prisoner(s). The use of protective gloves to prevent contact with bodily fluids is strongly recommended.

8.5.3 Search of Cell Phones Incident to Arrest

SAs may discover cell phones and other smartphone devices during the search incident to arrest. In order to conduct a search of a cell phone upon arrest, SAs must either secure a warrant before searching the content of the cell phone or rely on another exception to the warrant requirement, such as consent, exigent circumstances, or plain view. If timing and circumstances permit, SAs should consider obtaining an anticipatory search warrant for a suspect's cell phone(s). SAs may still seize a cell phone during a lawful arrest, and may still examine the physical aspects of the phone to ensure that it will not be used as a weapon, including, for example, searching between the phone and its case for a razor blade. For further details, reference is made to the U.S. Supreme Court decision in Riley v. California, 134 S. Ct. 2473 (2014), holding that law enforcement officers must generally secure a warrant before conducting a search of a cell phone incident to arrest.

Since a search authorized by consent is wholly valid, SAs should always request consent (in writing, if possible) to search the contents of a cell phone of an individual who is arrested. If consent is not secured, exigent circumstances may still justify a search. Emergencies such as texts that are sent to armed and dangerous accomplices or location data of missing children in an abductor's cell phone could qualify as exigent circumstances and justify warrantless searches of cell phones upon arrest. However, such searches should be limited to addressing the exigency, and should not be used as a means to collect evidence

LE

LE

(Note: For guidance on searches of other electronic devices, SAs should see the Search and Seizure Handbook (HSI HB 12-04), dated September 14, 2012, or as updated.)

8.6 Smoking

Individuals in custody will not be allowed to smok LE LE At the discretion of the arresting SAs and once the individuals in custody are in a secure location that allows smoking, SAs may choose to allow them to smoke as part of the interviewing techniques. Individuals in a detention cell will not be allowed access to smoking materials.

8.7 Threat from Third Parties

SAs and other officers should take into consideration the potential threat from third parties that could cause harm to the SAs, officers, and/or the individual(s) in custody. SAs or other officers must be assigned to concentrate on the individual(s) in custody while others remain alert for third party threats.

8.8 Hostile Environments

In hostile environments, any and all individuals in custody must be removed as quickly as possible to a safe place. Individuals in custody must not be used as shields by SAs or other officers present during the completion of the law enforcement operation.

8.9 Safety for Individuals in Custody

SAs should not engage in any enforcement activities while they have an individual in custody unless failure to act at the immediate moment would risk death or serious bodily injury to oneself or another person. In both life threatening and non-life threatening yet serious situations, SAs should attempt to call for back-up assistance if practicable and SAs may remain on hand until such assistance has arrived. Regardless, SAs must maintain the safety of individuals in custody at all times.

8.10 Immunity from Arrest

Individuals who have immunity from arrest are:

A. Diplomats who are accredited to the United States or their family members (with the exception of U.S. nationals). (See Section 7.11.)

B. Diplomats accredited to a foreign country or their family members who are directly en route between their home country and the country of accreditation. (Note: Mere possession of a diplomatic passport does not confer diplomatic immunity.) (See Section 7.11.)

C. Sitting judges while court is in session.

D. Members of Congress during their attendance at sessions of Congress, or while traveling to or from a session may be arrested but may not be otherwise detained. (Note: Immunity from arrest is a privilege; members of Congress can be detained and/or arrested when Congress is not in session.)

8.11 Arrest of Foreign Nationals

The arrest of foreign nationals requires certain actions depending on their nationality, immigration status in the United States, and where the arrest took place. If the individuals are aliens, they have the right to speak to their consular officer. (See ICE Directive 10066.1 (former number: 7-3.0), entitled "Consular Notification of Detained or Arrested Foreign Nationals," dated February 13, 2006, or as updated.)

8.11.1 Right to Communicate with Consular Official

An alien who is being detained must be notified that he or she may communicate with a consular official in accordance with Title 8, Code of Federal Regulations (C.F.R.), Section 236.1(e). If an alien is a national of one of the countries listed in 8 C.F.R. § 236.1(e), a consular official of that country must be notified, even if the alien specifically requests that no notification be made. SAs must not reveal to any consular official the fact that the alien may have requested asylum.

8.12 Statement of Rights

8.12.1 Miranda Warning Following a Criminal Arrest

Following a criminal arrest and prior to questioning beyond what is needed for identification or processing purposes, individuals in custody must be informed that anything they say may be used against them and that they have the right to remain silent, to consult with a lawyer, to have a lawyer present during questioning, and, if indigent, to have counsel appointed. The purpose of these warnings, commonly termed Miranda warnings, is to provide an individual in a custodial setting with notice of Fifth and Sixth Amendment rights available to that person prior to their interrogation. Absent exigent circumstances, Miranda warnings should be conducted in writing using ICE Form 73-025, "Statement of Rights," used for criminal cases. (Note: For additional information on Miranda warnings and on the definitions of "interview" and "interrogation," see OI HB 10-03, Interviewing Techniques Handbook, dated April 28, 2010, or as updated.)

8.12.2 Notice of Rights Warning Following an Administrative Arrest

Every apprehended individual charged with a violation of the INA must be given an administrative notice of rights, including the right to communicate with the alien's respective consular official as stated in Section 8.11.1. ICE uses multiple forms for this purpose as a result of decisions in certain court cases. Salvadorans are given a Notice of Rights to Salvadorans (DHS Form I-848), juveniles are given the Notice of Rights and Request for Disposition (DHS Form I-770), which is a simplified version, and all others are given DHS Form I-826, which bears the same title as DHS Form I-770. As part of the processing procedure of an apprehended alien, SAs must provide a copy of the appropriate form and make sure that the alien understands these rights.

Each of the rights forms contains a section for recording a decision by the apprehended alien to accept voluntary departure and immediate return, under appropriate safeguards, in lieu of formal removal proceedings.

8.13 Juveniles

8.13.1 Criminal Arrest of Juveniles

Juveniles require special handling as established in 18 U.S.C. § 5031 *et seq.* SAs must immediately notify the U.S. Attorney of the criminal arrest. If prosecution is authorized, the following steps must be taken:

A. SAs must advise juveniles of their Miranda rights using language the juveniles can understand.

B. The parents or guardian of the juvenile must immediately be notified of the nature of the charges and of the juvenile's rights.

C. Juveniles must immediately be brought before an appropriate legal authority, e.g., a magistrate, a judge, etc., for their initial appearance.

D. SAs must not release the name of the juveniles, fingerprints, photographs, or any reports of information about the juveniles to anyone other than as authorized by 18 U.S.C. § 5031 *et seq.* or by order of the court.

E. Juveniles 14 years old and older should be fingerprinted and photographed. Those under 14 should not.

8.13.2 Administrative Detention of Juveniles

Aliens who are defined as minors should be treated in accordance with the *Flores v. Reno* Settlement Agreement which sets nationwide policies for the detention, release, and treatment of juveniles in ICE custody. At the earliest opportunity, coordination and notification should be made with the appropriate local Enforcement and Removal Operations (ERO) office for the disposition of the juvenile(s).

The appropriate foreign consulate must be notified in the event that a minor is taken into custody by HSI who is not accompanied by a parent, family member, or legal guardian.

Chapter 9. TRANSPORTATION PROCEDURES AND RELATED ISSUES

9.1 General Guidelines for Transporting Individuals in Custody by Motor Vehicle

Transporting an individual can be one of the most dangerous undertakings that SAs will encounter. The hazards and problems that they may encounter are countless. When considering the transportation of one or more restrained individuals, SAs must take into account:

A. The nature of the charge;

B. The name, address, history, etc. of the individual(s);

C. The kind of vehicle that will be used for the transportation – for example, caged or not caged;

D. The number of SAs involved in the transportation;

E. The number of individuals to be transported;

F. Possibility of injury to the individual(s) or the SAs;

G. The time that will elapse during the time of transportation; and

H. Whether the individual(s) was/were compliant prior to being restrained.

SAs should determine whether the need to immediately transport the individual(s) outweighs the danger if the SAs were to wait and call for a different vehicle or a back-up unit. Individuals in custody shall be transported in a government vehicle.

LE

Whenever possible, at least one of the SAs shall be of the same sex as the individual(s) in custody. Female and male individuals should be separated during the transportation, if possible.

If possible, juveniles should be transported within the same vehicle as their parent or guardian if the parent or guardian is also in custody. (Note: For specific questions regarding juveniles, SAs should contact ERO's Juvenile Family Residential Management Unit.)

9.2 Number of Officers Transporting an Individual in Custody

In order to ensure officer safety, at least two law enforcement officers must transport an individual in custody, except in unforeseeable, exigent circumstances. This requirement applies regardless of whether it is for criminal or administrative offenses, and regardless of the means of transportation. If a vehicle is used, this should be accomplished by having two officers in the same vehicle. Utilizing two vehicles to transport one individual in custody should not be employed without first obtaining supervisory approval unless exigent circumstances clearly prevent this approval from being obtained.

When utilizing a prisoner transport van to move more than one individual in custody, a minimum of two officers must be involved. Supervisors have the discretion of assigning additional vehicles to follow the transport van for officer safety concerns.

(Note: See Section 9.12 for guidance on transporting prisoners via a commercial air carrier.)

9.3 Securing Weapons

SAs shall take measures to secure their handguns in an OFTP-defined and approved holster. Long guns shall be secured using an approved retention device for long guns. This will ensure that individuals in custody cannot gain access to the SAs' weapons during the transportation.

9.4 Use of Restraints Prior to, During, and After the Transportation

The use of restraints will be in accordance with Section 8.4 of this Handbook.

9.5 Vehicle Search and Child Safety Locks

All vehicles to be used in the transportation of individuals in custody should be searched for weapons, evidence, and any item that can inflict injury or be used by the individual(s) to aid an escape. This search should be done before the individuals in custody are placed in the vehicle and again immediately after they are removed from the vehicle. When transporting individuals in custody, SAs or other law enforcement officers should activate the vehicle's child safety locks if the vehicle is so equipped.

9.6 Seating of Individuals in Custody

Individuals should be transported in a manner that allows for constant visual observation. The seating of SAs, other law enforcement officers, and individuals in custody should be as follows:

A. Individuals in custody shall always be seated in the back seat of a vehicle and safety

LE

9.7 Transporting Juveniles

Juveniles should not be transported in the same area of a vehicle with adult individuals, unless the juveniles are being transported along with their parent(s) or guardian(s).

9.8 Use of Restrooms During the Transportation

Individuals in custody must be afforded the opportunity to utilize restroom facilities during the transportation only if:

A. the time in transit to reach the final destination is substantial; and

B. the use of the restroom can be accomplished in a safe and secure manner.

9.9 Medical Considerations

The physical well-being of individuals in custody should be monitored during transit. Particular attention should be directed to individuals reported or suspected of being under the influence of drugs and/or alcohol or who have a history of, or propensity for, violence.

Individuals in custody who report/display symptoms of serious illness during transit should immediately receive medical attention by a medical professional LE

LE

LE any deviation during the transit of the individuals in custody should immediately be reported to management. (Note: See Section 9.11 for instructions on required communications during the transportation of individuals in custody.)

Symptoms or reports of physical or mental illness, such as threats of suicide or psychotic behavior, should be reported to all SAs or other law enforcement officers involved in the processing of the individuals in custody.

9.10 High Risk Individuals

Special precautions should be employed when transporting high risk individuals.

A. Belly chains and leg irons should be employed in addition to handcuffs.

B. Rival gang members should not be transported together.

SAs should consider having a second vehicle (with additional SAs or other law enforcement officers) follow to render immediate assistance.

9.11 Required Communications

LE

LE

9.12 Transportation of Prisoners Via Commercial Air Carrier

General safety precautions remain when transporting prisoners via commercial air carrier; however, the Federal Aviation Regulations (F.A.R.) have specific guidelines related to the transportation of prisoners. SAs and management need to be aware that not every airline will allow prisoners onboard. Furthermore, for those airlines which allow for the transportation of prisoners, the aircraft captain is the final authority and may refuse boarding for the prisoner. It is recommended that, if possible, SAs and supervisors explore other transportation options prior to deciding to utilize commercial air services.

The F.A.R. limit the type of prisoners onboard a commercial aircraft, the number of prisoners, and the officer-to-prisoner ratio. SAs transporting prisoners via commercial aircraft must have completed the "Law Enforcement Officers Flying Armed" course.

SAs must determine whether the prisoner is considered high risk or low risk prior to contacting the commercial air carrier

LE

In order to transport a prisoner onboard a commercial aircraft, SAs must notify the airline at least 24 hours prior to the departure or, if not possible, as far in advance as possible of the identity of the prisoner, the proposed flight number, and whether the prisoner is high risk or low risk.

SAs should arrive at the airline check-in counter at least 1 hour prior to the scheduled takeoff, or as advised by the airline. The SAs will be required to assure the airline personnel that each prisoner has been searched and does not have on or about his or her person or property anything that can be used as a deadly or dangerous weapon.

Prisoners shall remain handcuffed at all times during the transportation. LE

LE

Food and beverage will not be served to the prisoner without the authorization of the escorting SAs. If a meal is anticipated, SAs should confirm the type of eating utensils provided and, if necessary, bring plastic eating utensils with them. Prisoners will not be given metal eating utensils. (Note: If the decision is made to feed the prisoner prior to boarding the airline, SAs should confirm that the prisoner has returned all metal eating utensils provided to him or her.) Neither the prisoner nor the escorting SAs will be served alcohol.

Prior to boarding the aircraft, one of the escorting SAs shall contact the NLECC and provide the flight information, scheduled departure and arrival times, and the identity of the prisoner. Prior to the announcement that the cabin door is being closed, one of the SAs will update the NLECC with the departure time. Upon landing, one of the SAs will again notify the NLECC with the landing time and arrival gate information, if known.

(Note: SAs should also see Part 1, Section D of the Interim ICE Firearms Policy, dated July 7, 2004, or as updated.)

9.13 Outside Enforcement Activities

LE

LE

Chapter 10. BOOKING PROCEDURES

The arrest of an individual is not complete until he or she has been properly "booked" in the ICE Enforcement Integrated Database Arrest Graphic User Interface for Law Enforcement (EAGLE) and turned over to a law enforcement detention facility. (See HSI Directive 14-01 entitled, "Mandatory Booking of Arrestees Using EAGLE," dated April 23, 2014, or as updated.) Examples of such facilities would be a county jail or a Federal detention facility. This type of facility should not be confused with a holding cell in either an HSI office or a U.S. Customs and Border Protection port of entry. SAs are responsible for the individual until they have turned him or her over to the U.S. Marshals Service (in the case of an arrest on Federal offenses) or a State or local authority (in the case of an arrest on State or local offenses).

Detention facilities will generally accept only individuals in good health. If the individual has been injured and needs immediate medical attention or has a pre-existing injury or health condition (e.g., a heart condition or cancer), SAs should coordinate with their Group Supervisors to determine if the individual can be turned over to a detention facility or if another option can be identified.

Symptoms or reports of physical or mental illness, such as threats of suicide or psychotic behavior, should be reported to all SAs or other officers involved in the processing of the individuals in custody.

SAs should consult with their Group Supervisors regarding the specific process and procedures for booking individuals in their SAC's AOR. SAs must be familiar with local procedures as they may vary greatly between each jurisdiction or location. SAs are required to use Federal Bureau of Prisons Form BP-a377, "Prisoner Remand," to document the arrest of individuals arrested for violating Federal law. (Note: Since many SACs' AORs cross State and county lines, there may be many different procedures within just one SAC's AOR.)

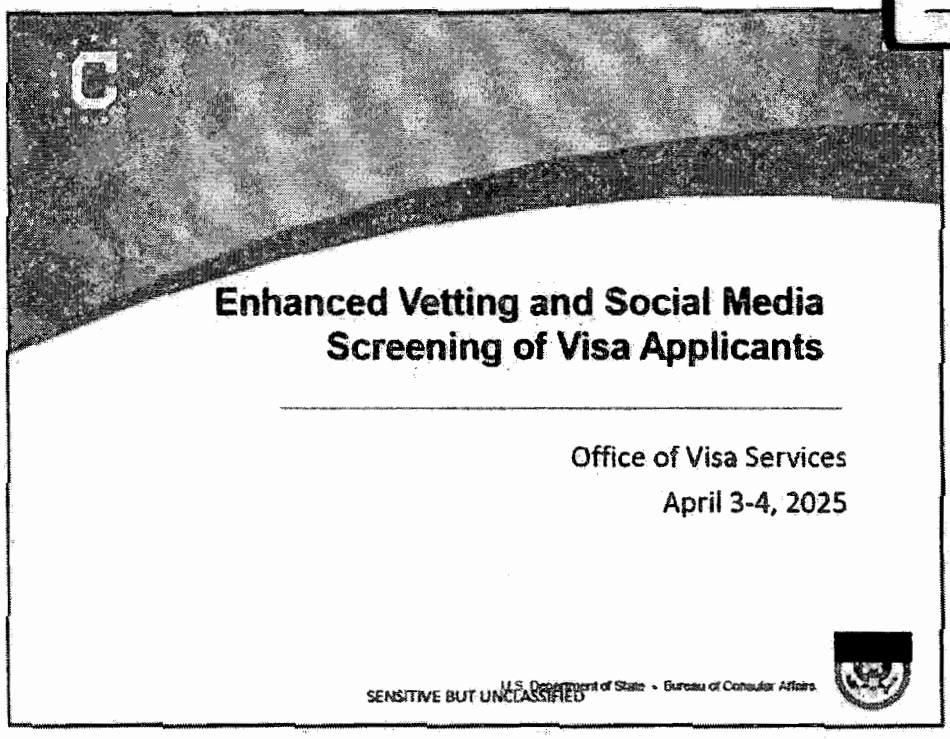
Appendix A

ACRONYMS

AOR	Area of Responsibility
C.F.R.	Code of Federal Regulations
DHS	Department of Homeland Security
DOS	Department of State
EAGLE	Enforcement Integrated Database Arrest Graphic User Interface for Law Enforcement
ERO	Enforcement and Removal Operations
F.A.R.	Federal Aviation Regulation
FOUO	For Official Use Only
HB	Handbook
HSI	Homeland Security Investigations
ICE	U.S. Immigration and Customs Enforcement
INA	Immigration and Nationality Act
NATO	North Atlantic Treaty Organization
NLECC	National Law Enforcement Communications Center
OFTP	Office of Firearms and Tactical Programs
OI	Office of Investigations
SA	Special Agent
SAC	Special Agent in Charge
U.S.C.	United States Code

EXHIBIT 49

CONFIDENTIAL - SUBJECT TO PROTECTIVE ORDER

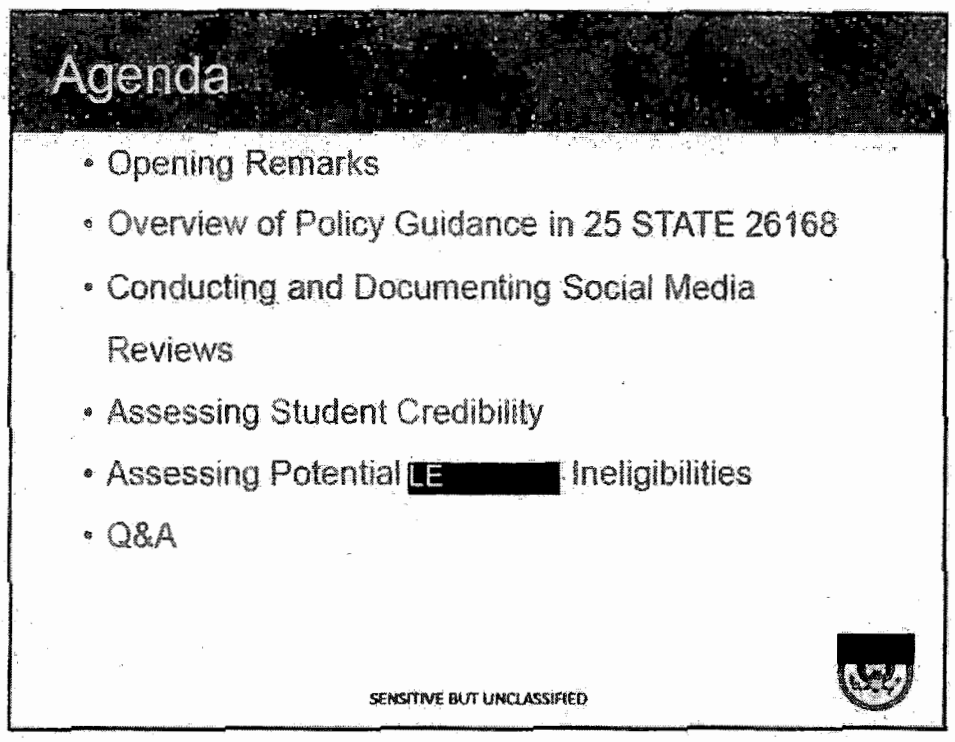


[redacted] – welcome to VO Webinar on…

Introduce self + participants (MD [redacted], [redacted] of CA/[redacted] [redacted] of VO/SAC, [redacted] [Thurs]/[redacted] [Fri] of L/CA)

First/second of two identical webinars, will not be recorded

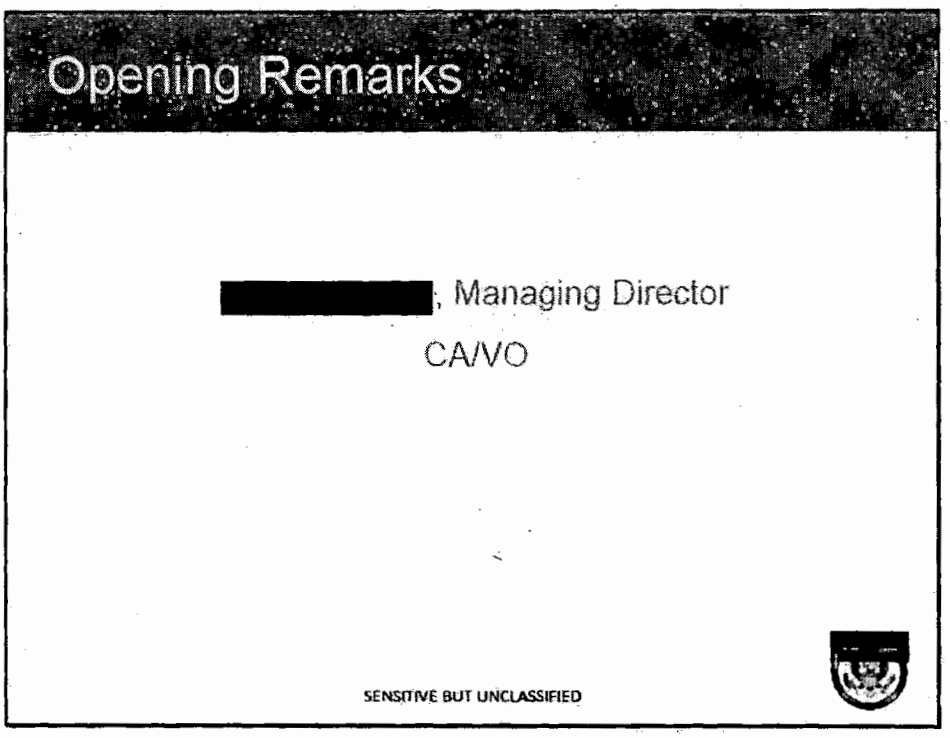
As a reminder, please be sure you are muted.



[redacted] to run through agenda

I know there are a lot of questions about this process and we hope to answer many of them along the way.

turn it over to MD [redacted]



MD[redacted]

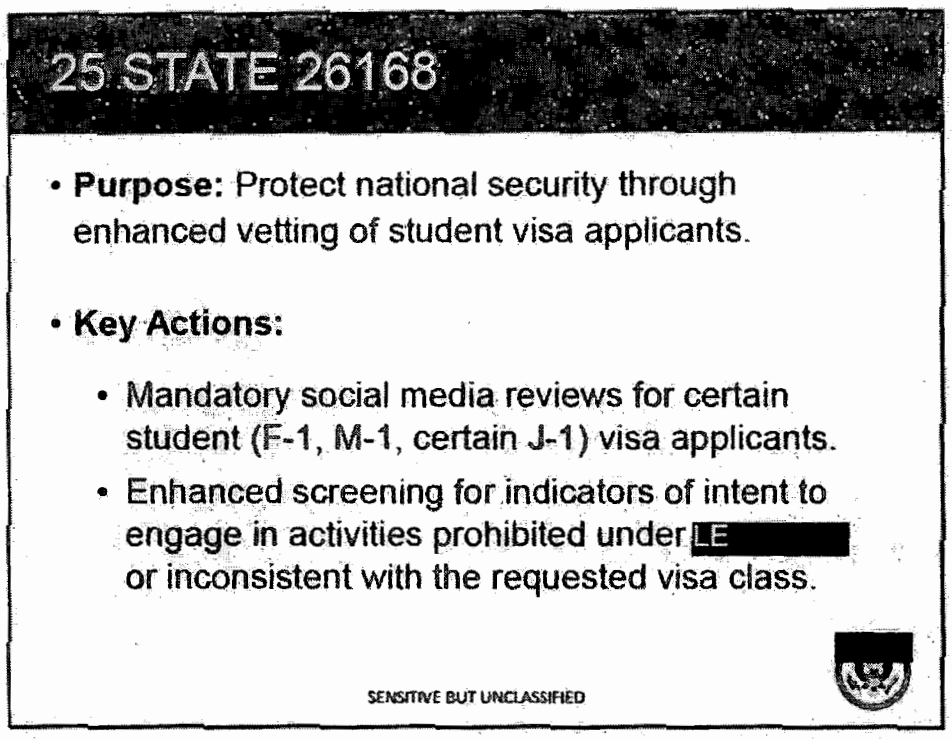
Secretary Rubio – March 16, 2025

"If you tell us when you apply for a visa, 'I'm coming to the U.S. to participate in pro-Hamas events,' that runs counter to the foreign policy interests of the United States…We don't want people in our country that are going to be committing crimes and undermining our national security or the public safety. It's that simple."

SENSITIVE BUT UNCLASSIFIED

[redacted]

This guidance is part of our implementation of Executive Orders 14161 and 14188 aimed at protecting the U.S. from foreign terrorists, supporters, and other threats as well as combatting antisemitism. As Secretary Rubio has said, engaging in activities that advocate for terrorist activity or organizations is contrary to our foreign policy and national interests.

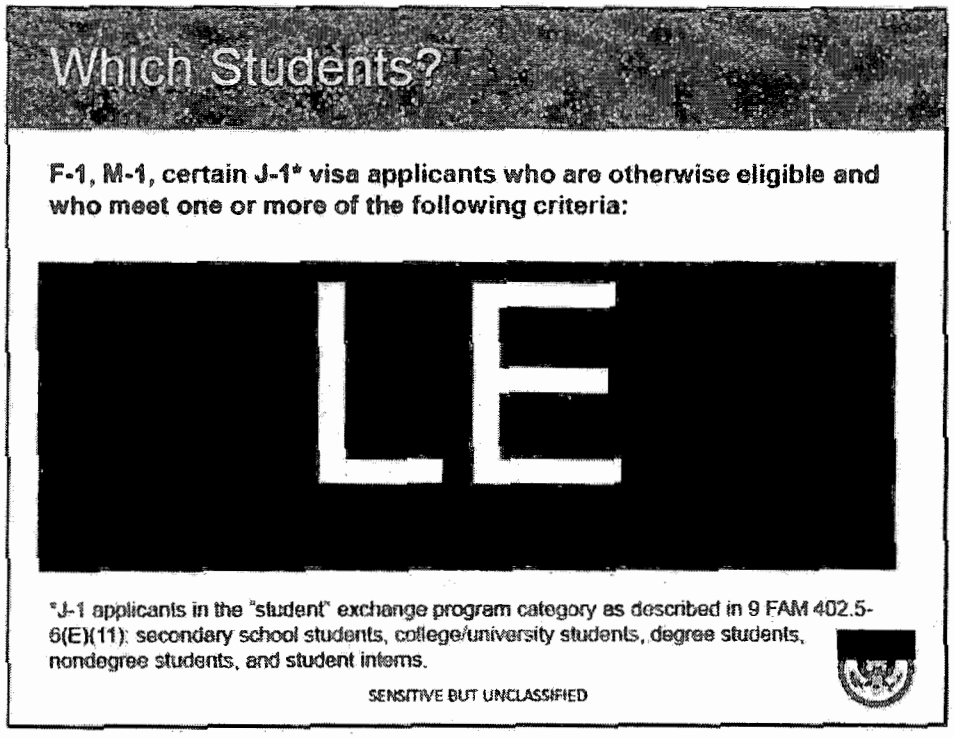


[redacted]

The guidance that we put out in 25 STATE 26168 is the preventative piece of this policy – ensuring that we address any derogatory information related to intent to engage in prohibited activities or those that are inconsistent with the visa status. Any applicant who has not demonstrated to your satisfaction that they meet all of the standards required by their visa classification should be refused.

As part of this screening effort, Consular officers must refer specific student visa applicants to the LE [redacted] for social media checks. Consular officers should then use the information obtained by the checks as part of their assessment of the totality of the applicant's circumstances.

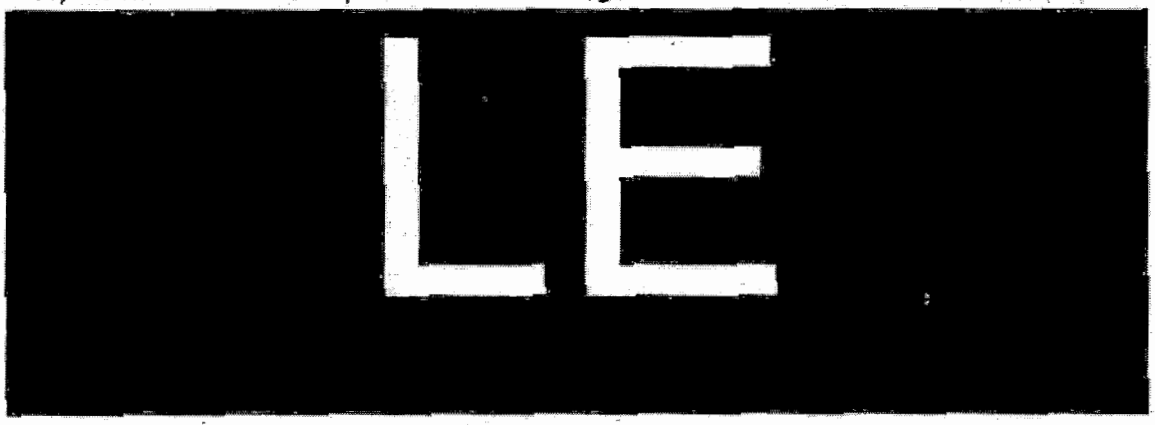
In the next slide, we'll discuss which students are included in this requirement.



[redacted]

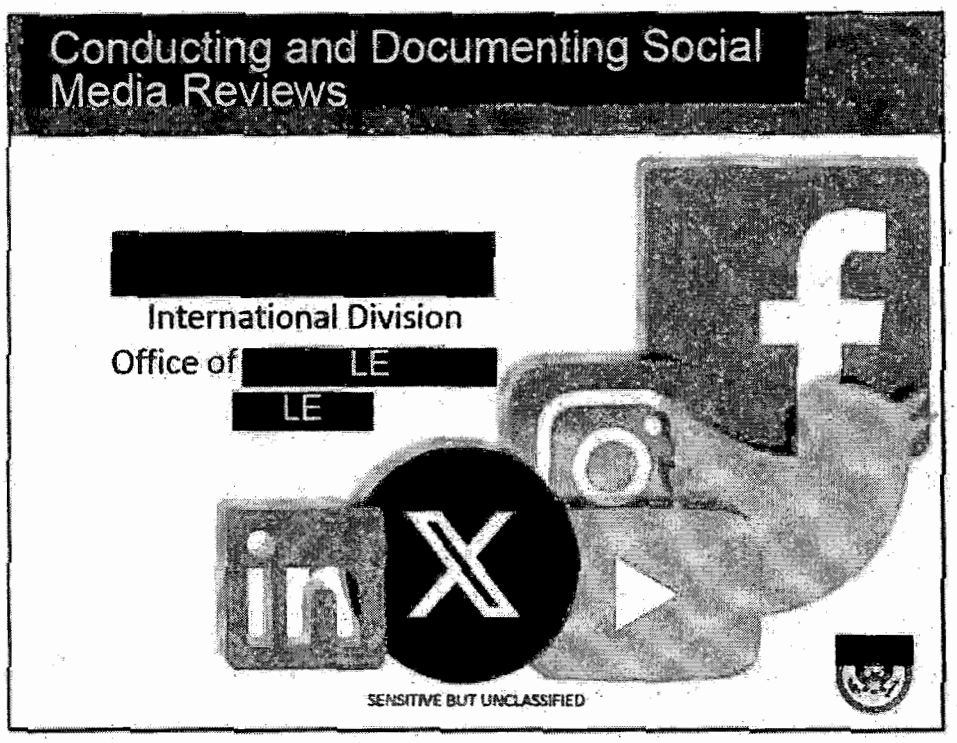
By "students" we mean F-1, M-1, and J-1 applicants in the "student" category of exchange programs as noted at the bottom of the slide. The social media review is not mandatory for J-1 applicants who *happen* to be students but are applying for other exchange programs such as au pair or SWT.

So, this universe of students, who are otherwise eligible and meet one or more of the three criteria:

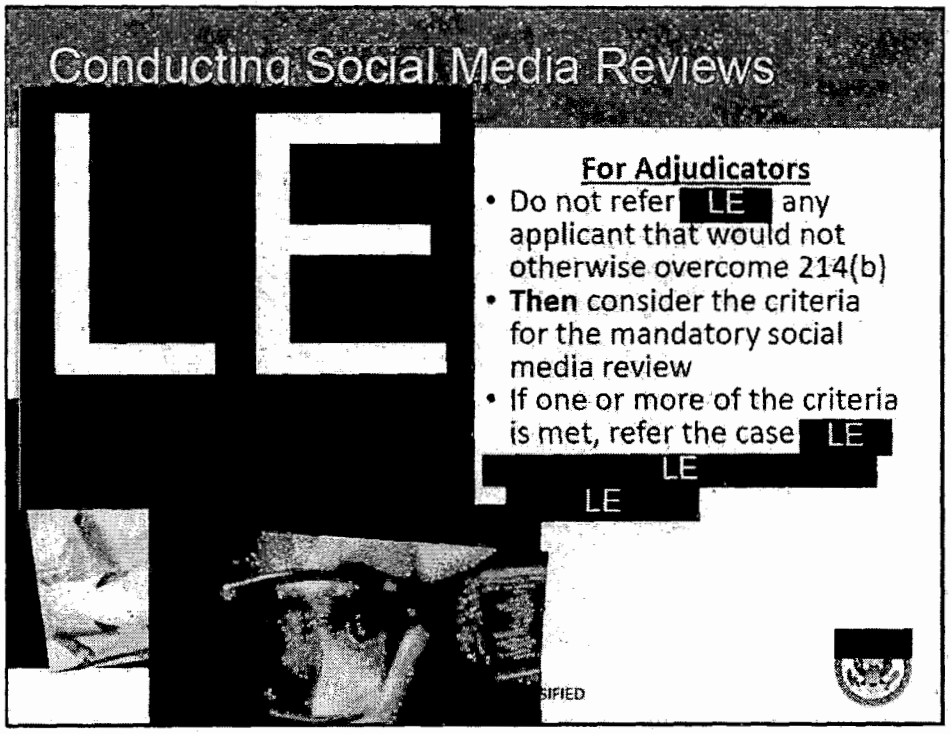


Remember that social media reviews are only for applicants who are otherwise eligible for the visa. If you've already determined they don't overcome 214(b), that's the end of the road for them.

Now moving on from which applicants to review, we'll talk about how to conduct and document the review. I'll turn it over to [redacted] from LE.

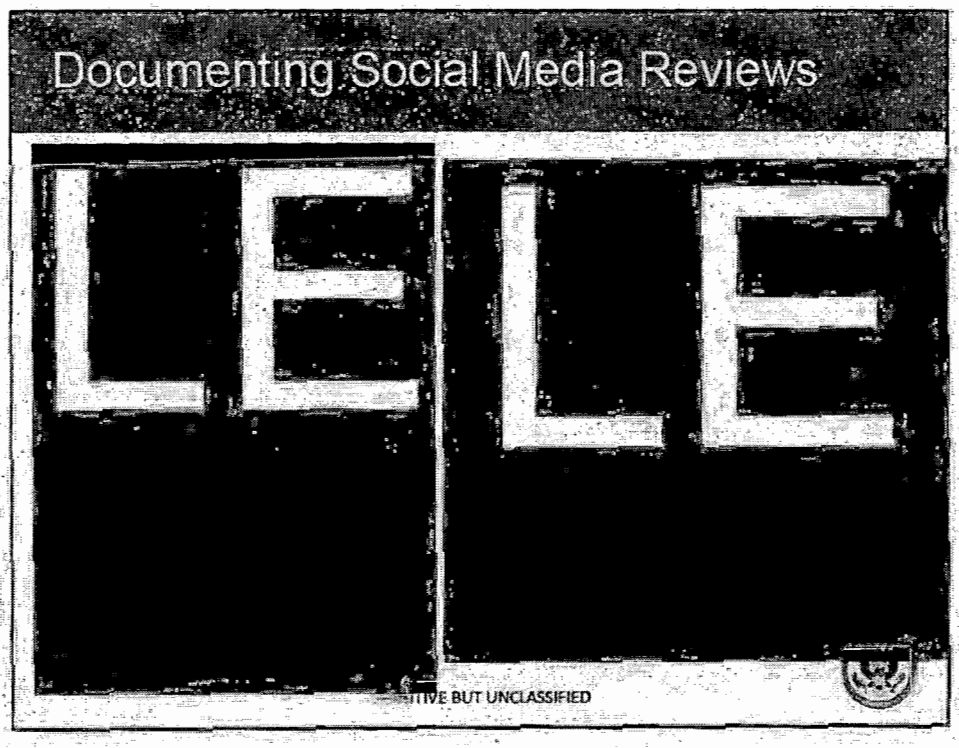


CA/LE [redacted]



CA/LE

CA/LE [redacted]

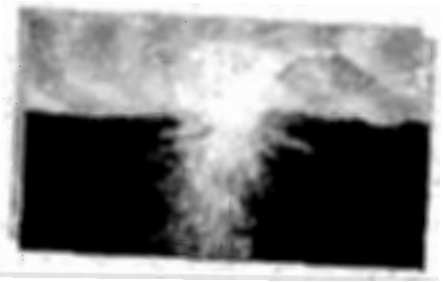


CA/LE [redacted]

Documenting Social Media Reviews

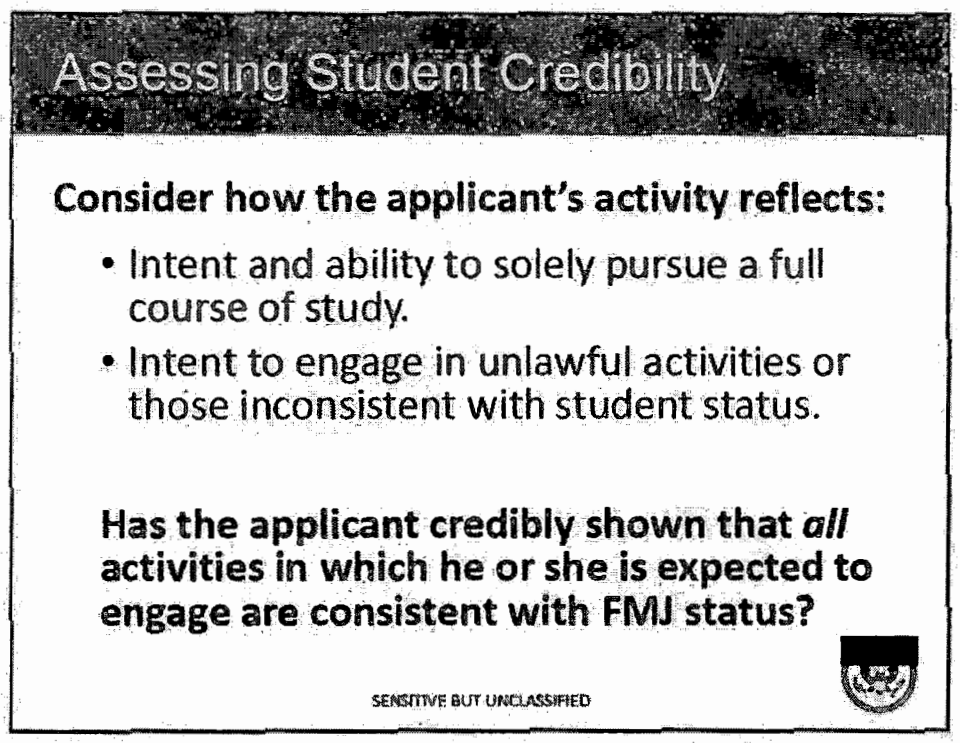
Road ahead

- Refining guidance for searching specific social media platforms
- Want to hear your best practices
- Reach to LE LE with any questions about conducting or documenting social media reviews



SENSITIVE BUT UNCLASSIFIED

CA/LE



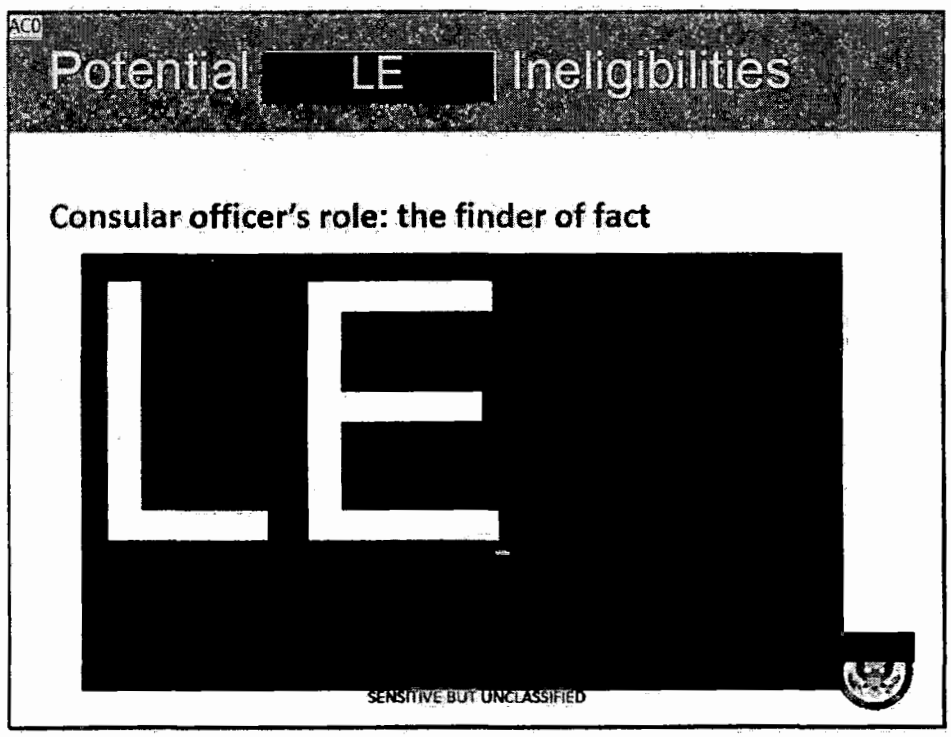
[redacted] Now, turning to what consular officers should do with the results of the social media review.

We've received a few questions about what activity should or should not be considered derogatory. Broadly speaking, you should look for any information that impacts the applicant's eligibility for the visa – [redacted]

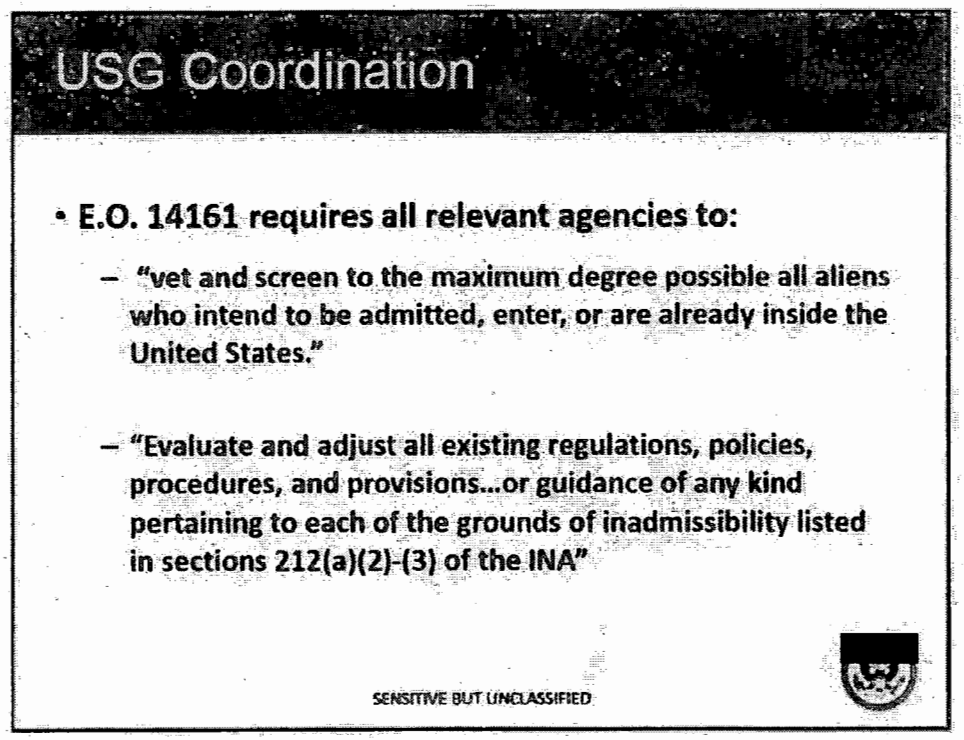
The FAM requires that an F-1 or M-1 applicant must demonstrate intent to enter the United States solely to pursue a full course of study. Relatedly, J-1 applicants for student programs are required to pursue a full course of study.

[redacted]

For applicants whose activities may rise to a higher level, I'll turn to [redacted] of L/CA and [redacted] of VO/SAC to talk about assessing applicants for [redacted] ineligibilities.



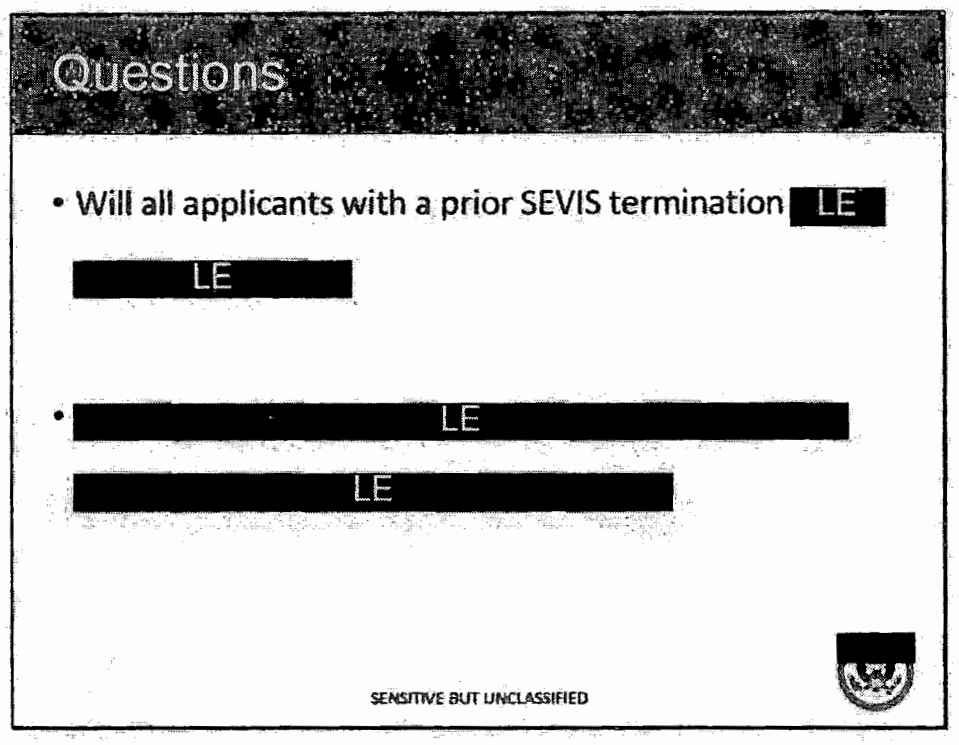
L/CA and SAC



[redacted] We received a few questions related to DHS's involvement in the enhanced vetting procedures, whether that's through screening at the POE or in the removal process. EO14161 tasks all relevant agencies to evaluate their policies and procedures to ensure maximum vetting.

We have been working closely with DHS on several lines of effort related to vetting and information sharing. As one example, we've established a Student Visa Working Group to facilitate information flow and coordinate actions on individuals with derogatory information.

While we won't get into depth today on these efforts, we wanted to reassure you that CA is not doing this alone – we are closely coordinating with our partner agencies on enhanced vetting efforts.



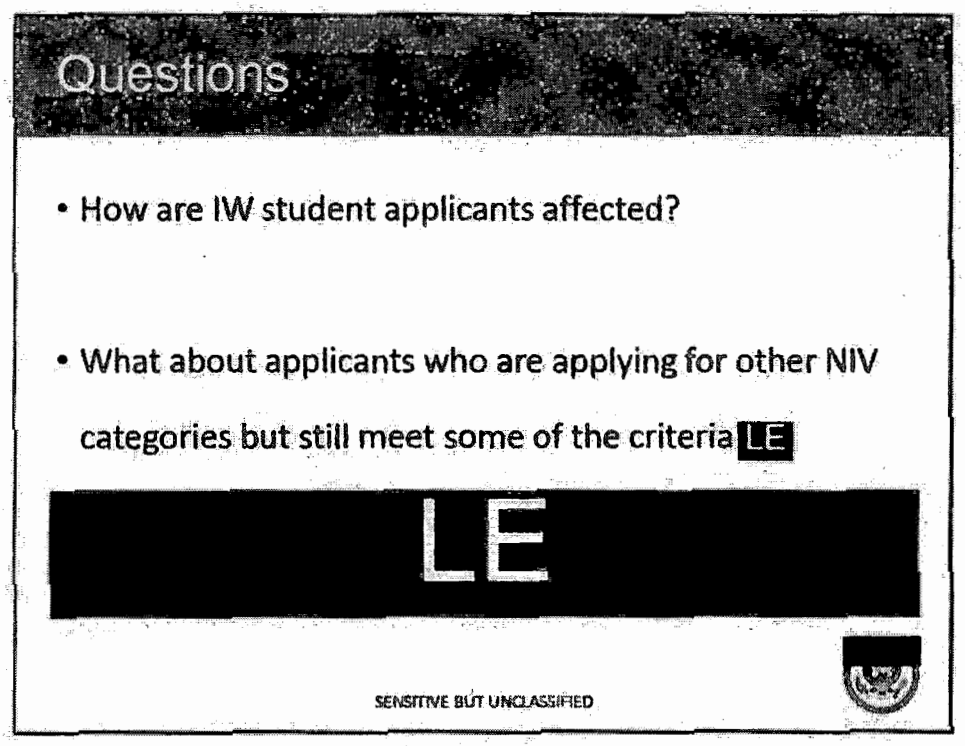
We're going to dig into the Q&A portion of the webinar, starting with questions that were submitted by posts ahead of time. Similar questions have been combined in the interests of time.

1. VO/F : LE

LE

2. VO/F : LE

LE



1. VO/F [redacted] : [redacted] F

LE

2. VO/F [redacted]: You aren't limited to conducting social media checks for only student visa applicants. While the social media check is mandatory for student visa applicants who fall into the criteria, if you have doubts about any applicant's activities during their previous stay as a student, and you otherwise intend to issue, post should conduct a social media review to help you assess the totality of the applicant's circumstances.

Questions

- Can LE Staff conduct the social media review?
- What social networks are we allowed to check? Is Tiktok ok?
- What if the account is set to private?

SENSITIVE BUT UNCLASSIFIED

Back over to [redacted] for a few questions about the social media review process.

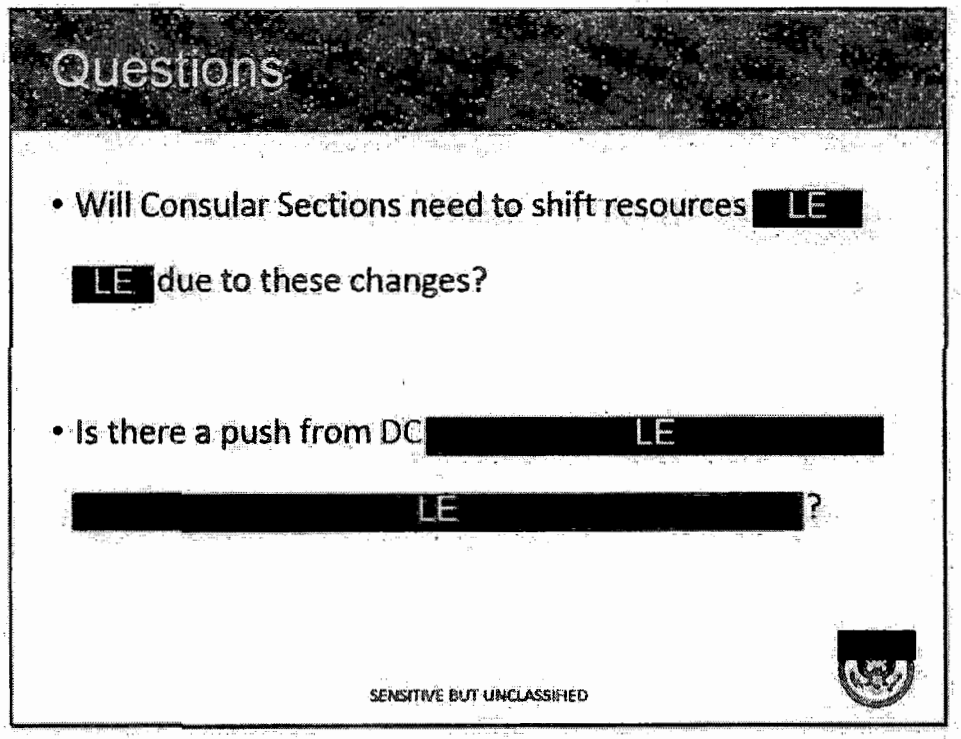
Questions

- How should we handle applicants who don't provide accurate/any social media information?

SENSITIVE BUT UNCLASSIFIED

VO/F [redacted]:

1. [redacted] LE



1. VO/F : LE
LE

2. VO/F : LE
LE

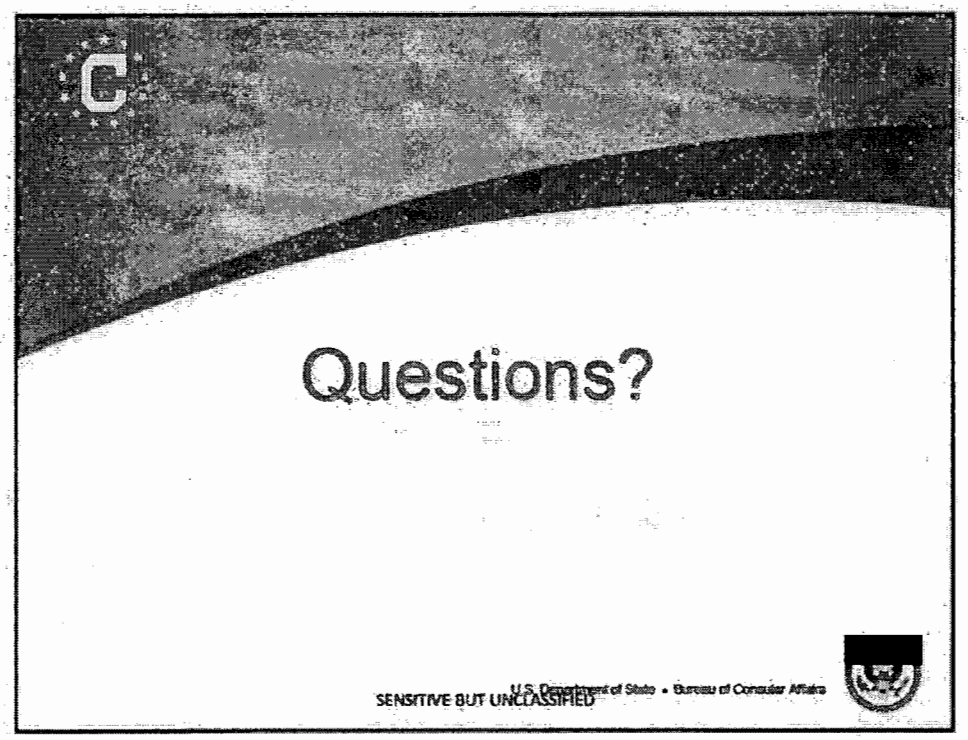

Questions?
SENSITIVE BUT UNCLASSIFIED
U.S. Department of State • Bureau of Consular Affairs

EXHIBIT
50

UNCLASSIFIED
SBU

MRN:	25 STATE 45612
Date/DTG:	May 15, 2025 / 151708Z MAY 25
From:	SECSTATE WASHDC
Action:	ALL DIPLOMATIC AND CONSULAR POSTS COLLECTIVE *Routine*
E.O:	13526
TAGS:	CVIS, CMGT, KCSY
Captions:	SENSITIVE
Reference:	A) 25 STATE 17178 B) 25 STATE 5914
Subject:	Caught and Revoked: Updated Guidance on Systems Messages

1. (SBU) **SUMMARY**: E.O. 14161 states to "protect Americans the United States must be vigilant during the visa-issuance process to ensure that those aliens approved for admission into the United States do not intend to harm Americans or our national interests. More importantly the United States must identify them before their admission or entry into the United States." Thanks to consular sections' LE [redacted] LE, visa revocation actions increased by 200 percent in the week following the action request (REF A). To help posts continue to focus resources on priority cases and protect U.S. borders, [redacted] LE [redacted] This cable also serves to correct an error in the original request (REF A), which incorrectly stated that INA 222(g) does not apply to overstays of fewer than 180 days. INA 222(g) renders void an NIV on which an alien entered if that alien remains beyond the period of authorized stay. The alien does not have to have remained more than 180 days beyond the period of authorized stay for INA 222(g) to apply (see 9 FAM 302.1-9). **END SUMMARY.**

A LEG UP FROM WASHINGTON

2. (SBU) [redacted] LE [redacted]

3. (SBU) [redacted] LE [redacted]

LE

Before	Removed	After	Percentage
[redacted] LE [redacted]			

*Contact your VO/F analyst and/or your RCO if you need specific data for your post.

4. (SBU) This initial sweep addressed the backlog of system messages. New messages in these categories will continue to accumulate. [redacted] LE [redacted]

5. (SBU) Following the transmission of REF A on March 1, [redacted] LE [redacted] to protect U.S. borders and Americans in the weeks following REF

A. This focused work resulted in an immediate doubling in visa revocations for aliens who no longer qualify for their visas, and a sustained 150 percent increase in visa revocations as compared to March 1-April 15, 2024.

VISA REVOCATIONS PORTAL

6. (SBU) With the migration of CAWeb, there is a new link to the Visa Revocations Portal containing the new template spreadsheet for bulk prudential revocation requests, links to 9 FAM revocation sections, and the email address of the VO/SAC revocations team where requests should be sent. There is also helpful guidance on what to consider when submitting revocation requests and tips.

ADDRESSING LE RECORDS

7. (SBU) [redacted]

LE

FURTHER GUIDANCE

8. (U) Please contact your VO/F analyst with questions on this effort. Please contact LE with questions about prudential revocations.

Signature:	RUBIO
XMT:	BASRAH, AMCONSUL; CARACAS, AMEMBASSY; CHENGDU, AMCONSUL; KABUL, AMEMBASSY; MINSK, AMEMBASSY; SANAA, AMEMBASSY; ST PETERSBURG, AMCONSUL; VLADIVOSTOK, AMCONSUL; YEKATERINBURG, AMCONSUL

UNCLASSIFIED
SBU

EXHIBIT 51

UNCLASSIFIED
SBU

MRN:	25 STATE 17178
Date/DTG:	Feb 28, 2025 / 280143Z FEB 25
From:	SECSTATE WASHDC
Action:	ALL DIPLOMATIC AND CONSULAR POSTS COLLECTIVE *Routine*
E.O:	13526
TAGS:	CVIS, CMGT, KCSY
Captions:	SENSITIVE
Reference:	25 STATE 5914
Subject:	(U) Catch And Revoke: National Security Through Timely Processing of Visa Systems Messages

1. (U) This is an **Action Request**. Please see paragraph 5.

2. (SBU) **SUMMARY**: Among the best evidence of a person's eligibility for a visa is his or her actual behavior. Therefore, recurrent vetting conducted throughout the entire validity period of a visa - based on actual travel to the United States and actual encounters with United States law enforcement authorities - is necessary to protect Americans and U.S. borders. Under Executive Order (E.O.) 14161, "Protecting the United States from Foreign Terrorists and Other National Security and Public Safety Threats," the Department is directed to ensure maximum screening and vetting throughout the visa process. Therefore, consular officers must utilize whole-of-government law enforcement systems to vigilantly monitor the activities of aliens - whether they are inside the United States or not. In particular, Posts LE [redacted] daily and revoke or request revocation of any visas for a visa holder you determine is no longer eligible under Section 214(b) or 212(a) of the Immigration and Nationality Act (INA), or has overstayed. In other words, when a consular officer catches an alien misusing a visa, the officer should generally revoke it. Catch and revoke. **END SUMMARY.**

3. (SBU) Section 1(b) of E.O. 14161 states that, "[t]o protect Americans, the United States must be vigilant during the visa-issuance process to ensure that those aliens approved for admission into the United States do not intend to harm Americans or our national interests. More importantly, the United States must identify them before their admission or entry into the United States." Timely and stringent processing of LE [redacted] after visa issuance, and revoking visas when appropriate, is necessary to this effort. Visa holders who overstay their admission period in the United States even by one day, engage in conduct that poses a threat to U.S. national security, or otherwise misuse their visas should have their visas revoked under INA 221(i). In accordance with 9 FAM 403.11-(A), Posts should also carefully review for revocation any visa holders who are arrested or convicted of crimes in the United States, including assessing whether the visa holder remains eligible for the visa classification under INA 214(b).

4. (SBU) LE [redacted]

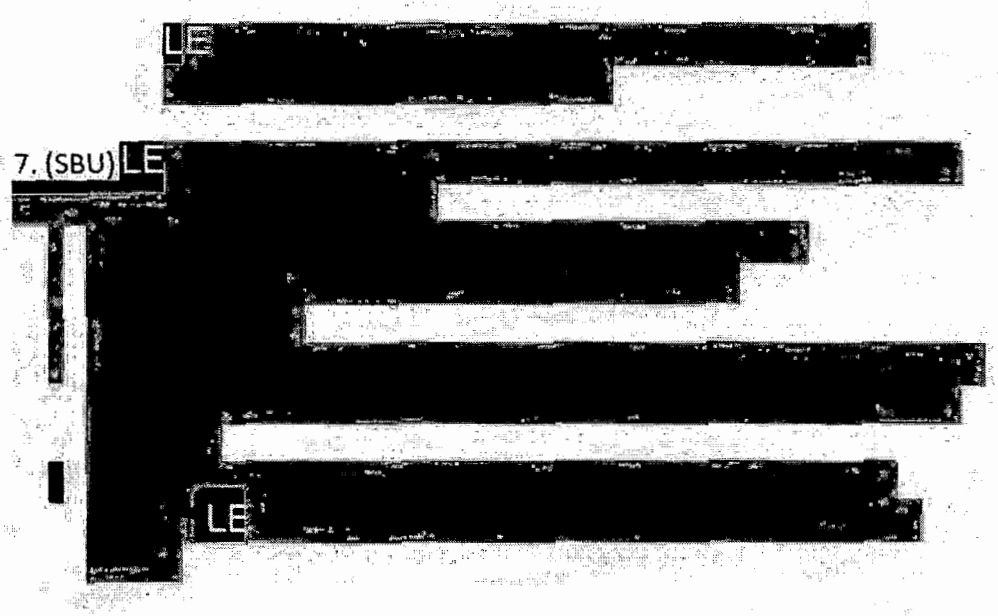
ACTION REQUEST/IMPLEMENTATION GUIDANCE

5. (SBU) **ACTION REQUEST:** LE [redacted]

LE [redacted] If a post anticipates a large quantity of cases will require prudential revocation, post must also include the VO/SAC revocations team. Managers should monitor the queue size daily and take action if messages accumulate.

6. (SBU) LE [redacted]

LE



8. (SBU) Applicants may not or visa holders may no longer overcome 214(b) if they engage in activities that are inconsistent with the claimed nonimmigrant status (Ref A). Even if an alien has not yet been convicted of crime and his or her visa is not yet revocable under INA 212(a)(2)(A)(i)(1), consular officers must evaluate whether the visa should be revoked under INA 214(b). LE , you must assess whether INA 214(b) applies as a basis for revocation. Every overstay and/or arrest requires you to weigh whether the alien is ineligible under 212(a) or no longer overcomes INA 214(b). Remember, applicants may not, or visa holders may no longer, overcome 214(b) if they engage in activities that are inconsistent with the claimed nonimmigrant status (Ref A).

9. (SBU) If a consular officer already suspects at the interview window that an applicant has committed a crime in the United States, then the consular officer must carefully consider all potentially applicable grounds of ineligibility and enter these considerations through case notes. A consular officer will usually refuse to issue a visa to such a suspected criminal applicant. LE

LE [redacted] If a consular officer knows at the window that an applicant will overstay a visa even beyond the admit-until date permitted by U.S. Customs and Border Protection authorities at ports of entry (let alone beyond the applicant's stated purpose of travel), then the consular officer will likely refuse to issue a visa to such an applicant. Yet this is exactly what a visa overstay means: a one-day overstay is still an overstay. Even if such a visa holder has not yet overstayed by more than 180 days and his or her visa is therefore not yet void under INA 222(g), nonetheless the alien likely no longer overcomes INA 214(b).

Revocation If the Alien Has Departed the United States

10. (SBU) LE [redacted] If the alien has departed from the United States, posts should initiate revocation procedures in accordance with 9 FAM 403.11-3(A)(2), including LE [redacted]. Consular officers do not have the authority to revoke a visa for individuals who are still in the United States based on a suspected ineligibility or based on derogatory information that is insufficient to support an ineligibility finding, other than a revocation based on driving under the influence (DUI).

Revocation If the Alien is Still in the United States

11. (SBU) Requests for revocation of visas where the individual is in the United States must be sent to the Revocation Team in VO/SAC/RC at LE [redacted]

Immigrant Visa (IV) Cases

12. (SBU) LE [redacted] For unused, valid IVs, use the guidance in 9 FAM 303.7-6(C)(1) to determine whether the information is sufficient to render the person ineligible for an IV. If so, initiate revocation procedures in accordance with the guidance in 9 FAM 504.12.

TRAINING & GUIDANCE

13. (SBU) LE [redacted]

14. (U) Additional guidance and contacts: Guidance related to Executive Orders can be found on CAWeb. State Department personnel can also join the CA/VO Transition Coordination Team to review official guidance and submit questions to VO subject matter experts regarding the E.O.

15. (U) Inquiries: For any media or congressional inquiries on E.O.s, posts must use pre-cleared language from public talking points located on CA Web (linked here), and copy CA/P on any responses. When responding to general or press inquiries about the E.O., copy CAPressRequests@state.gov. When responding to any congressional inquiries, copy ConsularOnTheHill@state.gov.

16. Minimize Considered.

MINIMIZE CONSIDERED
Signature: RUBIO

XMT: BASRAH, AMCONSUL; CARACAS, AMEMBASSY; CHENGDU, AMCONSUL; KABUL, AMEMBASSY; MINSK, AMEMBASSY; SANAA, AMEMBASSY; ST

PETERSBURG, AMCONSUL; VLADIVOSTOK, AMCONSUL;
YEKATERINBURG, AMCONSUL

UNCLASSIFIED
SBU

MEMORANDUM OF AGREEMENT
BETWEEN
UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES (USCIS)
AND
UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT (ICE)
REGARDING
COORDINATION OF ICE OPERATIONAL VISITS TO USCIS FACILITIES

1. Introduction

U.S. Citizenship and Immigration Services (USCIS) and U.S. Immigration and Customs Enforcement (ICE) have long maintained an effective and cooperative relationship, as both agencies share a primary mission to protect national security and public safety. USCIS leadership recognizes the importance of seamless cooperation with law enforcement partners such as ICE. Therefore, this Memorandum of Agreement (MOA) is designed to memorialize each agency's commitment to work together, in terms of proper visit notification and facility access for ICE visits to USCIS facilities for the questioning, apprehension, and/or arrest of Persons of Interest (POIs), and information sharing, while also ensuring that information is appropriately safeguarded when addressing emergent matters of national security and public safety.

2. Scope

This MOA applies to all domestic USCIS Field Offices, USCIS Asylum Field Offices, and all domestic ICE Field Offices.

3. Parties

The parties to this agreement are the Department of Homeland Security USCIS and ICE.

4. Authorities

- Department of Homeland Security (DHS) Delegation Number 7030.2, Delegation of Authority to the Assistant Secretary for U.S. Immigration and Customs Enforcement (Nov. 13, 2004)
- DHS Delegation No. 0150.1, Delegation to the Bureau of Citizenship and Immigration Services (Mar. 1, 2003)

5. Purpose and Intent

USCIS and ICE jointly enter into this MOA and hereby agree to:

- Maintain and follow all existing information-sharing laws, regulations, policies, procedures, and guidelines when addressing matters of national

security and public safety;

- Follow established information-sharing guidelines and processes for routine case inquiries; and
- Follow visitation procedures listed in this MOA during exigent circumstances, operational, and undercover activity. Operational activity not specified in this MOA is governed locally by USCIS field office and asylum field office policy and procedures.

6. Responsibilities of the Parties to the Agreement

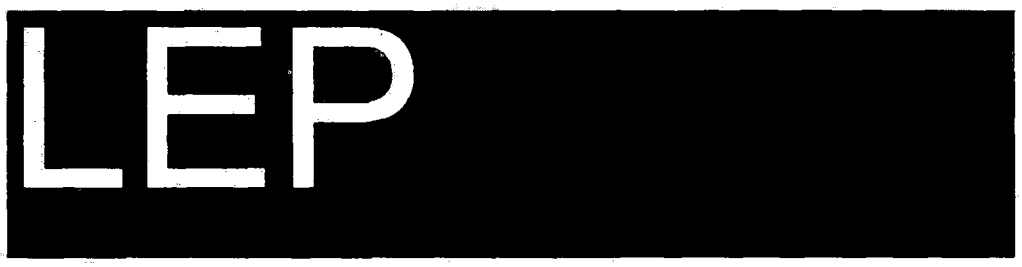
USCIS and ICE agree to the following:

A. Regular Meetings

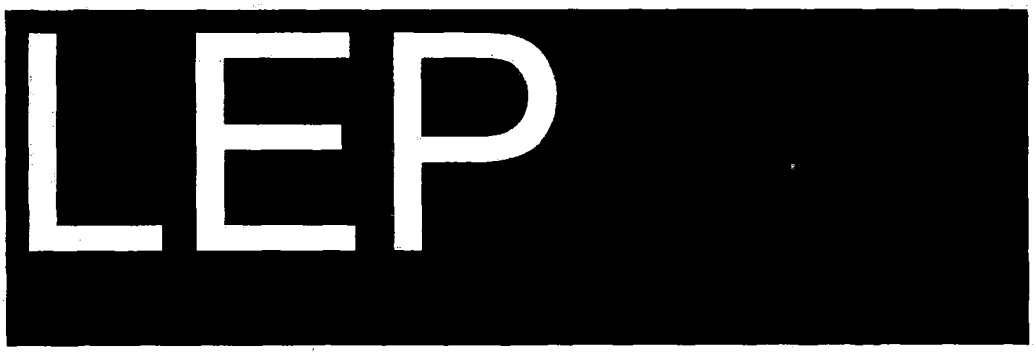
USCIS Field Office Directors (FODs), USCIS Asylum Office Directors, ICE Homeland Security Investigations (HSI) Special Agents in Charge (SACs), and ICE Enforcement Removal Operations (ERO) FODs and/or their respective designated senior staff shall meet regularly - but no less than on a quarterly basis - to discuss trends, issues, and concerns arising from the terms of the MOA. Additional meetings may be scheduled as needed to address any concerns or urgent matters. At the discretion of USCIS FODs and USCIS Asylum Office Directors, USCIS Office of Chief Counsel (OCC) may be included in the aforementioned meetings. Also, at the discretion of the HSI SAC or ERO FOD, the OPLA Chief Counsel may be included in the aforementioned meetings.

B. Scheduling Operational Visits to USCIS Facilities

C. Enforcement Activities and FDNS Coordination



D. Coordinating Exigent Visits to USCIS Facilities



7. **Other Provisions**

Nothing in this MOA is intended to conflict with current law or regulation or the directives of DHS. If a term of this MOA is inconsistent with such authority, then that term will be invalid, but the remaining terms and conditions of this MOA shall remain in full force and effect.

8. **Effective Date**

The terms of this agreement will become effective on May 31, 2016.

9. **Modifications of this MOA**

This MOA may be modified upon the mutual written consent of the parties

10. **Termination**

The terms of this signed MOA and any subsequent modifications consented to in writing by both parties to the MOA will remain in effect until terminated by either party to the MOA. Either party to the MOA may terminate the agreement by providing 60 (sixty) days' written notice to the other party.

Lori L. Scialabba
Deputy Director
DHS USCIS
5/31/16
DATE

Daniel H. Ragsdale
Deputy Director
DHS ICE
5/31/16
DATE