ICE Information Sharing and Access Agreements Handbook

U.S. Immigration and Customs Enforcement

Foreword

U.S. Immigration and Customs Enforcement (ICE) is responsible for enforcing customs, immigration, and other Federal laws. To support this mission, ICE may enter into cooperative agreements with parties external to the Department of Homeland Security (DHS) that involve sharing ICE information and data, and permitting access to DHS systems that contain ICE data. This *Handbook*, which accompanies ICE Directive 4006.1, *Development and Approval of ICE Information Sharing and Access Agreements*, establishes consistent and definitive guidance for developing, coordinating, formalizing, and approving information sharing and access agreements that share or provide access to ICE information and data. This *Handbook* and associated Directive are to be read jointly for complete documentation on ICE's policies and procedures regarding information sharing and access agreements. In entering into such agreements, ICE will comply with all applicable laws, regulations, and policies.

Contents

Introduction

Purpose

This *ICE Information Sharing and Access Agreements Handbook* provides guidance and procedures for developing, coordinating, formalizing, and approving information sharing and access agreements (ISAAs) that address the sharing of ICE information and data with parties *external to DHS*. Though not intended to be prescriptive in addressing every legal and policy issue that might arise, this *Handbook* provides users with best practices and guidance, and supplements the ICE Directive 4006.1, *Development and Approval of ICE Information Sharing and Access Agreements* ("Directive").

Scope

The Directive and this accompanying Handbook apply only to information sharing and access agreements in which one or more parties external to DHS[1] are given or provided access to ICE information or data. Types of ISAAs include, but are not limited to, Memoranda of Understanding (MOU), Memoranda of Agreement (MOA), Memoranda of Cooperation (MOC), Letters of Intent (LOI), or pilot projects.

Certain information sharing is exempt from the requirements of the Directive and this Handbook. These include, but are not limited to, Interconnection Security Agreements (ISA); Interface Control Agreements (ICA); Service Level Agreements (SLA); Interagency Agreements (IAA); Customs Mutual Assistance Agreements (CMAA); 287(g) agreements; court orders and civil and criminal discovery; requests for specific information in the process of advancing a case during the course of routine operational or law enforcement activities or litigation; sensitive law enforcement activities and/or agreements; transfers of authorized information or knowledge through an established liaison arrangement; regulatory compliance; exigent threats; information that falls under the Third Agency Rule; individual requests made under the Freedom of Information Act (FOIA) or Privacy Act; transactions with contracted vendors; individual *ad hoc* requests for information such as those from Congress, the White House, and the media; or individual *ad hoc* requests for information related to agencies, entities, and persons in order to comply with Executive Orders, laws, and regulations.

Background

ICE uses ISAAs to build on partnerships with law enforcement, the Intelligence Community (IC), and foreign, Federal, State, local, and tribal agencies that share overlapping and complementary mission operations responsibilities. ISAAs play a central role in sustaining ICE's information and data governance practices by providing the critical procedural controls necessary to effectively identify and manage the risks of unauthorized use, uncontrolled sharing, and non-compliant information processes that may ultimately impact privacy, civil rights and

[1] Parties external to DHS include domestic or foreign entities, such as foreign governments, entities in the private or public sector and government agencies at the Federal, State, local, or tribal level.

civil liberties, and security mandates. To understand the context and circumstances that prompt the use of an ISAA, it is necessary to first define and outline the general categories of information and data collected and used at ICE.

I. Identifying Information and Data

Information is defined as any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual.[2]

Data is defined as a value or set of values representing a specific concept or concepts. Data becomes "information" when shared, analyzed and combined with other data in order to extract meaning and to provide context. The meaning of data can vary depending on its context. Within this document, the term data is inclusive of all formats. It includes, but is not limited to, 1) geospatial data 2) unstructured data, 3) structured data.[3]

Additional definitions may be found in Appendix A: Definitions and Commonly Used Terms of this Handbook.

II. Categories of Information and Data

ICE differentiates operational and management supporting information and data according to the following four broad categories:

- ***Law Enforcement Information:*** Information collected in the course of or related to preliminary, open, pending, or closed administrative, criminal, or civil investigations or enforcement activities within an agency's assigned law enforcement mission. The ICE Executive Agent for law enforcement information and data sharing is the Homeland Security Investigations (HSI) Executive Associate Director (EAD) or Enforcement and Removal Operations (ERO) EAD, as appropriate. Refer to Appendix H: Frequently Asked Questions (FAQs) for information regarding sharing related to internal ICE security investigation and physical security threat activities.

[2] National Institute of Standards and Technology. *Special Publication 800-30, Appendix B.* 2012. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[3] The Federal Enterprise Architecture Program. *The Data Reference Model, v 2.0.* November 17, 2005. *https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/DRM_2_0_Final.pdf#:~:text=The%20Data%20Reference%20Model%20%28DRM%29%20is%20one%20of,and%20the%20promotion%20of%20uniform%20data%20management%20practices.https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/DRM_2_0_Final.pdf#:~:text=The%20Data%20Reference%20Model%20%28DRM%29%20is%20one%20of,and%20the%20promotion%20of%20uniform%20data%20management%20practices.*

ICE Executive Agent for
Law Enforcement Information
is the **HSI EAD**
or **ERO EAD, as appropriate**

- *Example:* (b)(7)(E)

- ***Homeland Security Information***: Information that relates to the threat of terrorist activity; relates to the ability to prevent, interdict, or disrupt terrorist activity; would improve the identification or investigation of a suspected terrorist or terrorist organization; or would improve the response to a terrorist act.[4] HSI EAD is the ICE Executive Agent for information and data sharing for homeland security information or with the IC. Refer to Appendix H: Frequently Asked Questions (FAQs) for information regarding sharing with foreign governments or international organizations.

ICE Executive Agent for
Homeland Security Information
is the **HSI EAD**

- *Example*: (b)(7)(E)

- ***Immigration Administration Information***: Information supporting the logistical and administration activities used to manage the nation's civil immigration detention and removal system. This includes logistical aspects of the removal process, including domestic transportation, detention, alternatives to detention programs, bond management, supervised release and for the disclosure of this information to the public, Federal, State and local governments, foreign governments and international organizations.[5] The ICE Executive Agent for immigration administration information and data sharing is the ERO EAD. Refer to Appendix H: Frequently Asked Questions (FAQs) for information regarding sharing related to the Criminal History Information Sharing (CHIS) initiative.

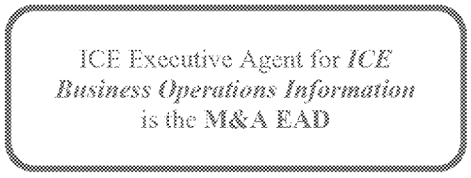
ICE Executive Agent for
Immigration Administration Information
is the **ERO EAD**

- (b)(7)(E)

[4] Public Law 107-296, Homeland Security Act, Section 892f.

(b)(7)(E)

- ***ICE Business Operations Information***: Information necessary for effectively and efficiently running the daily mission support activities of ICE to include public affairs, congressional affairs, financial management, acquisition, personnel, administrative law, and security activities. The ICE Executive Agent for ICE business operations information and data sharing is the Management and Administration (M&A) EAD. Refer to Appendix H: Frequently Asked Questions (FAQs) for information regarding sharing related to security activities that are part of the daily mission support.



Each category of information and data has its own unique mission purposes and processes used during collection, processing, sharing, and storage. However, they all share common governance requirements with associated standards and processes necessary to safeguard the information and data from unauthorized and non-compliant use. To meet these concerns and to ensure compliance with the Directive, ICE Directorates and Program Offices ("Program Offices") should follow the guidance and procedures herein when developing, coordinating, and formalizing information sharing and access agreements.

Information Sharing and Access Agreements

I. Definition of Information Sharing and Access Agreements

Information Sharing and Access Agreement (ISAA) is an agreement that is used to facilitate the exchange of information between the Department (or any element or entity within the Department) and one or more outside parties. Agreement types include, but are not limited to, Memorandums of Understanding (MOU), Memorandums of Agreement (MOA), Memorandums of Cooperation (MOC), Letters of Intent (LOI), or agreements related to pilot projects. Parties include domestic or foreign entities in the private or public sector and government agencies at the Federal, State, or local level.

II. Purpose of Information Sharing and Access Agreements

ISAAs are a method of accountability for access to or receipt of information and data between parties. Completing the ISAA development process can help to ensure that such access and sharing of information and data is conducted in compliance with applicable laws and policies.

ISAAs are used to authorize the repeated, continuing, or enduring exchange of or access to information and data. ISAAs define the terms and conditions of information and data sharing between two or more parties, and clearly identify controls for managing the risks of unauthorized use, uncontrolled sharing, and non-compliant information processes, among other terms.

III. Participants in Information Sharing and Access Agreements

ICE Program Offices each have a specific set of activities they undertake that are directed towards a common purpose or goal in support of ICE's mission, functions, activities, services, projects, and processes. To accomplish their ICE-related activities, ICE Program Offices may need to share or provide access to ICE information and data to parties external to DHS. All ISAAs are initiated, negotiated, and developed by ICE Program Offices.

ICE Key Stakeholders are subject-matter experts within ICE with expertise in the areas of privacy, civil rights and civil liberties, information classification, records management, information technology, information governance, intelligence, ICE and DHS policy, and legal issues, and Program Offices responsible for the information and data involved. Depending on the information and data being shared, or the intended use of the information and data, specific ICE Key Stakeholders may be asked by an ICE Program Office to participate early in the ISAA process. While the ICE Key Stakeholders provide advice and assistance to the ICE Program Office, they do not draft the ISAA.

ISAAs within the scope of the ICE ISAA Directive are reviewed and cleared by ICE Key Stakeholders prior to execution. ICE Key Stakeholders include the following offices, when appropriate: Office of Policy and Planning (OPP), Office of the Principal Legal Advisor (OPLA), Office of Information Governance and Privacy (IGP), Office of Diversity and Civil Rights (ODCR), Office of the Chief Information Officer (OCIO), Office of Professional Responsibility (OPR), Law Enforcement Information Sharing Initiative (LEISI), and HSI Intel

(if sharing with the Intelligence Community). Directorate and Program Offices may also be included as they may be most knowledgeable about the information and data involved.

ICE Executive Agents are the ICE Executive Associate Director (EAD) aligned with the category of information under their area of responsibility which is addressed by the ISAA. The Executive Agent is responsible for overseeing the development and signing of their respective ISAA. For law enforcement information, the Executive Agents are the HSI and ERO EAD. For homeland security information, the Executive Agent is the HSI EAD. For immigration administration information, the Executive Agent is the ERO EAD. For ICE business operations information, the Executive Agent is the M&A EAD. The Executive Agent is responsible for facilitating the development of the ISAA through collaboration with relevant ICE Program Offices to ensure potential legal, policy, civil rights and civil liberties, classification, technical, and data breach risks prior to finalization of the ISAA. The ICE Executive Agent is tasked with developing and maintaining standards, developing training programs, coordinating administrative support, and providing ICE-wide visibility of the designated activity.

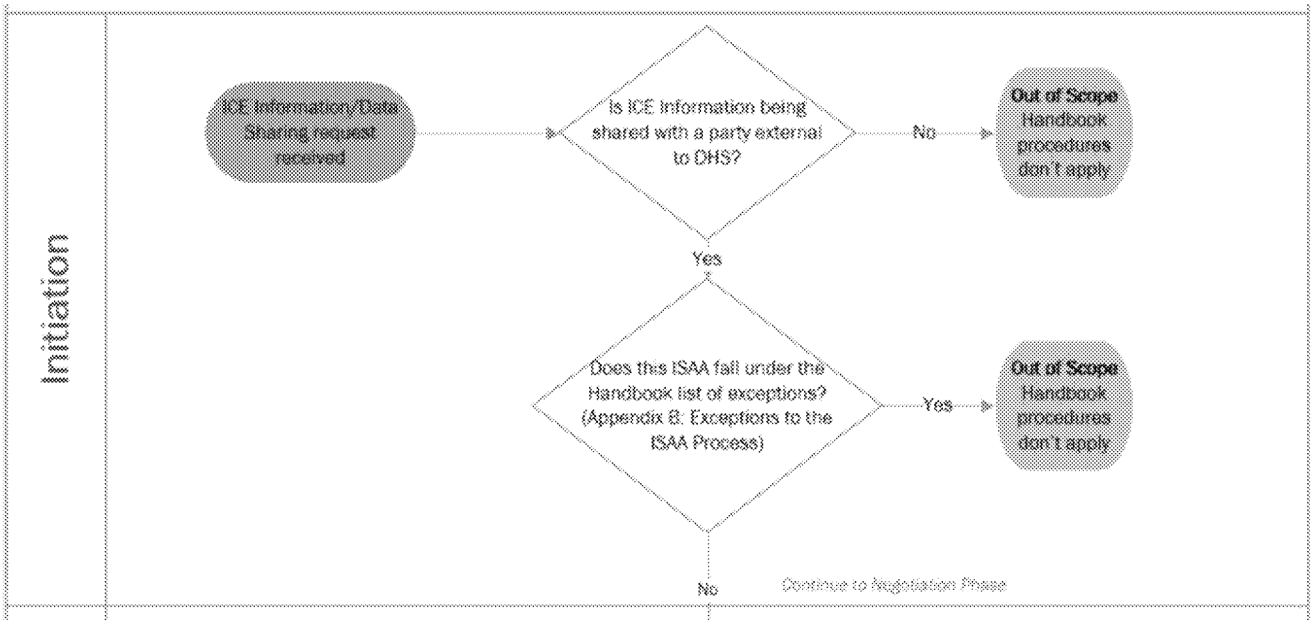
ISAA Development Guidance and Procedures

The process for developing ISAAs that address the sharing and access of ICE information and data by parties external to DHS can be separated into five phases:

1. Initiation and identification,
2. Negotiation,
3. Development,
4. Clearance, and
5. Maintenance, auditing, and termination.

The initiation phase of the ISAA begins with receiving a request or identifying the need for information sharing and encompasses the initial outlining and scoping of the ISAA to determine the type of information being requested and the intended use of the information. The negotiation phase consists of negotiations with the external party regarding the information exchange and providing guidelines for the parameters of an ISAA, to include areas of risk mitigation with the support of ICE Key Stakeholders. The development phase of the ISAA is the drafting and revision process to achieve the final language for an ISAA. The clearance phase includes completing due diligence on the ISAA by circulating the document through the clearance process for review and approval by Key Stakeholders and signatures by the parties to the ISAA. Finally, the maintenance, auditing, and termination phase includes managing the ISAA in a repository, reviewing the fully executed ISAA on a regular basis, performing periodic audits to ensure the terms of the agreement continue to be met by all parties, and termination when ISAAs are deemed to be no longer needed. The following sections expand on each of the five phases of developing ISAAs.

Initiation and Identification Phase



See Appendix C: ISAA Process Flow for the entire process flow chart.

IV. Receiving a Request for Information Sharing

It is a best practice to include subject- matter experts (SME) early in the discussion so that any risks can be identified, discussed, and mitigated prior to release of ICE information to those parties external to DHS. An ICE ISAA can be initiated by external request, or through implementation of an initiative at DHS or ICE, such as a technology pilot project. ICE Program Offices may have specific points of contact and/or internal processes for handling initial requests. However, in addition to the internal processes, ICE Program Offices should verify the requestor's authenticity and receive statements outlining the clear mission requirements and objectives driving the desired acquisition of ICE information and data. It is the responsibility of the ICE Program Office to also confirm there are no existing active ISAAs in place that can be leveraged. By leveraging existing ISAAs, ICE Program Offices may minimize duplicative efforts, and gain a more holistic view of information and data sharing already in place, and limit scope or purpose expansion of data through discrete agreements from external parties. If ICE Program Offices are having difficulty conducting this vetting effort, contact IGP via their intake process for support.[6]

For more information on how internal processes function in relation to this Handbook, please refer to Appendix H: Frequently Asked Questions (FAQs) on Internal Processes.

[6] Contact IGP via their intake process by completing the IGP Support Request Form located on the IGP intranet homepage: (b)(7)(E)

V. Identifying the Scope of the Request

When an information sharing request is being processed, ICE Program Offices will need to first identify whether the scope of the request falls under the ICE ISAA Directive and the process outlined in this Handbook. If the information sharing request falls out of scope of the ICE ISAA Directive and this Handbook, ICE Program Offices must comply with the internal procedures of their program office, as well as any other applicable ICE or DHS policies.

In-Scope Sharing Requests

The process described in this Handbook is valid for requests for ICE information and data to be shared with or provided access to by parties external to DHS.

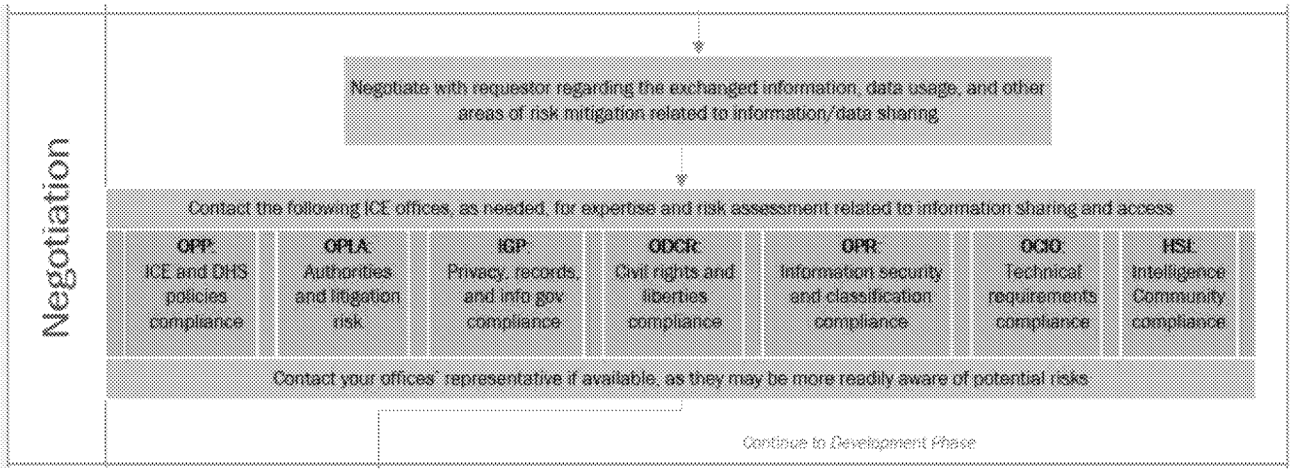
Out-of-Scope Arrangements for Sharing or Accessing ICE Information and Data

ISAAs that pertain to ICE information and data shared internally within DHS are not included in the scope of this Handbook and associated Directive. There are also exemptions for certain types of external information sharing covered in detail in Appendix B: Exemptions to the ISAA Process. Additionally, the process described in this Handbook does not cover ICE-only access or receipt only of data from parties outside of DHS. For example, arrangements are considered out-of-scope of the ICE ISAA Directive and this Handbook in instances where ICE accesses an external information system, or when an external party provides ICE its (the external party) data without ICE reciprocating by sharing or allowing access to ICE information and data.

However, even if information sharing arrangements are considered out-of-scope, it is highly recommended and good practice to include ICE Key Stakeholders in early discussions and negotiations as necessary, as well as to follow established policies and procedures, to ensure their expertise in the areas of legal, policy, civil rights and civil liberties, classification, technical, privacy, and records can help identify and mitigate potential issues that may arise and cause harm to the Agency or individuals.

To view frequently asked questions about ISAAs coordinated by DHS, please reference the DHS section in Appendix H: Frequently Asked Questions (FAQs).

Negotiation Phase



See Appendix C: ISAA Process Flow for the entire process flow chart.

VI. I. Negotiating Terms of the ISAA

Upon initiating negotiation of an ISAA, ICE Program Offices should propose specific terms regarding what information and data will be exchanged or accessed, the usage of data, the analytical approach for using the ICE information and data, the disposition of information and data, restrictions such as access controls and limiting dissemination of the information and data, and risk mitigation efforts in the event of unauthorized information and data spillage or misuse.

It is important to note that in the case of Personally Identifiable Information (PII) being shared, the Privacy Unit in the ICE Office of Information Governance and Privacy (IGP), and ICE Office of Professional Responsibility (OPR) must be contacted. Please reference the Privacy and OPR sections below for more details on the roles of these Program Offices. Additionally, view the PII section in Appendix H: Frequently Asked Questions (FAQs) for details on ISAAs regarding information with PII.

VII. II. ICE Key Stakeholder Engagement

ICE Program Offices should ascertain and identify the relevant stakeholders, supporting systems, data stewards, and specific information and data requirements when working with the external party on the ISAA's scope.

ISAA development relies heavily on the early involvement of ICE Key Stakeholders with subject-matter expertise in the sharing processes, and ICE Program Office leadership should identify their points of contact at the very beginning of ISAA development to support these initial fact-finding efforts, including engaging with the designated ICE Executive Agents who may provide additional support.

Below are ICE Key Stakeholders that may potentially be engaged to identify risks associated with the sharing or access of ICE data and provide possible mitigation efforts to minimize those risks. Not every ISAA is the same, so depending on the nature of the arrangement, different expertise may be needed. It is important to contact the relevant experts at the earliest stages of ISAA negotiation and development. Waiting to engage these offices during the final clearance process may cause delays in finalizing an ISAA.

ICE Office of Policy and Planning (OPP)

ICE Program Offices should include OPP to ensure compliance of the ISAA with both ICE and DHS policies. OPP has awareness of current and developing ICE and DHS policies that could have implications for information sharing activities. It is possible that such policies could restrict sharing activities or even limit what activities are allowed with such shared information and data. Keeping OPP abreast of ISAAs during development helps to ensure such ISAAs and the activities described are not contrary to ICE or DHS policy.

ICE Office of the Principal Legal Advisor (OPLA)

ICE Headquarters Program Offices should consult with OPLA HQ regarding any novel legal issues involved in a particular ISAA. Field Offices may contact their local OPLA field location, which may coordinate with OPLA HQ as appropriate. During the final clearance process, OPLA HQ may be asked to review the ISAA for legal sufficiency and litigation risk, as appropriate.

OPLA HQ may recommend that an ISAA should be elevated to the DHS level. Please refer to the DHS portion of Appendix H: Frequently Asked Questions (FAQs) for more information.

ICE Office of Information Governance and Privacy (IGP)

ICE Program Offices should include IGP for privacy, records and data management, and information governance compliance. In some program offices, there are IGP representatives or individuals that coordinate closely with IGP. Reach out to these IGP representatives for initial conversations about potential issues with the ISAA being developed. These representatives help to identify the particular authority that allows or that may restrict the sharing of or access to ICE information and data, or combination of certain data that results in the identity of individuals, as well as the length of time the information and data may be retained.

Privacy Unit

Proactively engaging with ICE Privacy during the negotiation phase of ISAA development is critical to identifying potential restrictions and risks regarding the sharing of PII, especially Sensitive PII.[7] Even when data sets are de-identified, privacy implications can still arise. Engaging ICE Privacy early and throughout the project's lifecycle not only aligns with the Fair Information Practices Principles (FIPPs)[8] but will also help better achieve the project's goals and ICE's mission. To learn more about the risks associated with failing to reach out to Privacy in cases of ISAAs regarding PII, see the PII section in Appendix H: Frequently Asked Questions (FAQs). An in-depth discussion of the FIPPs, as well as other privacy protections to develop during the negotiation process can also be found in Appendix F: Tips to Expedite the Review Process.

What authority option allows the information and data to be shared outside of DHS/ICE?

1. The person whose PII is being shared requests or consents to the sharing; **or**

2a. The recipient's need for the information is related to his or her official duties; **and**

2b. If the PII is contained in records covered by a system of records (SORN), there must be an authorized disclosure exception (e.g., a published routine use in the applicable SORN) that permits sharing pursuant to the Privacy Act, as amended, 5 U.S.C. § 552a; **and**

2c. The sharing of PII to third parties must be consistent with DHS policy, including DHS's privacy policies and information-sharing policies; **and**

2d. Sharing must be consistent with all ICE policies.

Records and Data Management Unit

Engaging with the ICE Records and Data Management (RDM) Unit during the negotiation phase of the ISAA development is important to identify the length of time shared data can be maintained by the requesting party. The RDM Unit follows the National Archives and Records Administration (NARA)-approved records retention schedules, which are determined based on the needs of the agency, laws, and other Federal requirements. Additionally, following retention schedules helps minimize privacy issues due to privacy incidents, data calls related to litigation holds, and FOIA requests on data that is overdue for disposition based on its retention schedule.

What is the agreed upon retention period for the information and data?

[7] A subset of PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if the data is inappropriately accessed or compromised.

[8] DHS uses the FIPPs in Privacy Impact Assessments (PIAs), oversight activities, information sharing agreements, privacy policies, redress activities, and its other privacy responsibilities. See Fn. 8, Privacy Policy Guidance Memorandum 2017-01, DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information ("DHS Memorandum 2017-01"), *available at* *https://www.dhs.gov/sites/default/files/publications/PPGM%202017-01%20Signed_0.pdf.*

Information Governance Unit

The ICE Information Governance (IG) Unit handles data governance for ICE. Data governance consists of the processes and policies used to manage and ensure the availability of data. The IG Unit supports the ISAA negotiation and development efforts by helping Program Offices coordinate with the appropriate ICE Key Stakeholders to ensure proactive advice on mitigating information and data sharing risks is collaboratively discussed. The IG Unit is also responsible for all updates to the ICE ISAA Directive and Handbook. If there are significant changes needed to either document, the IG Unit is responsible for directing such changes and arranging for representatives from the ICE Key Stakeholders and Program Offices to convene an ISAA Working Group to participate in any necessary discussions on or concurrence of these changes. This is an *ad hoc* working group that focuses on high-level guidance for the Agency.

> I have a question related to the Clearance Phase of the ISAA process. I developed a checklist that could be useful for the ISAA process, how do I get it included in the ISAA Handbook?

Freedom of Information Act (FOIA) Unit

The ICE FOIA Unit handles all FOIA requests made by the public. If the request for ICE information and data does not require an ISAA and is not identified as an exemption or covered under a routine use from a SORN, then the information may need to go through the FOIA process for the ICE information and data to be released to the external party. There are nuances depending on whether the requesting party is from Congress or the media, at which point specific instructions and points of contacts should be involved prior to any release of ICE information and data.[9]

ICE Office of Diversity and Civil Rights (ODCR)

ICE Program Offices should involve ODCR for civil rights and liberties requirements. ODCR is required by statute to carry out investigations concerning abuses of civil rights, civil liberties, and profiling on the basis of race, ethnicity, or religion. By engaging with ODCR proactively, ODCR can provide recommendations that are intended to strengthen and improve, as well as resolve any issues that could arise with the sharing or access of ICE information and data that might have civil rights or civil liberties implications.

> Is the information and data being shared related to individual characteristics of persons such as race, ethnicity, gender, religion, sexual orientation, gender identity, country of birth, and nationality? Could the proposed use have an impact on an individual's constitutional rights and liberties?

ICE Office of the Chief Information Officer (OCIO)

ICE Program Offices should involve OCIO for technical requirements compliance. If sharing or exchanging information between ICE and an external party to DHS will require technical

[9] For more information pertaining to FOIA requests, please visit https://www.ice.gov/foia/overview.

assistance, it is essential that OCIO is involved in the conversation. There are also other forms of information sharing arrangements (e.g., Interconnection Security Agreement (ISA), Interface Control Agreement (ICA)) required for all data sharing to or from ICE technology systems, including sharing between other ICE and DHS systems. Financial considerations will need to be discussed as interfacing with an external system outside of DHS may require additional resources and expertise, thus requiring additional funding to accomplish.

What is the proposed IT solution? Does the IT solution exist today? If not, can it be created? What are the proposed costs associated with the IT solution?

ICE Office of Professional Responsibility (OPR)

ICE Program Offices should involve OPR, Security Division (SD) Security Management Operations Unit (SMOU) for information security and classification compliance. Field Offices should engage OPR SD SMOU representatives with questions concerning information security or classification. OPR SD is responsible for reviewing, providing clarification, and ensuring all ICE ISAAs are compliant with required classification markings, restrictions and caveats, prior to formalization in accordance with DHS Instructions[10] and statutory requirements. Proactive engagement with OPR SD ensures that information and data that is identified with specific classification markings, whether classified or controlled unclassified information, is appropriately marked and continues to adhere to statutory requirements when this information and data is shared to parties external to DHS. If classified information is shared and becomes declassified, such instruction is also included so proper steps are taken to ensure the correct information and data is processed appropriately.

Is Classified or Controlled Unclassified Information (CUI) information (including deliberative or otherwise privileged information) being shared?

ICE Homeland Security Investigations Office of Intelligence (HSI INTEL)

All ISAAs involving the sharing of information between ICE and Intelligence Community members must be reviewed by the Assistant Director of the HSI Intel prior to execution.[11]

Is the information and data being shared with the Intelligence Community?

---

[10] DHS Instruction Manual 121-01-011, Appendix A, The Department of Homeland Security Administrative Security Program provides definitions, as identified in the DHS Lexicon, that further explain the information, documents, and activities that fall under the purview of OPR, SD.

[11] Pursuant to the designation of the Assistant Director of HSI Intel as the ICE Key Intelligence Officer (KIO), and as stated in ICE Directive 12002.2, section 4.1.2, the ICE KIO reviews, coordinates, and approves all agreements between ICE and elements of the IC prior to their execution.

HSI Law Enforcement Information Sharing Initiative (LEISI)

All ISAAs that fall under the Law Enforcement Information Sharing (LEIS) Service must be reviewed and signed by the Executive Director of LEISI, Homeland Security Investigations prior to execution. Information sharing requests between ICE and foreign governments or international organizations need to be coordinated through the HSI International Operations (IO) and HSI LEISI prior to release.

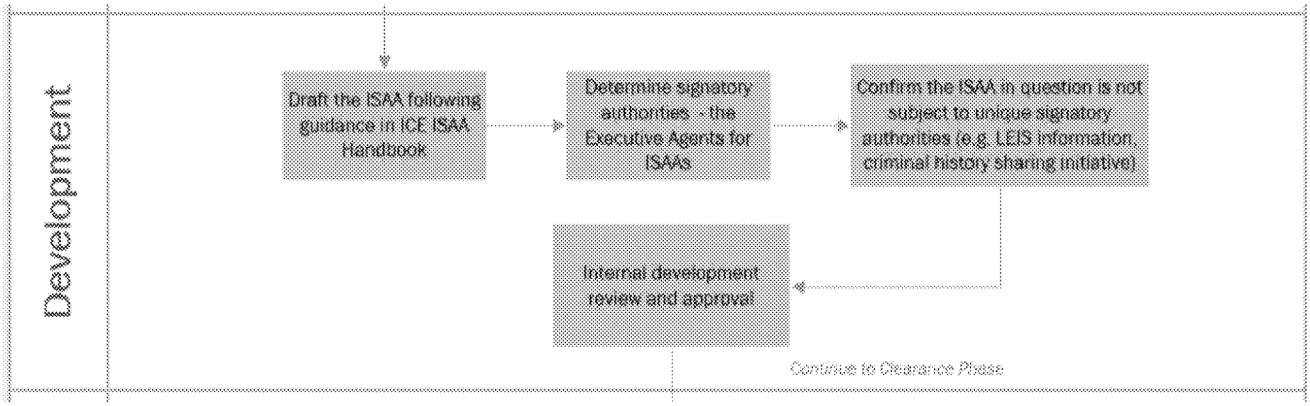
Does the information and data being shared fall under the Law Enforcement Information Sharing (LEIS) Service?

HSI International Operations (IO)

HSI IO is the designated signatory authority for international ISAAs. Information sharing requests between ICE and foreign governments or international organizations need to be coordinated through the HSI IO and HSI LEISI prior to release.

Is the information and data being shared with foreign governments or international organizations?

Development Phase



See Appendix C: ISAA Process Flow for the entire process flow chart.

VIII. I. ISAA Development

During ICE ISAA development, ICE Program Offices should lead open and transparent negotiations with all stakeholders, including clearly stating the purpose and details of the sharing, and addressing potential privacy, civil rights and civil liberties, security, and legal issues. The appendices to this Handbook provide common language and considerations for ISAAs to guide discussions with ICE stakeholders.

ICE Program Offices should continue to engage with ICE Key Stakeholders to coordinate the processes for agreement draft and final reviews and to discuss how relevant privacy, legal, security, and civil liberties issues will be addressed in the agreement.

The general standards to be met are as follows:

Standard Baseline
When drafting an ISAA, offices should verify they have addressed the following information necessary to develop a comprehensive agreement between ICE and parties external to DHS.

1) Provide a **title** which describes the subject matter and parties included in the sharing of information and data agreement;

2) Provide an **introduction** and identify the **purpose** for the sharing or access. Be sure to identify how the information and data will be used by the parties and identify the alignment of such use with what is identified as the use when the information is collected. If the current use differs from the use identified during the collection of the information, identify what routine use from the system of records allows the sharing or access of this information and data for this current use.

3) Provide documentation of **authorities**, **mission needs**, **information and data sharing requirements**, including the future transfer, use, and/or third-party information and data sharing constraints;

4) Identify all **processes**, **parties**, **responsibilities**, **systems**, **points of contact**, and **ICE information** and **data** involved in the sharing, including all safeguard, retention, classification markings, dissemination limitations, auditing and reporting requirements; and,

5) Provide effective **dates of issuance** and **termination** of the agreement as well as information on **information security** and the **disposition of data**.

For information on the importance of using detailed language when developing ISAAs, see Appendix F: Tips to Expedite the Review Process.

Other Considerations:

Cost Considerations

ICE Program Offices should conduct initial assessments of the costs associated with the information and access endeavor early in the agreement development process. Ensuring that deliberate and comprehensive consideration is given to the IT and logistical costs of initiatives will help ensure that any lack of financial resources does not become an insurmountable obstacle to the partnering endeavor. An inability to determine the associated costs of an initiative, however, does not preclude execution of the initiative if cost relevant implications are understood.

Classified ISAAs

If the ISAA is or may be classified, the drafting of the ISAA should only occur on Homeland Secure Data Network (for SECRET agreements) or C-LAN (for TOP SECRET agreements) with notifications sent via secure electronic mail or other protected notification processes according to the requirements for handling classified material. ISAAs involving the sharing of information between ICE and Intelligence Community members must be reviewed by HSI Intel prior to release.

Protected Activities and Classes of Data

Even when an ICE ISAA does not involve sharing PII, civil rights or civil liberties must be a consideration if the agreement includes information collected or aggregated based on special protected classes such as race, ethnicity, national origin, or religious affiliation, or based on constitutionally protected activities, such as First Amendment rights. Information and data aggregated or gathered based on such categories have potentially significant civil rights and civil liberties impacts, and ICE Program Offices should proactively coordinate with OPLA and ODCR during the initial phases of ISAA development, as appropriate.

All ICE ISAAs must be compliant with required classification markings, restrictions and caveats, prior to formalization in accordance with DHS Instructions[12] and statutory requirements. Any questions or issues needing clarification regarding the classification marking or classified transmission of the classified document will be coordinated with OPR SD SMOU; therefore, minimizing the possibility of a security incident. All security incidents involving classified information must be reported to OPR SD immediately by contacting ICE.ADSEC@ice.dhs.gov or the Joint Intake Center (JIC) at Joint.Intake@dhs.gov.

For more detail related to classified agreements and agreements containing protected activities and classes of data, access Appendix E: Special Cases and Considerations for Classified Agreements in this Handbook.

IX. II. DHS Involvement

Input from DHS-level Stakeholder Offices

There may be situations when an ICE Key Stakeholder needs to confer with its DHS HQ counterpart. This may be due to awareness of similar Departmental or multi-Component sharing or activity, or the need for further expertise to appraise risks and mitigation approaches. Prior to consulting with DHS HQ, the ICE Key Stakeholder should notify the Program Office of the intent to contact DHS HQ. After conferring with DHS HQ, the ICE Key Stakeholder would continue their interaction with the ICE Program Office within the ICE ISAA process.

For situations in which information is being received by ICE in exchange for ICE data being shared with an external party, compliance with the One DHS Rule is required. For more information on how and when the One DHS Rule applies, see Appendix H: Frequently Asked Questions (FAQs) under the DHS section.

X. Signatory Authority

The ICE Executive Agent responsible for the information and data involved in the sharing is the final agreement's signatory authority.

> ***Law Enforcement Information***: The ICE Executive Agents for law enforcement information and data sharing are the HSI EAD and the ERO EAD, depending on which Program Office the information involves.
>
> Specified below are information and data sharing activities where the ICE Executive Agent has granted specific signatory authority to particular ICE Program Offices. For all other ISAAs not specified below that share or allow access to law enforcement information, the ISAAs are signed by the applicable ICE Executive Agent.

[12] DHS Instruction Manual 121-01-011, The Department of Homeland Security Administrative Security Program, April 25, 2011

- ISAAs that fall under the LEIS Service may be signed by the Assistant Director of Homeland Security Investigations, LEISI.

- ISAAs that are classified and related to IC information may be signed by the Assistant Director, HSI Intel.

Homeland Security Information: The ICE Executive Agent for homeland security information and data sharing is the HSI EAD.

Specified below are information and data sharing activities where the ICE Executive Agent has granted specific signatory authority to particular ICE Program Offices. For all other ISAAs not specified below that share or allow access to homeland security information, the ISAAs are signed by the applicable ICE Executive Agent.

- ISAAs that involve classified information and related to IC information and data sharing with the IC are to be signed by the Assistant Director HSI Intel.

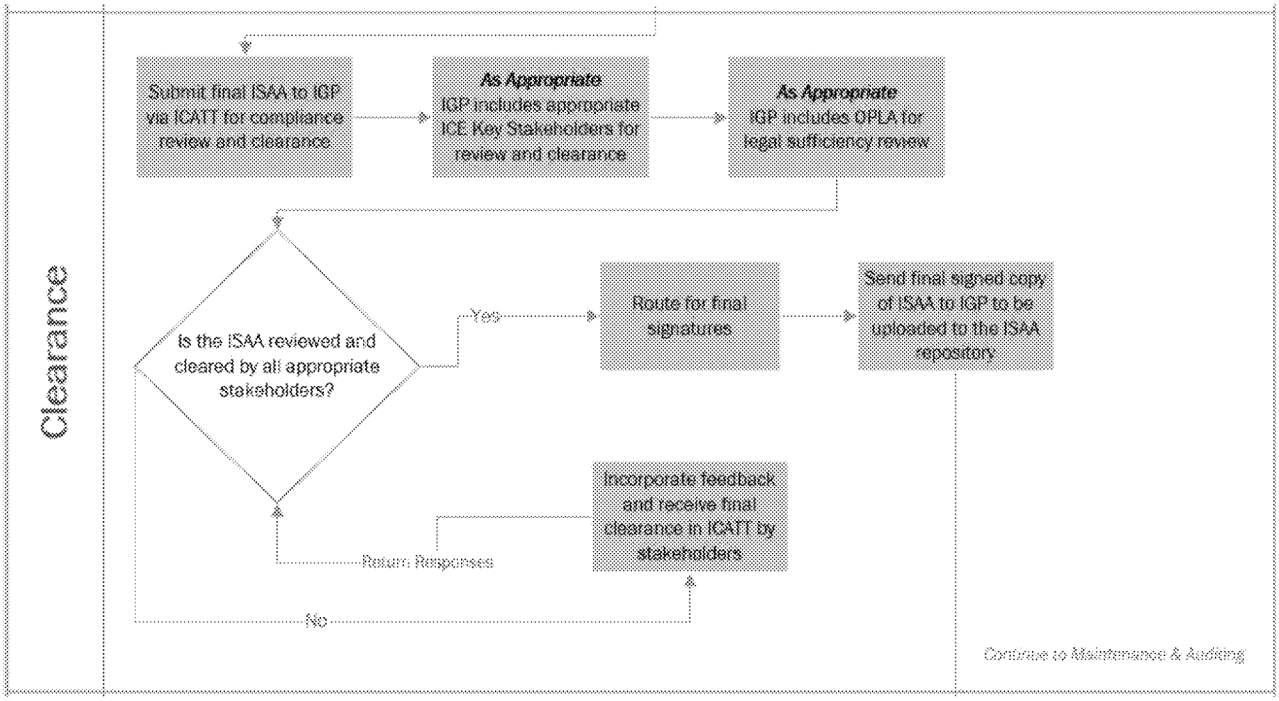
Immigration Administration Information: The ICE Executive Agent for immigration administration information and data sharing is the ERO EAD.

ICE Business Operations Information: The ICE Executive Agent for ICE business operations information and data sharing is the Management and Administration (M&A) EAD.

XI. Dispute Resolution

If there is a lack of concurrence on the details related to the information sharing or data accessed by a party external to DHS between ICE Program Offices and/or Key Stakeholders that cannot be resolved at the Program AD level, and escalation to ICE Directorates is also unable to resolve, then the ICE Director will make the final determination as to what will be memorialized within the ISAA and agreed upon by all ICE Directorates, Program Offices, and Key Stakeholders involved.

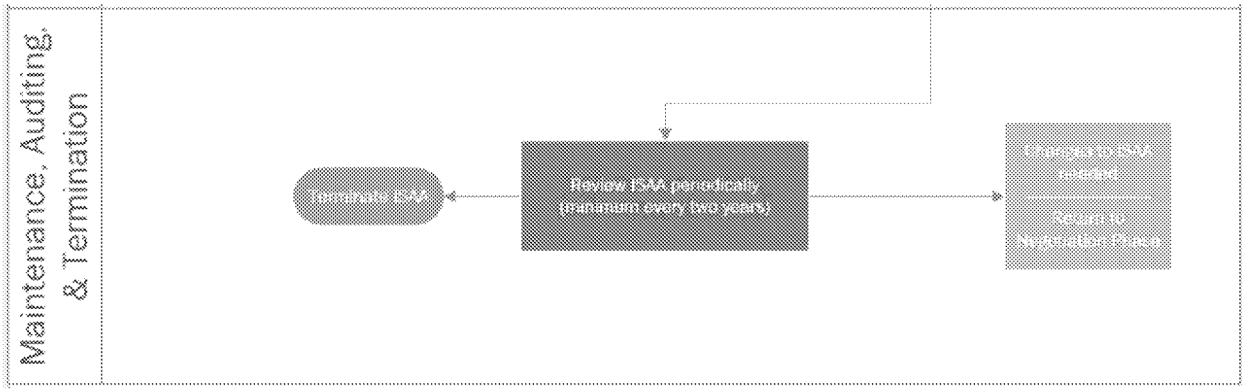
Clearance Phase



See Appendix C: ISAA Process Flow for the entire process flow chart.

Once the ICE Program Office concludes the ISAA negotiations and has a finalized draft ISAA, the ISAA is ready for circulation and clearance within the ICE Program Office following any internal procedures. Once that internal review and clearance is completed, the ISAA is ready to be circulated through ICE's online clearance system, ICE Correspondence and Task Tracking System (ICATT), for final review and clearance by IGP and other appropriate ICE Key Stakeholders. IGP will determine if other ICE Key Stakeholders should be included in the clearance process. If multiple ICE Key Stakeholders will be included in the clearance process, this activity will be performed concurrently and timely, to the extent possible, to limit operational delays that may be caused by extended clearance time for ISAAs. Following all other ICE Key Stakeholders completing their review, the Program Office may seek OPLA's legal review as appropriate. If OPLA determines that the ISAA warrants further review by the DHS Office of General Counsel (OGC), any review or clearance processes carried out by DHS OGC is out of the scope of this Handbook. If the ISAA has been cleared by IGP, the ICE Key Stakeholders and OPLA, as appropriate, the ISAA is ready for signature. The ICE Program Office will provide the ISAA to the appropriate signatories, as identified by the ICE Executive Agent associated with the category of information being shared and/or accessed. Once an unclassified, domestic ISAA has been fully executed by all parties, a copy of the fully executed ISAA will be provided to IGP. IGP will work towards creating a protected, searchable, central electronic repository for maintaining active, unclassified, domestic ICE ISAAs.

Maintenance, Auditing, and Termination Phase



See Appendix C: ISAA Process Flow for the entire process flow chart.

ICE ISAAs should be reviewed by ICE Program Offices' point of contact for the ISAA and the recipient of ICE data at a minimum, every two years, to determine whether the information sharing activity still supports the missions identified in the agreement, determine whether the terms and conditions—as written and applied—remain consistent with applicable law, regulations, and policies, and verify all parties' adherence to the terms and conditions within the agreement. ICE Program Offices should reach out to those applicable ICE Key Stakeholders for guidance and input. This maintenance process should also include verifying that current training practices and resources for supporting the information and data sharing activity are current and relevant.

Agreements may also contain reporting requirements that delineate the specifics of what must be reported back to DHS and at what intervals; for agreements that require partners to provide feedback or reports to DHS or ICE, ICE Program Offices should verify that the reporting mechanisms (e.g., points of contact or group email addresses) are still valid in the agreement. Some agreements call for periodic reviews by both (or all) parties. It is advised that after these reviews, the parties will either affirm their intent to continue the information or data sharing agreement in writing or modify or terminate the agreement consistent with the requirements of that agreement.

IGP will oversee the maintenance, auditing, and termination of ISAAs performed by ICE Program Offices. This oversight is to help ensure ISAAs are regularly being reviewed for changes in the purpose of the ISAA, the use of the information and data sets shared, the points of contact for the parties, etc. The goal for maintenance of ISAAs is to have accurate, active ISAAs that clearly identify the information and data being shared, how that information and data will be used, and the alignment of that use with the missions of DHS and ICE.

Appendices

Appendix A: Definitions and Commonly Used Terms

Bulk data transfer. The collection or dissemination of large quantities of intelligence or information, a significant portion of which is not reasonably likely to have any ultimate intelligence or operational value to the recipient, but which is provided to the data recipient for the recipient to identify information of intelligence or operational value within it.

Customs Mutual Assistance Agreements (CMAA). These are binding agreements that are entered into between the United States and a foreign country. ICE and U.S. Customs and Border Protection (CBP) enter into a CMAA on behalf of the United States, and the foreign customs administration enters into the CMAA on behalf of the foreign country. The purpose of a CMAA is to facilitate the exchange of information and documents as well as investigative assistance between the United States and the foreign country concerning customs offenses.

Data Access Review Council (DARC). A DHS coordination body consisting of representatives from the DHS Office of Intelligence and Analysis (I&A), the DHS Office of Policy, the DHS Privacy Office, the DHS Office of Civil Rights and Civil Liberties, and the DHS Office of the General Counsel that serves as the coordinated oversight and compliance mechanism for the review of departmental initiatives and activities involving the internal or external transfer of Personally Identifiable Information (PII) through bulk data transfers in support of the Department's national and homeland security missions.

Executive Agent. The ICE Executive Associate Director (EAD) aligned with the category of information addressed by the ISAA, responsible for overseeing the development and signing of the respective ISAA. For law enforcement information, the Executive Agents are the HSI and ERO EADs. For homeland security information, the Executive Agent is the HSI EAD. For immigration administration information, the Executive Agent is the ERO EAD. For business operations information, the Executive Agent is the M&A EAD. The Executive Agent is responsible for facilitating the development of the ISAA through collaboration with relevant ICE Program Offices to ensure potential legal, policy, civil rights and civil liberties, classification, technical, and data breach risks prior to finalization of the ISAA.The ICE Executive Agent is tasked with developing and maintaining standards, developing training programs, coordinating administrative support, and providing ICE-wide visibility of the designated activity.

Information Sharing and Access Agreement (ISAA). An agreement that is used to facilitate the exchange of information between the Department (or any element or entity within the Department) and one or more outside parties. Agreement types include, but are not limited to, Memorandums of Understanding (MOU), Memorandums of Agreement (MOA), Memorandums of Cooperation (MOC), Letters of Intent (LOI), or agreements related to pilot projects. Parties include domestic or foreign entities in the private or public sector and government agencies at the Federal, State, or local level.

Information Sharing and Safeguarding Governance Board (ISSGB). A Departmental Steering Committee and decision-making body for DHS collaboration on information sharing and safeguarding issues. Where appropriate, the ISSGB reviews ICE ISAAs to determine whether an exception to the One DHS Rule is warranted, but does not otherwise review

individual ICE ISAAs. The ISSGB develops and oversees the implementation of the Department's information sharing and safeguarding strategy, establishes goals and priorities relating to information sharing and safeguarding, and ensures consistency in information sharing and safeguarding policy and procedures both within the Department and between the Department and other Federal agencies, State and local governments, and private sector and international partners.

Interagency Agreement (IAA). An agreement between Federal agencies which is part of an interior intra-agency transaction, for goods and services to be provided by a servicing agency in support of a requesting agency. An IAA is required for assisted acquisitions and Interagency Reimbursable Work Agreements. Specific formats of IAAs are negotiated between agencies, also known as Trading Partners.

Interconnection Security Agreement (ISA). An agreement between system owners that facilitates the direct connection of two or more information technology (IT) systems for the purpose of sharing data and other information resources. An ISA is a follow-on, implementing agreement to an ICE ISAA that describes the purpose(s) of interconnecting the IT systems, identifies the terms under which interconnection may occur, the methods and levels of interconnectivity, and addresses potential security risks associated with such interconnection.

Interface Control Agreement (ICA). An agreement between system owners that defines the direct connection of two or more IT systems and details how these systems exchange data and to a lesser extent, how system functionality is implemented through these data exchanges. An ICA is a follow-on, implementing agreement to the ISA and provides detailed functional and technical details.

Key Stakeholder. Subject-matter experts in the areas of privacy, civil rights and civil liberties, information classification, records management, information technology, information governance, intelligence, ICE and DHS policy, and legal issues, and Program Offices responsible for the information and data involved. ICE Key Stakeholders provide their expertise to ICE Program Offices during discussions, negotiations, and development of ICE ISAAs. Depending on the information and data being shared or accessed, or the scenario of the information and data's use, specific ICE Key Stakeholders will need to participate early in the ISAA process. It is the Executive Agent's responsibility to have all relevant Key Stakeholders involved during the ISAA development process.

Law Enforcement Sensitive. A type of Sensitive But Unclassified/For Official Use Only information that is compiled for law enforcement purposes and which the loss or misuse of, or unauthorized access to could adversely affect the national interest or the conduct of investigative work, disclose the identity of a confidential informant or source of information, endanger life or physical safety, or impact the privacy protections afforded to individuals under applicable law, regulation, and policy.

Letter of Intent (LOI). A written document with and between DHS and a domestic or foreign partner, including governmental and private entities, expressing a desire to enter into a Memorandum of Understanding, Memorandum of Agreement, or other form of arrangement at a

future date. An LOI signifies the genuine interest of all parties in reaching a final agreement contingent upon more detailed due diligence and negotiations. If applied to data and information exchanges, an LOI can be a type of ICE ISAA.

Memorandum of Agreement (MOA). A document that describes in detail the terms of the relationship, the specific responsibilities of, and actions to be taken by DHS and a domestic or foreign partner, including governmental and private entities, so that their goals may be accomplished. MOAs are regularly used for financial types of transactions and for support agreements.

Memorandum of Cooperation (MOC). A document that describes the terms of the relationship between DHS and a domestic or foreign partner, including governmental and private entities. MOCs are regularly used with foreign entities. [13]

Memorandum of Understanding (MOU). A document that describes the broad concepts of mutual understanding, goals and plans between DHS and a domestic or foreign partner, including governmental and private entities.

One DHS Rule. A DHS policy that states, for information sharing and safeguarding purposes, including for purposes of Title 5, United States Code, Section 552a, "Privacy Act of 1974," the Department is one agency, and no Component is a separate agency from another Component. In accordance with the One DHS Rule, Components share information as one Department, rather than as separate entities to the extent permitted by and consistent with those Component Heads' authorities and any restrictions imposed by statute, Executive Order, Presidential or other directive, or national or Departmental policy.

Personally Identifiable Information (PII). Information that permits the identity of an individual to be directly or indirectly inferred, including other information that is linked or linkable to an individual. "Individual" includes, but is not limited to, U.S. citizens, lawful permanent residents, visitors to the United States, and Department employees and contractors.

Service Level Agreement (SLA). An agreement establishing a defined, constrained, objective relationship in contractual terms between a service provider and a customer with respect to the delivery of a service. An SLA is a follow-on, implementing agreement to an ICE ISAA and defines the expected level of services, the metrics associated with these services, acceptable and unacceptable service levels, and incentive awards for service levels exceeded and/or penalty provisions for services not provided. Applicable ICE Directorates and Program Offices are responsible for executing SLAs.

Sensitive Personally Identifiable Information (SPII). Sensitive PII is PII which, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some categories of PII are sensitive as stand-alone data elements. Examples include: SSN, driver's license or state identification number, passport number, Alien Registration Number, or financial account

[13] Please note that a MOC may be titled a MOU or MOA at the request of the foreign partner.

number. Other data elements such as citizenship or immigration status, medical information, ethnic, religious, sexual orientation, or lifestyle information, and account passwords, in conjunction with the identity of an individual (directly or indirectly inferred), are also Sensitive PII.

Special Protected Classes of Data (SPC). Data and other information subject to specific nondisclosure provisions and other limitations on use under existing law and policy, including but not limited to sections 222(f) (Department of State visa records); 244(c)(6) (temporary protected status), and 245a(c)(5) (adjustment of status of certain entrants) of the Immigration and Nationality Act; 8 U.S.C. § 1367 (Violence Against Women Act claims); 8 C.F.R. § 214.11(e) (T and U non-immigrant claims); and 8 C.F.R. § 208.6 (asylum information; protections afforded to refugee data as a matter of DHS policy), and Convention Against Torture (CAT) data (afforded protection as a matter of DHS Policy).

Third Agency Rule. A principle that restricts the release of shared information. Information originating in one U.S. agency shall not be disseminated by another agency to which the information has not been made available without the consent of the originating agency. It is DHS policy that information from another government agency is subject to that agency's policy and regulations concerning dissemination of the information unless other arrangements have been made. For ICE, the Third Agency Rule is also applied towards external parties or foreign partners, thus restricting further dissemination of ICE information and data without prior approval. It is also important to note, as established in the One DHS Rule, DHS components are not separate agencies for the purpose of information sharing, thus, the Third Agency Rule may not be used to restrict sharing within DHS components.

Appendix B: Exemptions to the ISAA Process

Below is a non-exhaustive list of common scenarios when ICE Program Offices would NOT be required to follow the clearance process as outlined in the ICE Information Sharing and Access Agreements Directive and Handbook. Even if an agreement meets the conditions of an exception, Program Offices may still request review and expertise from the relevant ICE Key Stakeholders.

Exemptions: The general requirements described in Directive Number 4006.1 do not apply under the following circumstances.

1. **Court Procedures:** Where information is shared with a court, magistrate, or administrative tribunal due to a court order or in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations, or in connection with criminal law proceedings.

2. **Legal:** Where the information at issue is generated by the ICE Office of the Principal Legal Advisor, including attorney-client privileged, deliberative and attorney-work product information.

3. **FOIA and Privacy Act Requests:** Where individual requests for information are made under the Freedom of Information Act (FOIA) or Privacy Act.

4. **Contracted Vendors:** Where ICE has entered into a contract with a vendor and the transaction of information is necessary to complete the service under contract.

5. ***Ad Hoc* Requests:** Where individual *ad hoc* requests for information are made, such as those from Congress, the White House, and the media. Additionally, when *ad hoc* requests for information are made by agencies, entities, and persons in order to comply with Executive Orders, laws, and regulations.

6. **Routine Operational or Law Enforcement Activity:**
   Where the information shared relates to specific case information to enhance ongoing investigative or law enforcement activities (e.g., criminal investigation or immigration enforcement) or for litigation purposes including discovery and settlement negotiations. This exemption is limited to individual cases, not continual or enduring exchanges of information between ICE and parties external to DHS. For example, exchanging information and data, such as multiple criminal investigation cases through a Task Force requires an ISAA in place prior to the exchange of ICE information. ICE may coordinate with local law enforcement to exchange information or data to assist in the progress of a specific case without an established agreement. Other activities that this exemption covers include local system access agreements where no ICE data is being shared, and investigative or law enforcement support agreements that facilitate the exchange of training materials.

7. **Sensitive Law Enforcement Activity:** Where the nature of either the agreement itself, or the information to be shared under an agreement, is of a particularly sensitive law enforcement

nature. The decision to designate an agreement or the information being shared as law enforcement sensitive, thereby exempting the agreement from the ICE ISAA process, must be approved by the Executive Associate Director of the ICE Directorate (i.e., HSI or ERO).

8. **Regulatory Compliance:** Where information is transferred or access to information is provided in furtherance of a regulatory compliance activity (e.g., transfer of records to the National Archives and Records Administration) or to satisfy obligations to authorized oversight entities such as the Government Accountability Office or the Office of Special Counsel.

9. **Liaison Relationships:** Where authorized information or knowledge is transferred through an established liaison, such as the exchange of information between personnel assigned to a foreign or domestic interagency or intergovernmental task force, fusion center, or U.S. Embassy. Agreements that establish a liaison relationship are not exempt from the review clearance process. This exemption may only be used if a liaison agreement has already gone through the ICE ISAA process and been executed by all parties; or if there is already a clearance process in place for liaison relationships such as National Security Decision Directive (NSDD) 38 related to overseas full-time mission staffing for all U.S. Government agencies.

10. **Exigent Threat:** Where the Secretary or Deputy Secretary of DHS, or the ICE Director, or their designee(s), determines that a clear, imminent threat exists and that the failure to provide or receive information before a written ISAA is executed is reasonably likely to endanger national or homeland security, ICE must utilize its exigent threat standard operating procedures, or the I&A ISE-003 Standard Operating Procedure (SOP): Response to Bulk Data Information Sharing Request Regarding an Exigent Threat. When the sharing of bulk data and its use are not addressed in an existing ISAA, ICE must follow the I&A ISE-003 SOP. If the requested bulk data and its use are addressed in a previously signed ISAA then ICE should follow relevant ICE SOP(s) for addressing exigent threat requests. If the sharing of the requested bulk data is not addressed in an existing ISAA, the information sharing arrangement must be memorialized in an ISAA no later than five business days from the execution of the data transfer, unless otherwise approved by the Secretary or Deputy Secretary of DHS, or the ICE Director, or their designee(s).

11. **287(g) Agreements:** As authorized by Section 287(g) of the Immigration and Nationality Act, where ICE enters into agreements with state and local law enforcement agencies to delegate immigration enforcement functions to designated law enforcement officers who, once trained and certified, may perform delegated functions under ICE supervision and direction.

12. **Interconnection Security Agreements (ISA):** Where ICE has already entered into an ISAA and requires the direct connection of two or more information technology (IT) systems for the purpose of sharing data and other information resources. An ISA is a follow-on, implementing agreement to an ICE ISAA that describes the purpose(s) of interconnecting the IT systems, identifies the terms under which interconnection may occur, the methods and

levels of interconnectivity, and addresses potential security risks associated with such interconnection.

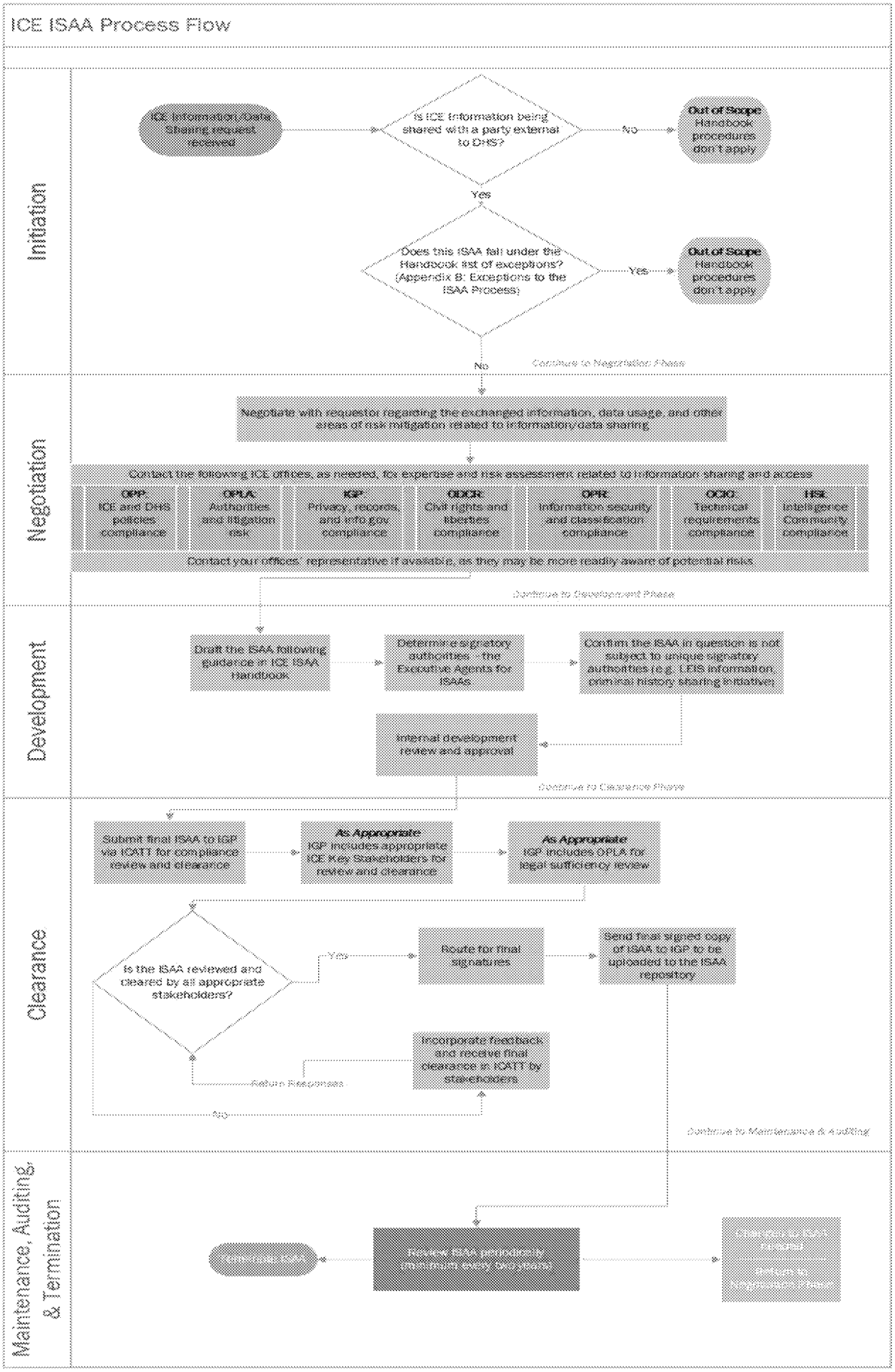
13. **Interface Control Agreements (ICA)**: Where ICE has already entered into an ISAA and ISA. The Parties require the direct connection of two or more IT systems and require details as to how these systems exchange data and to a lesser extent, how system functionality is implemented through these data exchanges. An ICA is a follow-on, implementing agreement to the ISA and provides detailed functional and technical details.

14. **Service Level Agreements (SLA):** Where ICE already has entered into an ISAA and the sharing of information is subject to defined, constrained, objective relationship in contractual terms between a service provider and a customer with respect to the delivery of a service. An SLA is a follow-on, implementing agreement to an ICE ISAA and defines the expected level of services, the metrics associated with these services, acceptable and unacceptable service levels, and incentive awards for service levels exceeded and/or penalty provisions for services not provided. Applicable ICE Directorates and Program Offices are responsible for executing SLAs.

15. **Interagency Agreements (IAA):** Where ICE enters into agreements internal to ICE and DHS, or with other Federal agencies for goods and services to be provided by a servicing agency in support of the requesting agency. The IAA must provide the information required to demonstrate a bona fide need exists and authorize the transfer and obligation of funds.

16. **Customs Mutual Assistance Agreement (CMAA):** Where ICE, in cooperation with CBP, enters into agreements with foreign customs administrations for the purpose of exchanging information, documents, and investigative assistance between the United States and the foreign country concerning customs offenses.

Appendix C: ISAA Process Flow



Appendix D: Authorities/References

Executive Order 13526: Classified National Security Information, dated December 29, 2009.

Title 5, U.S. Code, Section 552a, Privacy Act of 1974, as amended.

DHS Delegation Number 23014, *Delegation to the Assistant Secretary for Policy Regarding Information Sharing*, dated January 3, 2017, as updated or superseded.

DHS Directive Number 262-05, *Information Sharing and Safeguarding*, dated September 4, 2014, as updated or superseded.

Policy Directive Number 262-15, *The Department of Homeland Security's Federal Information Sharing Environment Privacy and Civil Liberties Policy*, dated June 5, 2009, as updated or superseded.

DHS Directive Number 0450.1, *Memoranda of Understanding (MOU) and Memoranda of Agreement (MOA)*, dated January 24, 2003, as updated or superseded.

DHS Instruction Number 262-05-001, *DHS Information Sharing Environment*, dated September 12, 2014, as updated or superseded.

DHS Secretary Chertoff Memorandum, *DHS Policy for Internal Information Exchange and Sharing* (commonly known as the One DHS Rule), dated February 1, 2007, as updated or superseded.

Under Secretary for Intelligence and Analysis Allen Memorandum, *Policy Guidance: Implementation of the One DHS Information Sharing Memorandum—Information Sharing Access Agreements*, dated February 6, 2008, as updated or superseded.

Privacy Policy Guidance Memorandum 2017-01, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information*, dated April 25, 2017, as updated or superseded.

DHS Information Sharing and Safeguarding Governance Board Charter, as amended, dated June 16, 2015, as updated or superseded.

DHS Data Access Review Council Charter, dated February 09, 2015, as updated or superseded.

DHS Handbook for Safeguarding Sensitive Personally Identified Information, revised December 2017, as updated or superseded.

DHS Instruction Manual 121-01-011, The Department of Homeland Security Administrative Security Program, April 25, 2011, as updated or superseded.

ICE Delegation Order 0001, *Delegation of Authority to the Directors, Detention and Removal and Investigations, and to Field Office Directors, Special Agents in Charge and Certain Other Offices of the Bureau of Immigration and Customs Enforcement*, dated June 6, 2003, as updated or superseded.

ICE Delegation Order 73008.1, *Authority to Sign Law Enforcement Information Sharing and Access Agreements*, dated September 2, 2009, as updated or superseded.

ICE Directive 2-8.0, *Service Level Agreement Policy*, dated February 1, 2008, as updated or superseded.

ICE Directive 4003.2, *Safeguarding Law Enforcement Sensitive Information,* dated May 20, 2014, as updated or superseded.

ICE Directive 12002.2, *Non-Routine Assistance Requested by the U.S. Intelligence Community*, dated September 11, 2015, as updated or superseded.

HSI Delegation Order 10001.1, *Authority to Sign Memoranda of Understanding and Memoranda of Agreement Within Homeland Security Investigations,* dated June 3, 2011, as updated or superseded.

ERO Delegation Order 130002, *Authority to sign and enter into cooperative agreements, such as Memoranda of Understanding, Memoranda of Agreement, and Memoranda of Cooperation, with foreign government agencies as it pertains to the Criminal History Information Sharing initiative within Enforcement and Removal Operations*, dated June 21, 2018, as updated or superseded.

ERO Delegation Order 130003, *Authority to Sign Memoranda of Understanding and Memoranda of Agreement Within Enforcement and Removal Operations*, dated Feb. 21, 2020, as updated or superseded.

Appendix E: Special Cases and Considerations for Classified Agreements

ICE ISAAs that enable sharing of classified information and data or involve sharing of information or data with a classified mission partner should be drafted according to the guidelines in this *Handbook*, however the agreement itself or the fact that there is an agreement may be classified. In those instances, drafting of the agreement should only occur on Homeland Secure Data Network (for SECRET agreements) or C-LAN (for TOP SECRET agreements) with notifications sent via secure electronic mail or other protected notification processes according to the requirements for handling classified material. ICE HSI Office of Intelligence (HSI Intel) is the Executive Agent for classified agreements and will be involved with all classified agreements.

Constitutionally Protected Activities and Special Protected Classes of Data including 8 U.S.C. § 1367

Constitutionally Protected Activities, Civil Rights, and Civil Liberties

Even when an ICE ISAA does not involve sharing PII, civil rights or civil liberties must be a consideration if the agreement includes information collected or aggregated based on special protected classes such as race, ethnicity, national origin, or religious affiliation, or based on constitutionally protected activities, such as First Amendment rights. Information and data aggregated or gathered based on such categories have potentially significant civil rights and civil liberties impacts and ICE Program Offices must closely coordinate with the oversight and legal offices, particularly OPLA and ODCR, early and often during the initial phases of development.

Individuals with pending or approved Violence Against Women Act (VAWA), T Visa, or U Visa applications (8 U.S.C. § 1367)[14]

ICE personnel cannot disclose any information about these categories of individuals outside of DHS unless the information to be shared falls into an exception enumerated by the statute.[15] This absolute confidentiality covers the entire person, not just information contained in VAWA, T Visa, or U Visa applications. The confidentiality requirement extends to both primary applicants and beneficiaries listed on the application.

Section 1367 information is any material regarding individuals who are seeking or have been approved for nonimmigrant or immigrant status as (1) battered spouses, children, or parents under provisions of the Violence Against Women Act (VAWA); (2) as victims of a severe form of human trafficking who generally are cooperating with law enforcement authorities (T nonimmigrant status); or (3) as alien victims who have suffered substantial physical or mental abuse as the result of qualifying criminal activity and have been, are being, or are likely to be helpful in the investigation or prosecution of that activity (U nonimmigrant status). This includes

---

[14] DHS Delegation Number 19004, "Delegation of Authority to Issue Guidance and Implement 8 United States Code 1367," September 23, 2013.

[15] Please contact OPLA's Government Information Law Division (GILD) for questions relating to disclosure under 8 U.S.C. § 1367. (b)(7)(E) @ice.dhs.gov.

information pertaining to qualifying family members who receive derivative T, U, or VAWA status. Because Section 1367 applies to *any* information and data about a protected individual, this definition includes records or other material that do not specifically identify the individual as an applicant for or beneficiary of T nonimmigrant status, U nonimmigrant status, or relief under VAWA.

Additional Restrictions on Disclosure

Pursuant to law, regulation, and applicable policy, ICE personnel are prohibited from disclosing outside of DHS information about the following types of applications or claims. This restriction on disclosure includes the fact that an application or claim has been made, as well as any information pertaining to the application or in the claim or raising an inference that the individual has filed an application or claim:

- Asylum, Withholding of Removal, Convention Against Torture, Refugee status, NACARA, and credible or reasonable fear proceedings. (8 C.F.R. § 208.6)
- Temporary Protected Status
- Special Agricultural Worker (SAW), Legalization, and LIFE Act.
- S Visa and Confidential Informant information
- Visa Records per the Immigration and Nationality Act (INA) § 222(f)

For questions regarding these legal and regulatory restrictions on the disclosure of information, ICE personnel should contact OPLA GILD **(b)(7)(E)** @ice.dhs.gov).

Private Sector

Information sharing with the private sector involves unique considerations which may require consultation with OPLA at the initiation of discussions.

Appendix F: Tips to Expedite the Review Process

Office of Information Governance and Privacy

Privacy Unit

Why it is Important to Engage with ICE Privacy

Proactively engaging with ICE Privacy during the negotiation phase of ISAA development is critical to identifying potential restrictions and risks regarding the sharing of personally identifiable information (PII),[16] especially Sensitive PII.[17] Even when data sets are de-identified, privacy implications can still arise. Engaging ICE Privacy early and throughout the project's lifecycle, not only aligns with the Fair Information Practices Principles (FIPPs)[18] (discussed more fully below) but will also help achieve the project's goals and ICE's mission. Without expert eyes to review the information request and determine any potential privacy risks, it is possible that a privacy incident could result. Privacy incidents can cost the agency money, time, and reputation. They can also cause damage to the individuals whose information/data is released without authority, including physical and reputational harm, and can cost the individual time and money related to identity theft. These costs, to both the agency and individuals, can be difficult to recoup once a breach occurs.

Privacy Basics related to Information/Data Sharing and Disclosure

The Privacy Act of 1974, as amended (see 5 U.S.C. § 552a)[19] governs whether you can disclose information about an individual[20] from ICE or DHS record systems. DHS policy also provides guidance specific to the handling of non-U.S. persons' PII.[21] Determining if you have authority to share information can be difficult, but ICE Privacy can help guide you in making decisions about disclosures to persons outside DHS.

---

[16] DHS defines PII 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, legal permanent resident, visitor to the U.S., or employee or contractor to the Department.

[17] A subset of PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if the data is inappropriately accessed or compromised.

[18] DHS uses the FIPPs in Privacy Impact Assessments (PIAs), oversight activities, information sharing agreements, privacy policies, redress activities, and its other privacy responsibilities. See Fn. 8, Privacy Policy Guidance Memorandum 2017-01, DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information ("DHS Memorandum 2017-01"), *available at* https://www.dhs.gov/sites/default/files/publications/PPGM%202017-01%20Signed_0.pdf.

[19] Privacy Act of 1974, as amended (see 5 U.S.C. § 552a), *available at* https://www.govinfo.gov/content/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf.

[20] This applies to disclosures made about U.S. Citizens, Lawful Permanent Residents, or those whose records are covered under the Judicial Redress Act (JRA).

[21] Privacy Policy Guidance Memorandum 2017-01, DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information, *available at* https://www.dhs.gov/sites/default/files/publications/PPGM%202017-01%20Signed_0.pdf.

Keep in mind, even if the Privacy Act authorizes disclosure, other legal restrictions on disclosure may limit your ability to share the information. Please see additional guidance via the ICE Implementation Guidance for DHS Privacy Policy 2071-01.[22] Remember, you can always contact ICE Privacy if you need help.

What ICE Privacy Looks For

It is ICE Privacy's practice to follow the FIPPs when assessing privacy risks. The FIPPs are principles taken from the Privacy Act of 1974 and form the basis of the DHS and ICE privacy compliance policies and procedures governing the use of PII. These principles are: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing.[23] The FIPPs are used to assess and enhance privacy protections by analyzing the nature and purpose of the collection of PII to fulfill DHS and ICE's missions and how we can best provide privacy protections in light of these principles.

When sharing information with external parties, there are particular principles that are applied when ICE Privacy is assessing the sharing request:

Purpose Specification

Articulate the authority that permits the collection of PII and specifically identify the purpose(s) for which the PII is intended to be used. Precise descriptions of the data sources, types, and fields are required with justification for each according to the intended purpose.

Data Minimization

Only share PII that is directly relevant and necessary to accomplish the specified purpose(s) and allow the recipient to only retain PII for as long as is necessary to fulfill the specified purpose(s).

Use Limitation

The request clearly identifies the intended use of the data. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

Limits the use of PII by the recipient to those that are permissible under law and articulated in published PIAs and SORNs. For external sharing, these uses are legally defined "routine uses," and must be compatible with the original collection and purpose specification. Absent a statutory requirement to disclose specific information, such routine use sharing decisions are made following a case-by-case review by the ICE Privacy Unit to ensure a request meets the requirements. Sharing PII with external entities is done pursuant to routine uses articulated in published SORNs and may also be authorized by a written information sharing agreement, such as a Memorandum of Understanding, between the Department/ICE and the receiving agency.

---

[22] ICE Implementation Guidance for DHS Privacy Policy 2071-01, *available at* **(b)(7)(E)**

[23] The Fair Information Practice Principles at Work, *available at* https://www.dhs.gov/sites/default/files/publications/dhsprivacy_fippsfactsheet.pdf.

Ensure there is an actual need for the data being shared, and that it links with the purpose and use. In some cases, data is over-disclosed simply because no one asked whether disclosure of the data was necessary. Look for ways (if there are any) to minimize the disclosure of unnecessary and/or high-risk data (e.g., SSNs).

Co-mingling ICE data with other datasets, especially commercial data can cause privacy concerns. If there will be co-mingling of data, it is important to discuss this proposed activity with ICE Privacy prior to this occurring.

Data Quality and Integrity
Clearly state the processes used to maintain data accuracy through edit/change/delete practices, including how data changes will be communicated to the data source.

Depending on the nature of the dataset, it may be necessary to update the data frequently and replace the old data entirely. Identify whether reliance on outdated information could be detrimental to individuals' interests and if so, the ISAA should contain provisions addressing controls that ensure data is refreshed at an appropriate interval and obsolete data is deleted. This will help ensure that outdated data is neither included in datasets, disseminated, nor relied upon for operational purposes.

Are there known accuracy concerns with data we are providing to the recipient? For example, in some systems it is well know that data in a certain field should not be relied upon as accurate. The recipient agency may be unaware of this. Question whether the inaccurate data field should even be provided, and if it is, look for ways to alert recipient to the accuracy concern, including a provision in the ISAA and marking of the paper or electronic records disclosed.

Security
Confirm the protection of PII (in all media) by the recipient through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure. Identify what safeguards and controls are in place to protect the information from non-compliance with Department policies, ISAA terms, and with the FIPPs.

Accountability and Auditing
Ensure that you are accountable for complying with these principles and are auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

How to help ICE Privacy Expedite its Review
Identify DHS sharing agreements already in place with External Party
If there is a DHS level sharing agreement that the ISAA is based on or will be part of, provide a copy of this agreement to ICE Privacy. This will allow ICE Privacy to identify any previously identified privacy-related documentation and DHS level privacy risk assessment and mitigation approaches.

Identify the System that the Data is Coming From
If the data is being shared from an ICE or DHS system, please provide the system name.

Identify what information or data is being shared
If the information relates to a person, ICE Privacy can review the type of information to determine the risk level if that individual's information is exposed in an unauthorized manner. ICE Privacy will review the data to ensure that ICE shares only as much PII as is necessary to achieve the mission. For example, if a mission can be achieved without sharing PII, ICE Privacy will require the data be removed from the dataset entirely or otherwise masked to limit the risk of re-identification. This helps reduce the level of risk of identity theft or other harm to individuals if a privacy incident occurs. It also mitigates harm to the agency if such data is exposed.

Identify the purpose of the sharing and how the information will be used
Provide ICE Privacy with the original purpose of the collection of the information and how the information would be used. Does the purpose of the sharing and use of the information align with the original collection? All uses of PII must be compatible with the uses stated at the point of collection of that data. There are exceptions however, so identifying the authority to share is important.

Identify authority to share PII outside of DHS/ICE
From the list below, identify for ICE Privacy what authority option allows the information to be shared outside of DHS/ICE:

- The person whose PII is being shared requests or consents to the sharing; **or**
- The recipient's need for the information is related to his or her official duties; **and**
- If the PII is contained in records covered by a system of records, there must be an authorized disclosure exception (e.g., a published routine use in the applicable SORN) that permits sharing pursuant to the Privacy Act, as amended, 5 U.S.C. § 552a; **and**
- The sharing of PII to third parties must be consistent with Department policy, including DHS's privacy policies and information-sharing policies; **and**
- Sharing must be consistent with all ICE policies.

If sharing is covered by a system of records notice (SORN), identify the disclosure exception (e.g., routine use(s))
Provide ICE with the SORN title(s) and associated routine use letter(s) from each SORN.[24] This will allow ICE Privacy to quickly review those documents and the specific routine use(s) identified. Otherwise, ICE Privacy must research all potentially applicable SORNs including all routine uses.

Records and Data Management Unit

Why it is Important to Engage with ICE Records

[24] All DHS SORNs are posted on the DHS Privacy Office website, *available at* www.dhs.gov/privacy

Engaging with ICE Records during the negotiation phase of the ISAA development is important for identifying the length of time the data being shared can be maintained by the requesting party.

By following the NARA-approved records retention schedules, which are determined based on the value of the information, agencies maintain data only so long as it is valuable. Additionally, following retention schedules helps minimize privacy issues due to privacy incidents, data calls related to litigation holds and FOIA requests on data that is overdue for disposition based on its retention schedule.

Records Basics Related to Information/Data Sharing and Disclosure

The Federal Records Act (FRA) provides the legal framework for Federal records management, including record creation, maintenance, and disposition. The FRA governs agencies' records management responsibilities. A few of these responsibilities include:

1. Records are made or received by a Federal agency either to comply with a law or to conduct public business. As a result, they belong to the Government rather than to individuals, and their legal disposition depends on the prior approval of the Archivist of the United States.
2. Records are, or should be, preserved because they constitute evidence or contain information of value. They document an agency's organization, functions, and activities or the persons, places, things, or matters dealt with by an agency.
3. Records vary widely in their physical form or characteristics. They may be on paper, electronic, audiovisual, microform, or other media.

Clearly articulated recordkeeping requirements are essential for creating adequate and proper documentation.

What ICE Records Looks For

It is ICE Records' practice to follow the FRA and guidance provided by NARA when assessing records risks. When assessing records risks related to information sharing to external parties, ICE Records' primary areas for concern revolve around ownership, retention, and secondary dissemination of the records.

Ownership

The ISAA should also address record ownership issues. ISAAs between Federal agencies subject to the Federal Records Act need to have a clearly defined provision as to who owns the shared records (once the recipient receives them) for the purposes of FRA, Privacy Act and FOIA. The ISAA should also require the parties to review and update their record schedules, PIAs, and Privacy Act SORNs as needed considering the ISAA.

Retention

Retention schedules will be tailored in each case to existing operational needs, the purposes for which the data will be used, the amount of information relating to U.S. persons contained in the data, and the overall sensitivity of the data shared. Mere speculation or possibility that DHS data could contain terrorism or other information related to the national security, or that unknown information may later reveal a currently undetected link to terrorism or national security threats,

is insufficient to warrant prolonged or indefinite retention of data that has not been identified as terrorism information. Absent prior written authorization from DHS leadership, IC partners must purge data in accordance with the NARA approved schedules.

ICE data should only be used in accordance with established guidelines and retention schedules. The use of derogatory data/information are governed separately through applicable policies, laws, and regulations that mandate how it will be maintained, archived, and disposed. Maintaining information longer than the associated records schedule can cause risk as the longer the information is retained, the more likely that it will be accessed or exposed without proper authority and may be used for purposes beyond the initial request.

The retention schedule for the information maintained in ICE systems are identified as the original record and those retention schedules apply to this original record.

Dissemination
If a new record is created by the recipient organization from ICE data/information that was disseminated, then it is incumbent upon the recipient to ensure that a records schedule exist or is created for retaining such data/information.

How to help ICE Records Expedite its Review

Does the ISAA clearly state who owns the data
Provide this information to ICE Records, as it is needed for purposes of the Federal Records Act, Privacy Act, FOIA. This is also necessary for declassification purposes, if the information is identified as being classified.

Identify how long the recipient party is to keep the data
Provide ICE Records with the records retention schedule that covers the information to be shared.

Work with ICE Records to determine how long the recipient party is permitted to retain the data in their IT or recordkeeping systems (may want exception for information reincorporated into new records created by recipient).

Identify whether recipients will notify DHS/ICE of requests or demands for disclosure, forced disclosures to public or in court
Responding to demands for disclosure is similar to secondary dissemination, however there are caveats when it comes to disclosing personal information on individuals, particularly to the public. When U.S. persons provide information to United States Government agencies, certain protections are afforded to them. Disclosing Federal records on individuals must be discussed at a minimum with OPLA, IGP, and OPA.

Appendix G: DHS Information Sharing and Access Agreement Template

This template is a resource for internal ICE use. It is intended to provide a flexible guide to negotiations and an example of the sections and language that may be included in an ISAA. It may not be appropriate to include all sections or language used in the template, and there may be sections or language that need to be included that are not accounted for in the template.

Version 1.0
Revised: 09/09/2020

MEMORANDUM OF AGREEMENT/UNDERSTANDING/COOPERATION

BETWEEN

THE DEPARTMENT OF HOMELAND SECURITY

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT

[ICE DIRECTORATE]

AND

[EXTERNAL PARTY]

REGARDING [SUBJECT MATTER]

I. **INTRODUCTION AND PURPOSE.** The U.S. Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement (ICE), [ICE Directorate] ("DHS") and [proposed recipient, External Party] ("External Party"), hereinafter collectively referred to as the "Parties," have entered into this Memorandum of Agreement/Understanding/Cooperation ("MOA"/ "MOU"/ "MOC" or "Agreement") to

[*example 1:* govern the information sharing, use and safeguarding] for the purpose of [purpose].

Or

[*example 2:* govern the information sharing, use, safeguarding and related cooperation] for the purpose of [purpose].

Or

[*example 3:* provide access to and/or data through [system] as specified within this Agreement for the purpose of sharing information within those systems] for the purpose of [purpose].

II. BACKGROUND.

[*Provide a brief description of* ***ICE****, as a component of DHS, responsibility related to subject matter of agreement and authority to share.*

[*Provide a brief description of* ***External Party*** *responsibility related to subject matter of agreement and authority to share.*]

[*If access to a system is to be provided by Agreement,* ***also add*** *a brief description of system.* ***Example:*** *The Student and Exchange Visitor Program (SEVP), managed by the Department of Homeland Security, U.S. Immigration and Customs Enforcement, maintains information on international students and exchange visitors and their dependents in F, M and J visa status in the United States, the schools that are DHS-certified to enroll international students, and the sponsors that are designated by State to host exchange visitors. SEVIS, SEVP's core technology, is a web-based tool for collecting, managing and reporting information on students, exchange visitors, schools, and sponsors and supports the administration of the SEVIS program. While SEVIS primarily collects and maintains information on non-immigrants who are not subject to the Privacy Act, the system does contain United States Citizen (USC) and Lawful Permanent Resident (LPR) information on the host families of some non-immigrants, and on former* non- *immigrants who have changed their status to a USC or LPR.*]

III. DEFINITIONS.

As used in this Agreement, the following terms will have the following meanings:

[*Define terms specific to this Agreement. If no definitions specific to the agreement, delete this section and renumber sections accordingly.*]

IV. AUTHORITY.

The information sharing and enhanced cooperation among the Parties to this [MOA/MOU/MOC] Agreement is authorized under and complies with the provisions of [DHS/ICE/Directorate] statutory and regulatory authority: [*list all applicable statutory and regulatory authority for each agency*] for [agency]
and for [External Party] [*list applicable statutory and regulatory authority*] for [agency].
[*Option for private party*] and for [External Party] that the executor of this agreement has authority to bind its organization to the terms of this agreement.

[*IF collecting/disseminating PII* - Information will be maintained and shared under the provisions of 5 U.S.C. § 552a, Privacy Act of 1974; [INSERT SPECIFIC DHS System of Records Notice (SORN), DHS/XXX, Date & Federal Register Citation.] and Section 208 of the E-Government Act of 2002; [INSERT SPECIFIC DHS UNCLASSIFIED Privacy Impact Assessment (PIA)]. *Please discuss with ICE Privacy Unit to verify that the Privacy Act and/or E-Government Act are applicable, or to identify the appropriate SORN and/or PIA.]*

V. RESPONSIBILITIES. The following roles and responsibilities have been defined for each of the parties to this [MOA/MOU/MOCMOA] [*enter the specific roles or requirements of each participating agency in the following areas*]:

A. DATA. DHS [shall/may] share [*describe the information/data to be made available or exchanged*]. [External Party] [shall/may] share[*describe the information/data to be made available or exchanged*].
Note: The parties to the agreement should come to a decision whether this is a binding or non-binding commitment.

B. DATA SENSITIVITY. It is the intent of the Parties to conduct the exchange of the information described herein at the [*Enter the sensitivity or classification level of the information to be exchanged, in particular, the highest sensitivity or classification for information to be shared.(i.e., Controlled but Unclassified)*]. Specific technical and security details are set forth in the SAFEGUARDS section, below, [*optional clause:* and in separate technical documentation.]

C. DELIVERY OF DATA. [*Enter a description of the requirements pertinent to the exchange of information/data among and between the parties. Clearly articulate what data is transmitted between each party. If direct access to a system is allowed, use option 3.*]

[*Delivery of Data – Option 1. Use if separate documents define technical standards. Must use this option if the DATA SENSITIVITY optional clause was used and no direct access of the system is contemplated.]* The attached documents [identify documents] provide the technical standards related to transfer of data between DHS and [External Party] as provided in this Agreement. In general, the Parties agree to use efficient, commercially available network and database technology to store and transfer data in a manner that will allow data to be transferred and updated in a real-time or near real-time manner. The Parties [are committed to updating the technologies employed to implement this Agreement to ensure maximum efficiency and data-sharing as data volumes increase and more efficient technologies become available.

OR

[*Delivery of Data – Option 2*] DHS will electronically transmit to the [title of External Party person responsible for receiving information] a dataset consisting [*add general description of data being sent*]. DHS will transmit the dataset to [External Party] via an agreed upon secure delivery system based on best practices and strong privacy protections.

Note: There may be alternative approaches to send, if necessary.

OR

[*Delivery of Data – Option 3. The business owner must draft a clause if the system will allow users of another system to directly access it. Specify the security parameters that are exchanged among/between systems that authenticates that the requesting system is the legitimate system and that the class(es) of service being requested are approved by the ISAA. Also, any additional security parameters that are required (like personal accountability) should be specified to allow the respondent system to determine whether a requestor is authorized to receive the information and/or services requested and whether all details of the transaction fall within the scope of user services authorized by the ISAA. See examples below*]

[*Delivery of Data – Option 3 – Example 1]* This Agreement provides for data sharing through the creation of user accounts and the transfer of data extracts. The Parties will continue to work together to develop and implement future real-time information exchange by separate agreement or separate addendum to this Agreement.

[*Delivery of Data – Option 3 – Example* 2] DHS will establish user accounts providing access to the [system] programs for [External Party] personnel at specified locations, including [specified locations, if any] [*optional clause:* and locations where [External Party] and DHS personnel are co-located]. DHS will transfer records on a timely, periodic basis to [External Party] from the [system] programs, as described in this Agreement. The periodic transfer of records will begin as soon as practicable. Separate addenda to this Agreement set forth the specific technical and operational requirements for the establishment of user accounts and the periodic transfer of data as described in this section.

D. SUPPORT. [*Describe the nature of analytic or technical services to be offered by each organization.*]

E. SAFEGUARDS. [*Summarize the measures that each party is required to take to reduce the risk of unauthorized or inadvertent disclosure of shared information, including handling, storage, destruction methods, and requirements for electronic, voice, fax, and website transmissions. If there are any specific equipment restrictions, describe the restrictions to be placed on terminals, including usage, location, and physical accessibility*]

[*Safeguards – option 1*] The Parties agree to maintain reasonable physical, electronic, and procedural safeguards to appropriately protect the information shared under this Agreement against loss, theft, or misuse, as well as unauthorized access, disclosure, copying, use, modification or deletion.

OR

[*Safeguards – option 2. Use if safeguards are based on statutory or regulatory requirements.*] DHS considers the information to be [category of information] under [statutory and regulatory citation] and will be handled in accordance with requirements for handling of [category of information].

AND/OR

[*Safeguards- option 3. A specific safeguard clause that can be used in conjunction with option 1 or 2.*] When the information is no longer used by the Parties, the Parties will delete all electronic data from their systems and all paper records that they have in their possession as a result of this project in such a manner as to render it unrecoverable.

F. TRAINING. [*Enter the details of any security awareness or training requirements and the assignment of responsibility for conducting it. If existing training will be used, so state.*]

[*Training – option 1*] The Parties shall be appropriately educated and trained regarding the proper treatment of personal information and proper care of the information systems to ensure the overall safeguarding of the information. Each Party will ensure that its employees, including contractors with access to any of the other Party's data, have completed privacy training on the handling of personal information.

OR

[*Training – option 2*] The [External Party] agrees to distribute to its [system] users the [title of User Handbook] and take steps to ensure that these users abide by the provisions of this document.

OR

[*Training – option 3*] Upon request from DHS, [External Party] will provide sufficient training and technical assistance to implement the transfer of [system] information and ensure appropriate interpretation of such information. This includes general training of a

core group of users in the functions of [system] to ensure accurate interpretation of the information. The core users would be utilized in a train the trainer program.

G. RECORDS. [*Describe any requirements for disposition/retention of records*]

The Parties will retain information covered under this Agreement only for as long as needed to fulfill the purposes stated in Section 1. In no instance will the retention period for any data item exceed the maximum period permissible by applicable legal and regulatory requirements or official retention policies. Each agency will dispose of the data accessed under this Agreement in accordance with its own records retention authorities.

H. USE. [*Describe any limits on authorized use of information*]

The information shared in accordance with this Agreement will be used only in a manner consistent with any statutory requirements, including privacy compliance requirements. [*Optional clause:* Each party will use the data only for the purpose stated in (statutory citation)].

Note: Consider if limitations of use imposed or expected from us will limit mission operations, such as using the information to advance investigations or to share such information with another Law Enforcement agency.

I. DISSEMINATION. [*Describe requirements for authorized access to information. Include a general clause and a "Third Agency" Rule clause.*]

[*Dissemination – general option 1*] The Parties will limit access to information covered under this Agreement to only those authorized personnel who have a need-to-know to carry out their official duties. This data will not be disseminated outside DHS without the expressed consent of [External party]. The data will not be disseminated outside of [External Party] without the express consent of ICE.

[*If the agreement is OneDHS compliant*] The signatories to this agreement have been made aware of the One DHS policy and identified the information sharing requirements, as they concern the sharing of proprietary private sector information, of the private sector party involved. Subsequent to this review, no non-disclosure concerns or other limitations on the sharing of information across DHS are present. Therefore, this Agreement entitles ICE representatives to share relevant information across DHS in accordance with the OneDHS policy.

OR

[*Dissemination – general option 2*] Each Party shall ensure that access to [insert marking level] information is limited to those persons who possess requisite security clearances [*optional clause:* and who have executed a non-disclosure agreement prohibiting unauthorized use and disclosure of information].

OR

[*Dissemination – general option 3*] All [External Party] personnel who receive user account access to the [system] programs must be verified as having a current [required security level, i.e., secret] or higher security clearance before being allowed access to the information.

AND [use one of the two options below]

[*Dissemination – Third Agency option*] Consistent with "Third Agency Rule" practice, before any information originating from ICE records can be disclosed to any third party other than exceptions required by law, e.g., Congress, Government Accountability Office, the courts, and the general public, the [External Party] will contact ICE to determine the appropriate action or response.

Should ICE and [External Party] agree to [External Party]'s disclosure of the information, [External Party] shall document the disclosure and provide such documentation to ICE.

Likewise, before any information originating from [External Party] records can be disclosed to any third party other than exceptions required by law, e.g., Congress, Government Accountability Office, the courts, and the general public, ICE will contact [External Party] to determine the appropriate action or response. Should ICE and [External Party] agree to ICE's disclosure of the information, ICE shall document the disclosure and provide such documentation to [External Party]. For the purposes of disclosure under this Agreement, components within DHS are not considered third parties or agencies.

OR

[*Dissemination – secondary sharing allowed]* The information provide pursuant to this Agreement may be shared with other agencies at the Federal, state, local, tribal, or foreign level, who, in accordance with their responsibilities, are lawfully engaged in collecting law enforcement, national security, and intelligence information and/or investigating, prosecuting, enforcing, or implementing civil and/or criminal laws, related rules, regulations, or orders. Such secondary sharing shall be carried out to the greatest extent possible, in a manner that permits the originating agency to know to whom the information has been provided.

J. PRIVACY.

The collection, use, disclosure, and retention of personal information shall be limited to that which is necessary for purposes of the Parties as set forth in this Agreement. Personally identifiable information will be maintained in accordance with [*cite applicable SORNs for both parties*].

Personally identifiable information shall be protected by administrative, technical and physical safeguards appropriate to the sensitivity of the information. Personally identifiable information will only be disclosed to authorized individuals with a verified need to know and only for uses that are consistent with the stated purposes under this Agreement and for which the information was originally collected.

K. COOPERATION/DECONFLICTION. [*Describe any coordination and/or deconfliction responsibilities*]
Note: This may be an optional provision.

[*Cooperation clause 1*] The Parties shall endeavor to work together to the greatest extent possible to achieve the maximum preventative, preemptive, and disruptive effect on potential threats, including coordinating simultaneous and complementary activities when appropriate.

The parties agree to coordinate operational activities to the greatest possible extent. Specifically, each party shall take all reasonable steps to ensure coordination and de-confliction of homeland-security-related law enforcement intelligence or national-security-related activities under its authority with such activities of the other party.

[*Cooperation clause 2*] Personal information shall, to the extent feasible, be as accurate, complete, and up-to-date as necessary for the purposes identified in this Agreement. The Parties shall cooperate with each other in this regard. The [External Party] will, in a timely manner, take appropriate action regarding any request made by the DHS for access, additions, changes, deletions, or corrections of personal information. In addition, the [External Party] will, in a timely manner, notify DHS of any data errors that it discovers.

[*Cooperation clause* 3] Where the Parties have a mutual investigative interest based on information shared pursuant to this Agreement, the Parties [will/may] coordinate with each other to determine the appropriate investigative/enforcement course of action. In such matters, unless there are exigent circumstances requiring immediate action, the [External Party] will verify information and coordinate with DHS before acting on leads or disseminating intelligence products developed as a result of information shared pursuant to this Agreement. In the event of exigent circumstances, the [External Party] will notify the designated [Component] representative as soon as possible and no longer

than 24 hours after taking the action. This section does not apply to matters in which DHS and [External Party] do not have a mutual investigative interest.

L. REPORTING AND COMPLIANCE. [*Describe the responsibilities concerning the reporting of and responses to information sharing incidents for both organizations. Also enter a description of how the audit trail responsibility, if any, is to be shared by participating systems and what events each shall note.*]

[*Reporting – clause 1]* The Parties will report incidents in accordance to their own [(procedure name]) procedures.

OR

[*If transmitting PII*] The Parties intend to provide notification in writing as soon as practicable after becoming aware of any accidental or unauthorized access, use, disclosure, modification or disposal of information received under this Agreement, and, as soon as practicable thereafter, to furnish all necessary details of the accidental or unauthorized access, use, disclosure, modification, or disposal of that information. Each party agrees to cooperate with the other participant's investigation or auditing of such information incidents and measures taken to respond to or mitigate the incident.

[*Reporting – clause 2]* To further safeguard the privacy, security, confidentiality, integrity and availability of the connected systems and the information they stored on these systems, process and transmit, the Parties agree to maintain records of information provided to each other under the terms of this Agreement consistent with applicable law, as well as established records retention policies and guidance of the respective Parties. The Parties will provide notice, written unless otherwise specified, of the events below [list events].

[*Reporting – clause* 3] The Parties shall designate responsible officials to meet annually, or at the request of any Party, to discuss and review the implementation of this [MOA/MOU/MOC]. Any disagreement over the implementation of this [MOA/MOU/MOC] shall be resolved in accordance with the ISSUE RESOLUION paragraph [insert number], above.

[*Reporting – clause* 4] Both Parties shall work together to develop review standards in order to conduct annual self-audits of their compliance with the privacy and security requirements set forth in this Agreement. The results of such audits shall be exchanged with the other party. The [official to receive reports] shall be provided copies of the self-audits of both Parties for review.

[*Reporting – clause* 5] As part of this responsibility, the [External Party] agrees to conduct annual audits of compliance with [security and privacy standards; security handbook; etc.] and provide the results of these audits to [title of DHS person to receive audit reports]. [DHS will also verify compliance with this requirement through a Computer-Based Training course and an automated certification test. All [External Party] [system] users will be required to pass this certification test in order to access any functions or data in [system].

VI. POINTS OF CONTACT. The individuals responsible for implementation of this [MOA/MOU/MOC] and the resolution of issue hereunder shall be:
[*Identify the POCs for DHS and the External Party, including office symbol, address and phone number (fax number and e-mail or internet addresses can also be included).]*

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

VIII. NO PRIVATE RIGHT. This [MOA/MOU/MOC] is an internal Agreement between ICE and [External Party]. It does not create or confer any right or benefit, substantive or procedural, enforceable by any third party against the Parties, the United States, or the officers, employees, agents, or associated personnel thereof. Nothing in this [MOA/MOU/MOC] [or its appendices] is intended to restrict the authority of either party to act as provided by law, statute, or regulation, or to restrict any party from administering or enforcing any laws within its authority or jurisdiction. If a term of this Agreement is inconsistent with such authority, then that term shall be invalid, but the remaining terms and conditions of this [MOA/MOU/MOC] shall remain in full force and effect.

IX. FUNDING. This [MOA/MOU/MOC] is not an obligation or commitment of funds, nor a basis for transfer of funds. Unless otherwise agreed to in writing, each Party shall bear its own costs in relation to this [MOA/MOU/MOC]. Expenditures by each Party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The Parties expressly acknowledge that this in no way implies that Congress will appropriate funds for such expenditures.

X. ISSUE RESOLUTION. Throughout the course of this Agreement, issues such as scope of the Agreement, interpretation of its provisions, unanticipated technical matters, including improvements, and other proposed modifications can be expected. Both parties agree to appoint their respective points of contact to work in good faith towards resolution.

XI. EFFECTIVE DATE. The terms of this Agreement will become effective on [insert

the effect date].

XII. ENTIRE AGREEMENT. This [MOA/MOU/MOC] [including all appendices] constitutes the entire agreement between the parties.

XIII. DURATION AND MODIFICATION. Upon effectuation of this Agreement, the parties will initiate review of this Agreement on a biennial basis to evaluate the existing [data sharing/data exchanges], examine the continuing needs for and uses of the [shared/exchanged] data, and determine whether provisions of this Agreement require amendment or revision. This Agreement may be modified upon the mutual written consent of the parties.

XIV. TERMINATION. The terms of this Agreement, as modified with the consent of both parties, will remain in effect until [date, completion of project, or upon agreement of parties.] The Agreement may be extended by mutual written agreement of the parties. Either party upon [number] day's written notice to the other party may terminate this Agreement.

The foregoing represents the Agreement reached by the Department of Homeland Security and [External Party].

APPROVED BY:
[*Give the name and position of the official signing and dating for the DHS. If known, give the name and position of the official signing and dating for the other party.]*

_____ _____

[Name] [Date]
[Position]
[Component]
Department of Homeland Security

_____ _____

[Name] [Date]
[Position]
[External
Party]

Appendix H: Frequently Asked Questions (FAQs)

- **Law Enforcement Information: Who do we contact if we receive information and data sharing or access requests related to ICE security?**
  Requests related to law enforcement information as it is used in such activities as a security investigation, a physical security threat, obtained from threat management, or obtained from pre-employment polygraph exams need to be coordinated through and signed by the Associate Director or Deputy Director of the Office of Professional Responsibility (OPR). Additionally, business operations information used for security activities that are part of the daily mission support activities also need to be coordinated through and signed by OPR.

- **Homeland Security Information: Who do we contact if we receive information and data sharing or access requests from foreign governments or international organizations?**
  Information and data sharing or access requests to ICE from foreign governments or international organizations need to be coordinated through the HSI International Operations (IO) before release. HSI IO has been granted signatory authority by the HSI EAD to sign for international information and data sharing activities.

- **Immigration Administration Information: Who do we contact if we receive an information and data sharing or access request related to CHIS?**
  Information and data sharing or access requests related to the criminal history information sharing (CHIS) initiative need to be coordinated through the ERO Enforcement Division. The ERO Enforcement Division Assistant Director has been granted signatory authority by the ERO EAD, as well as the Deputy Executive Associate Director for ERO (DEAD), to sign ISAAs for CHIS information and data sharing activities.

- **Personally Identifiable Information (PII): An ISAA with PII is being initiated. Which Program Offices must be contacted? What are examples of ICE Stakeholder responsibility when PII is being shared?**
  PII is a type of controlled unclassified information. Since the information and data being shared are identified under this classification,[25] the Office of Professional Responsibility needs to be contacted to ensure the information and data is appropriately labeled and to identify any special handling requirements that should be included in the ISAA. It is also necessary to include the Office of Information Governance and Privacy, Privacy Unit

---

[25] Executive Order (EO) Number 13556, *Controlled Unclassified Information*, available at https://insight.ice.dhs.gov/director/opr/Documents/pdf/eo13556cui.pdf

Federal Agencies are in the process of transitioning from FOUO and FOUO/LES unclassified information classifications to controlled unclassified information (CUI) classifications. Until such transition is complete, all existing agency policy for sensitive unclassified information remains in effect. Currently, ICE continues to use FOUO and FOUO/LES classifications.

early in the negotiations so that any potential risks may be identified, and responsive mitigation approaches provided to help limit future privacy incidents.[26]

- **Personally Identifiable Information (PII): What are the risks of not engaging with Privacy when negotiating ISAAs with PII?**
  Without expert eyes to review the information request and determine any potential privacy risks, it is possible that a privacy incident could result. Privacy incidents can cost the agency money, time, and reputation. They can also cause damage to the individuals whose information/data is released without authority, including physical and reputational harm, and can cost the individual time and money related to identity theft. These costs, to both the agency and individuals, can be difficult to recoup once a breach occurs.

  FIPPs: What are the FIPPs and their purpose in the Privacy review process?
  The FIPPs (Fair Information Practices Principles) are principles taken from the Privacy Act of 1974 and form the basis of the DHS and ICE privacy compliance policies and procedures governing the use of PII. It is ICE Privacy's practice to follow the FIPPs when assessing privacy risks.

  These principles are:
  - Transparency,
  - Individual Participation,
  - Purpose Specification,
  - Data Minimization,
  - Use Limitation,
  - Data Quality and Integrity,
  - Security, and
  - Accountability and Auditing.[27]

  The FIPPs are used to assess and enhance privacy protections by analyzing the nature and purpose of the collection of PII to fulfill DHS and ICE's missions and how Privacy can best provide privacy protections considering these principles.

- **Language: How important is it to have detailed or specific language in ISAAs?**
  ICE ISAAs should be robust, as they potentially allow for the sharing or access of large amounts of data, particularly including, where permitted by law, personally identifiable information (PII),[28] some of which may have substantial adverse impact on a given individual. When ISAAs are requested from sources external to DHS, this need for robust

[26] Appendix F of this Handbook outlines common concerns raised by sharing PII that should be addressed in consultation with the ICE Privacy Unit.

[27] The Fair Information Practice Principles at Work, *available at* https://www.dhs.gov/sites/default/files/publications/dhsprivacy_fippsfactsheet.pdf

[28] DHS defines PII 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 or contractor to the Department.

language increases because responsibility for the accountability and security principles shift to a new party – one that may not have been anticipated under the purpose specification of the original collection. It also becomes important for subject-matter experts, such as privacy, records, civil liberties, information technology, etc., to engage in the conversation and negotiation with the requestor, to ensure risks and mitigation approaches are identified and included early in the development of an ISAA.

- **Scope: Does the process outlined in this Handbook interfere or alter the internal processes for ISAA review in Program Offices?**
  No, the Handbook is not intended to interfere with internal processes. The Handbook's intent is to ensure that ISAAs are vetted and cleared by the proper SMEs to mitigate potential risks to the Agency. Program Offices are encouraged to use their internal processes and reference this Handbook to ensure other relevant stakeholders are leveraged when necessary during the development of the ISAA.

- **Scope: If DARC or ISSGB review is required, who do I contact to initiate the review process?**
  Program Offices will coordinate with IGP for those ISAAs that fall under the purview of the Data Access Review Council (DARC) or that require review and approval by the DHS Information Sharing and Safeguarding Governance Board (ISSGB) for a waiver to the One DHS Rule requirements. IGP should be contacted prior to initiating this process.

- **DHS: When does an ISAA have to be coordinated by DHS? How is the process handled if it is determined that the ISAA requires DHS Coordination?**
  There are limited scenarios when an ISAA may need to be coordinated through DHS, rather than or in addition to this ICE ISAA process. This may be based on the requestor, the nature of the information being shared, and how it will be used by the requestor. For instance, a party external to DHS may request a large quantity of ICE data containing PII from a DHS system for a purpose not previously identified as part of the original collection and beyond the normal law enforcement and homeland security activities at ICE. In these instances, the request needs to be processed by the DHS Data Access Review Council (DARC)[29] which includes DHS Key Stakeholders, who review the request, determine the risks involved, identify any mitigation steps to grant the request or determine if the request should be denied. Information sharing requests made through the DARC or sent to the DARC are outside the scope of the ICE ISAA Directive and review and development of any resulting ISAA will be done through the DARC process. This does not preclude ICE Key Stakeholders from participating in the negotiation and review of these ISAAs, as the DARC must include relevant Component stakeholders and owners of the data. This participation is arranged through the DARC.

  Other Occasions of DHS Coordination

  Occasionally, ICE Program Offices may be involved in the development of an ISAA that involves international parties; or multiple DHS components providing access or sharing

[29] IG and Program Offices may coordinate with the DHS Data Access Team (DART) at (b)(7)(E) (b)(7)(E)@hq.dhs.gov to process the information sharing or access request through the DARC process.

information with parties external to DHS. Although the ICE Program Office involved should contact and involve ICE Key Stakeholders as appropriate, the final review and clearance is performed at the DHS level.

The majority of ISAAs do not require DHS level review. Only similar scenarios, as described above, would require an ISAA to follow guidance and requirements beyond what is provided within the ICE ISAA Directive and Handbook.

- **DHS: What about ISAAs where multiple DHS Components are involved?**
  When multiple DHS Components are involved in an ISAA, DHS will determine the level of Component involvement in the vetting and approval process. In these cases, the handling of ISAA vetting and approval should be escalated to the DHS level. DHS Data Access Review Council (DARC) which includes DHS key stakeholders, who review the request, determine the risks involved, identify any mitigation steps to grant the request or determine if the request should be denied. Information sharing requests made through the DARC or sent to the DARC are outside the scope of the ICE ISAA Directive and review and development of any resulting ISAA will be done through the DARC process. This does not preclude ICE Key Stakeholders from participating in the negotiation and review of these ISAAs, as the DARC must include relevant Component stakeholders and owners of the data. This participation is arranged through the DARC.

- **DHS: How are ISAAs involving ICE data arranged by other DHS Components handled?**
  Based on existing mission cooperating arrangements, other DHS Components may also enter into information sharing agreements with external partners and may in some cases utilize ICE information and data previously acquired and agreed to by ICE. In these instances, the DHS Component should coordinate with ICE, through the applicable ICE Program Office, prior to the DHS Component sharing the information and data with an external partner. The ICE Program Office should coordinate review of the ISAA by appropriate ICE Key Stakeholders ensuring incorporation of a third-party clause into the DHS Component agreement addressing the sharing, retention, and protection requirements of ICE information and data. Coordinating a final review of the DHS Component agreement should go through the pertinent ICE Executive Agent.

  To help ensure DHS Components are involving ICE during the early discussions with the requestor and part of the negotiation process, it is best practice to write a Memorandum of Record (MOR) between ICE and the DHS Component. Similar to ISAAs, a MOR memorializes the purpose, use, and restrictions related to the information and data being shared or accessed. It is also used to record when ICE should be notified and involved with requests to access or share ICE data maintained by other DHS Components. The MOR ensures there is a record of the internal sharing for DHS Components to keep track of information and data flows and to allow DHS Components to identify data owners for their expertise and knowledge regarding the data and whether requests or use of data is appropriate.

  For information sharing arrangements developed by external agencies and organizations who are looking to share ICE data with additional parties, whether internal or external to

the agency or organization, it is essential that such limitations on dissemination and sharing of ICE data are clearly stated in all ICE ISAAs so that the external agency and organization can refer to it as they develop their information sharing arrangement. At a minimum, ICE should indicate in the ISAA that no dissemination or sharing of ICE data by parties external to DHS can occur without approval by ICE.

- **DHS: What if my ISAA is an exchange of information with another DHS Component? Is this considered to be information with an external party? Should there be any considerations for developing ISAAs where information from another DHS Component is being received in exchange for ICE information or data?**
  ICE follows the One DHS Rule[30] which states that for information sharing purposes, the Department is one agency, and no Component is a separate agency from another Component. In accordance with One DHS Rule, information received by one Component may be shared across the Department, as appropriate. Therefore, other DHS Components are not considered external parties and the requirements of this Handbook do not apply. However, the Program Office may choose to request OPLA review of the inter-DHS ISAA and may coordinate with the ICE Program Office developing the ISAA to ensure consistency with the One DHS Rule. If the ISAA requires a waiver to One DHS Rule requirements, the ICE Program Office should contact IGP in order to coordinate review and approval by the DHS Information Sharing and Safeguarding Governance Board.

  Additionally, as it is good practice to keep track of with whom and for what purpose information and data is shared, Program Offices may want to consider drafting a Memorandum of Record (MOR) to document the sharing of information and data for future reference. A MOR is an informal document that memorializes the internal sharing of or access to information within DHS. A MOR may record such information as the type of information and data being shared or accessed, the parties involved, any restrictions to the use or access of the information and data, and requirement to contact the data owner when ICE data is being requested for dissemination to other parties, whether internal or external to DHS.

- **IGP: If I need help with coordination or need assistance with the ISAA process, who do I contact?**
  Contact IGP via their intake process by completing the IGP Support Request Form located on the IGP intranet homepage:
  (b)(7)(E)

[30] DHS Secretary Chertoff Memorandum, *DHS Policy for Internal Information Exchange and Sharing* (commonly known as the One DHS Rule), dated February 1, 2007, *available at* https://www.hsdl.org/?view&did=469772