

U.S. Department of Homeland Security
500 12th St., SW
Washington, D.C. 20536



U.S. Immigration
and Customs
Enforcement

July 23, 2026

Daniel Martinez
American Oversight
1030 15th St. NW, B255
Washington, D.C. 20005
(202) 919-6303
foia@americanoversight.org

RE: American Oversight v. TSA, et al, 26-cv-00193
ICE FOIA Case Numbers 2026-ICFO-09147
ICE Litigation Case Number: 2026-ICLI-00029
First and final Release

Dear Mr. Martinez,

This is the first and final response to your Freedom of Information Act (FOIA) requests to U.S. Immigration and Customs Enforcement (ICE) and Transportation Security Administration (TSA), dated December 19, 2025, seeking:

A complete copy (including any attachments) of all contracts or subcontracts, amendments, inter-governmental service agreements, memoranda of understanding, or other written agreements between TSA and ICE. Please provide all responsive records created or in effect from March 1, 2025, through the date the search is conducted.

ICE has considered this request under the FOIA, 5 U.S.C. § 552.

A search of the offices of Homeland Security Investigations (HSI) located records that are potentially responsive to your request. For this production ICE reviewed 16 pages of potentially responsive records. Upon review, ICE has determined that 16 pages will be released in part pursuant to Exemptions (b)(6), (b)(7)(C), (b)(7)(E) and (b)(7)(F) of the FOIA, 5 U.S.C. § 552 as described below. Please note, 16 pages reviewed for this month's production were sent for consultation to the Transportation Security Administration (TSA) and include their recommendations. Therefore, we are releasing these 16 pages on behalf of ICE and TSA. The 16 pages have been Bates numbered 2026-ICLI-00029 00001 through 2026-ICLI-00029 00016.

ICE has applied FOIA Exemptions 6 and 7(C) to protect from disclosure the names, e-mail addresses, and phone numbers of ICE and DHS employees contained within the documents, as well as the names, and other personally identifiable information of other individuals contained within the records.

FOIA Exemption 6 exempts from disclosure personnel or medical files and similar files the release of which would cause a clearly unwarranted invasion of personal privacy. This requires a balancing of the public's right to disclosure against the individual's right to privacy. The privacy interests of the individuals in the records you have requested outweigh any minimal public interest in disclosure of the information. Any private interest you may have in that information does not factor into the aforementioned balancing test.

FOIA Exemption 7(C) protects records or information compiled for law enforcement purposes that could reasonably be expected to constitute an unwarranted invasion of personal privacy. This exemption takes particular note of the strong interests of individuals, whether they are suspects, witnesses, or investigators, in not being unwarrantably associated with alleged criminal activity. That interest extends to persons who are not only the subjects of the investigation, but those who may have their privacy invaded by having their identities and information about them revealed in connection with an investigation. Based upon the traditional recognition of strong privacy interest in law enforcement records, categorical withholding of information that identifies third parties in law enforcement records is ordinarily appropriate. As such, I have determined that the privacy interest in the identities of individuals in the records you have requested clearly outweigh any minimal public interest in disclosure of the information. Please note that any private interest you may have in that information does not factor into this determination.

ICE has applied FOIA Exemption 7(E) to protect from disclosure internal agency case numbers contained within the document.

FOIA Exemption 7(E) protects records compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law. I have determined that disclosure of certain law enforcement sensitive information contained within the responsive records could reasonably be expected to risk circumvention of the law. Additionally, the techniques and procedures at issue are not well known to the public.

ICE has applied FOIA exemption 7(F) protects the release of information that would jeopardize the lives and physical safety of the individuals and compromise the ability of employees to perform their duties.

FOIA Exemption 7(F) allows the agency to withhold records if release could reasonably be expected to endanger the life or physical safety of any individual. This exemption protects law enforcement agents, witnesses, informants, and third parties from harm, threats, or harassment.

If you have any questions about this letter, please contact Assistant U.S. Attorney Kaitlin Eckrote at kaitlin.eckrote@usdoj.gov.

Sincerely,
**MOLLY A
LLOYD**
Molly Lloyd
FOIA Litigation Team Supervisor

Digitally signed by
MOLLY A LLOYD
Date: 2026.07.23
07:27:17 -04'00'

Enclosure: 16 pages

Memorandum of Agreement
Between
Transportation Security Administration
and
U.S. Immigration and Customs Enforcement

I. INTRODUCTION AND PURPOSE:

This Memorandum of Agreement (MOA or Agreement) is entered into by U.S. Immigration and Customs Enforcement (ICE), and Transportation Security Administration (TSA) (collectively “the Parties”), which are both component agencies of the U.S. Department of Homeland Security (DHS).

The Parties have entered this Agreement to govern the terms, conditions, and safeguards under which ICE and TSA will share information. ICE will share information with TSA to identify individuals of interest to ICE in furtherance of its law enforcement mission.

(b)(7)(E)

II. BACKGROUND:

ICE has a statutory mission to enforce the immigration and criminal laws of the United States, including removing removable aliens from the United States and investigating criminal cases. To better accomplish its mission, (b)(7)(E)

(b)(7)(E)

III. SCOPE:

The scope of this Agreement is limited to the exchange of agreed-upon data between the Parties to enhance national security, transportation security, law enforcement, and immigration and border management.

ICE intends to share the data elements specified in Appendix C with TSA for the

purposes outlined in this Agreement. ICE will store information obtained from TSA in its data repository (b)(7)(E)

TSA intends to share the data elements specified in Appendices A and B with ICE for the purposes outlined in this Agreement.

IV. AUTHORITIES:

a. ICE Authorities: ICE is authorized to enter into this Agreement pursuant to the Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (Nov. 25, 2002), as amended, 6 U.S.C. § 112(b)(2), 6 U.S.C. § 251, 8 U.S.C. § 1103, 8 U.S.C. § 1373, 19 U.S.C. § 1589a, etc. The Secretary of Homeland Security has the authority to enforce laws contained in Titles 8, 18, 19, 21, 22, and 31 of the U.S. Code. The Secretary delegated this enforcement authority, *inter alia*, to the Director of ICE in DHS Delegation Order No. 7030.2, *Delegation of Authority to the Assistant Secretary for U.S. Immigration and Customs Enforcement* (Nov. 13, 2004), and the Reorganization Plan Modification for the Department of Homeland Security (Jan. 30, 2003). Through these statutes and orders, ICE has broad legal authority to enforce an array of federal statutes including responsibility for enforcing customs laws, federal criminal laws, and immigration laws.

b. TSA Authorities: TSA is authorized to share information pursuant to the Aviation and Transportation Security Act, Pub. L. No. 107-71, 115 Stat. 597 (Nov. 19, 2001), as amended, 49 U.S.C. § 114; *see also* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 4012, 118 Stat 3638 (2004); Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat 266 (2007); 49 U.S.C. §§ 5103(a), 44903, 70105. The Secure Flight Final Rule, codified at 49 C.F.R. § 1560, allows TSA to use larger sets of government-maintained lists when warranted by security considerations. Additionally, under the DHS Policy for Internal Information Exchange and Sharing, TSA can share information with other DHS components, such as ICE, when there is an authorized purpose and a need to know, as provided by 5 U.S.C. § 552a(b)(1). This intra-agency sharing is consistent with the Privacy Act's exception for internal use and supports the collaborative efforts to enhance national security (b)(7)(E)

(b)(7)(E)

V. RESPONSIBILITIES:

(b)(7)(E)

(b)(7)(E)

b.

(b)(7)(E)

VI. SECURITY PROCEDURES:

- a. TSA and ICE will comply with the requirements of the Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. Chapter 35, Subchapter II, as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283); related Office of Management and Budget (OMB) circulars and memoranda, such as OMB Circular A130, *Managing Information as a Strategic Resource* (July 28, 2016) and Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017); National Institute of Standards and Technology (NIST) directives; and the Federal Acquisition Regulations, including any applicable amendments published after the effective date of this Agreement. These laws, regulations, and directives include requirements for safeguarding Federal information systems and personally identifiable information (PII) used in Federal agency business processes, as well as related reporting requirements. Both agencies recognize, and will implement, the laws, regulations, NIST standards, and OMB directives including those published subsequent to the effective date of this Agreement.
- b. FISMA requirements apply to all Federal contractors, organizations, or entities that possess or use Federal information, or that operate, use, or have access to Federal information systems on behalf of an agency. Both agencies are responsible for oversight and compliance of their contractors and agents.
- c. Breach Reporting and Notification:

If either the TSA or ICE experiences an incident involving the suspected or

confirmed breach (i.e., loss) of PII provided by TSA or ICE under the terms of this Agreement, they will follow the breach reporting and notification guidelines issued by OMB. In the event of a PII breach, the agency experiencing the breach is responsible for following its established procedures, including notification to the proper organizations. In addition, the agency experiencing the breach will also notify the other agency's point of contact named in this Agreement within one hour of discovering the breach. If the agency that experienced the breach determines that the risk of harm requires notification to affected individuals or other remedies, that agency will carry out these remedies without cost to the other agency.

d. Administrative Safeguards:

TSA and ICE will restrict access to the data (b)(7)(E) (b)(7)(E) to only those users (e.g., employees, contractors) who have a need to know to perform their official duties in connection with the uses of the data authorized in this Agreement, except as required by federal Law. Further, TSA and ICE will advise all personnel who have access to the data (b)(7)(E) of the confidential nature of the data, the safeguards required to protect the data, and the civil and criminal sanctions for noncompliance contained in the applicable federal laws.

e. Physical Safeguards:

TSA and ICE will store the data (b)(7)(E) in an area that is physically and technologically secure from access by unauthorized persons at all times (e.g., door locks, card keys, biometric identifiers). Only authorized personnel will transmit or transport the data (b)(7)(E) (b)(7)(E) TSA and ICE have implemented and will adhere to suitable safeguards for the data, as identified through a risk-based evaluation of the relevant circumstances.

f. Technical Safeguards:

TSA and ICE will process the data (b)(7)(E) under the immediate supervision and control of authorized personnel in a manner that will protect the confidentiality of the data, so that unauthorized persons cannot retrieve any data by computer, remote terminal, or other means. Systems personnel must enter personal identification numbers when accessing data on the agencies' systems. TSA and ICE will limit authorization to those electronic data areas necessary for the authorized analyst to perform their official duties.

g. Application of Policies and Procedures:

TSA and ICE have adopted policies and procedures to ensure that each agency uses the information contained in its records or obtained from the other agency solely as provided in this Agreement. TSA and ICE will comply with these guidelines and any subsequent revisions.

h. Security Assessments:

NIST Special Publication (SP) 80037, as revised, encourages agencies to accept each other's security assessments to reuse information system resources and/or to accept each other has assessed security posture in order to share information. NIST SP 800-37 further encourages that this type of reciprocity is best achieved when agencies are transparent and make available sufficient evidence regarding the security state of an information system so that an authorizing official from another organization can use that evidence to make credible, risk-based decisions regarding the operation and use of that system or the information it processes, stores, or transmits. Consistent with that guidance, the parties agree to make available to each other upon request system security evidence for making risk-based decisions. Either party may make requests for this information at any time throughout the duration or any renewal of this Agreement.

VII. TREATMENT OF INFORMATION:

- a. Information obtained under this Agreement is for official use only, sensitive but unclassified, law enforcement sensitive, consistent with applicable law, regulation, and policy, and it is only to be used or disclosed for the official purposes specified herein. Except as set forth in VI.b, above, the receiving Party will not use such information for purposes inconsistent with this Agreement or disclose to third parties, unless the providing Party expressly approves such use or disclosure in writing. The Parties will limit access to the information shared to only those authorized personnel who have a need to know to carry out their official duties.
- b. Nothing in this Agreement precludes the use or disclosure of information obtained through this Agreement by the receiving Party to the extent that there is an obligation to do so pursuant to applicable law, regulation, or policy. The receiving Party will give advance notice of any such proposed use or disclosure to the providing Party, unless otherwise prohibited by law, regulation, or policy.
- c. In any individual case, a Party may, by way of protective marking or otherwise, apply additional restrictions to those already set out in this MOA with respect to the use or disclosure of information which it has provided hereunder, to include treatment of the information in a manner consistent with each. Where this is done, the other Party will act consistently with the restrictions.
- d. Each Party will provide notification, in writing, to the other Party 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, but no later than ten calendar days after becoming aware, to furnish all necessary details of the accidental or unauthorized access, use, disclosure, modification, or disposal of that information, and remedial

actions taken.

- e. Each Party will notify the other Party, in writing, of any error(s) discovered in information shared under this Agreement as soon as practicable, but no later than ten calendar days after such error(s) is discovered. Each Party will take appropriate action regarding any request from the other Party for additions, deletions, or corrections to the information, including in any disseminated products that contain such information. Location and correction of any records that contain the information, if appropriate, will occur as soon as is practicable, but no later than ten calendar days from the date of notification of error.
- f. The collection, use, disclosure, and retention of PII by the Parties will be limited to the purposes stated in this MOA. PII will be protected by administrative, technical, and physical safeguards appropriate to the sensitivity of the information. The Parties will use recognized security mechanisms such as password, encryption, or other reasonable safeguards to prevent unauthorized access. In addition, each Party will maintain any PII received under this Agreement in accordance with applicable law, regulation, and policy. The Parties will only disclose PII to authorized individuals with a verified need to know and only for uses that are consistent with the purposes of the MOA and in accordance with applicable law, regulation, and policy.
- g. Information obtained under this MOA will be retained only as long as necessary to carry out the purposes stated in this MOA and in accordance with applicable law, regulation, and policy, and will be disposed of thereafter, in accordance with the applicable National Archives and Records Administration (NARA) General Records Schedule(s) or NARA-approved agency-specific records retention schedule(s). If no applicable retention schedule exists, the records are retained indefinitely or until NARA approves a schedule(s). If a litigation hold is in place, the records are retained until no longer needed in the litigation and the hold is lifted.

VIII. POINTS OF CONTACT:

The individuals responsible for implementation of this Agreement and the resolution of issues hereunder shall be:

For ICE:

(b)(6),(b)(7)(C),(b)(7)(F)	Deputy Assistant Director, Intelligence
Name	Title
(b)(6),(b)(7)(C),(b)(7)(F)@hsa.dhs.gov	202-732-3 (b)(6),(b)(7)(C),(b)(7)(F)
Email address	Phone number

For TSA:

<u>(b)(6),(b)(7)(C),(b)(7)(F)</u>	<u>Executive Director Vetting, Intelligence and Analysis</u>
Name	Title
<u>(b)(6),(b)(7)(C),(b)(7)(F)</u>	<u>(b)(6),(b)(7)(C),(b)(7)(F)</u>
Email address	Phone number

IX. SEVERABILITY:

Nothing in this Agreement is intended to conflict with any statute or regulation, or with the policy of either Party. If a term of this Agreement is inconsistent with such an authority, then that term shall be invalid, but the remaining terms and conditions of the Agreement shall remain in full force and effect.

X. NO PRIVATE RIGHT:

This is an internal Agreement between ICE and TSA. 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.

XI. DURATION AND PERIODIC REVIEW:

- a. The terms of this Agreement will remain in effect until terminated in writing pursuant to Section XII below.
- b. The operation of this Agreement shall be reviewed every five years, beginning on the date on which it has been signed by all Parties, to reevaluate the continuing need for and uses of the shared data, and to determine whether the Agreement requires modification.

XII. AMENDMENT OF MOA:

This MOA may be amended by deletion or modification of any provisions, provided that such amendment is in writing and is signed by all parties to the MOA.

XIII. TERMINATION:

Either Party may terminate this Agreement by giving written notice to the other Party.

XIV. ISSUE RESOLUTION:

The Parties recognize that the success of this collaboration requires close cooperation by both Parties. Disagreements among the Parties arising under or relating to this

MOA shall be resolved only via consultation at the lowest practicable level by and between the Parties (or as otherwise may be provided under any separate governance procedures) and will not be referred to any court, person or entity for adjudication or resolution. Therefore, any problems that arise from the operation of this Agreement will be referred to the above-named Points of Contact, or to their designated successors, for resolution.

XV. FUNDING:

This Agreement is not an obligation or commitment of funds, nor is it a basis for transfer of funds. Unless otherwise agreed to in writing, each Party shall bear its own costs in relation to this MOA. 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.

XVI. ENTIRE AGREEMENT:

This MOA constitutes the entire Agreement between the parties.

XVII. EFFECTIVE DATE:

This Agreement becomes effective when the MOA has been signed by authorized representatives of all Parties, below.

APPROVED BY:

For ICE:

**PETER J
HATCH**

Digitally signed by
PETER J HATCH
Date: 2025.05.29
22:22:44 -04'00'

Peter Hatch
Assistant Director, Intelligence
Homeland Security Investigations
Immigration and Customs Enforcement

____ 2025-05-29 _____
Date

For TSA:

**HAO Y T
FROEMLING**

Digitally signed by
HAO Y T FROEMLING
Date: 2025.05.29
19:29:37 -04'00'

Hao-y Froemling
Acting Assistant Administrator
Intelligence and Analysis
Transportation Security Administration

____ 2025-05-29 _____
Date

Appendix A:

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

Appendix B: (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

Appendix C

(b)(7)(E)

(b)(7)(E)