Office of Information Governance and Privacy

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

U.S. Immigration and Customs Enforcement

September 6, 2023

Ms. Jacqueline Stevens
601 University Place, 2d floor
Political Science Department
Evanston, IL 60208

RE: Stevens v. ICE 20-cv-2725
ICE FOIA Case Number 2020-ICLI-00042
Supplemental Release

Dear Ms. Stevens:

This letter is a supplemental response to your client's Freedom of Information Act (FOIA) requests to U.S. Immigration and Customs Enforcement (ICE). Your client seeks records relating to the following Freedom of Information Act requests: 2018-ICFO-56530, 2020-ICFO-18634, 2019-ICFO-33429, 2019-ICFO-29171, 2018-ICFO-59138, and 2019-ICFO-24680. ICE has considered your request under the FOIA, 5 U.S.C. § 552.

For this production, ICE is making a discretionary re-release of 199 pages of records. ICE has reviewed the pages and determined that 77 pages will be released in full and portions of the remaining 122 pages will be withheld pursuant to FOIA Exemptions (b)(4), (b)(6), (b)(7)(C) and (b)(7)(E) as described below. The pages will retain their original Bates numbers.

FOIA Exemption 4 protects trade secrets and commercial or financial information obtained from a person that is privileged or confidential. This exemption covers two categories of information in federal agency records: (1) trade secrets; and (2) information that is commercial or financial, obtained from a person (which may include corporations or state governments), and privileged or confidential, which is both customarily and actually treated as private by the submitter of the information. *See Food Marketing Institute v. Argus Leader Media,* 139 S. Ct. 2356, 2362-63 (2019). I have reviewed the responsive documents, the submitter's objections to release, and relevant case law, and I have determined that portions of the responsive records are exempt from disclosure under subsection (b)(4) of the FOIA and must be withheld in order to protect the submitter's proprietary interests.

ICE has applied FOIA Exemptions 6 and 7(C) to protect from disclosure the personally identifiable information of DHS employees and third parties 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 non-public-facing 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 note of the strong interests of individuals, whether they are suspects, witnesses, investigators, or individuals performing their official duties in connection with a law enforcement agency, in not being unwarrantably associated with alleged criminal activity or becoming targets for revenge by begrudged individuals. 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 the non-public-facing 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.

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.

If you have any questions about this letter, please contact Assistant United States Attorney Alex Hartzler at Alex.Hartzler@usdoj.gov.

Sincerely,

Marcus K. Francis Sr.
Supervisory Paralegal Specialist

Enclosure: 199 pages

52.249-8 Default (Fixed-Price Supply and Service) (APR 1984)

52.251-1 Government Supply Sources (AUG 2010)

52.253-1 Computer Generated Forms (JAN 1991)

3052.204-70 Security Requirements for Unclassified Information Technology Resources (JUN 2006)

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within 30 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the Offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include—

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and

(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy