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

9. Disruptive behavior or threatening to harm another by Contractor employees or subcontractors is grounds for immediate removal from the facility;

10. The Contractor shall immediately remove its employee or subcontractor employee from performing duties under this contract and comply with further guidance from the CO upon learning of adverse or disqualifying information. The Contractor shall not submit and the Government shall not pay for invoiced hours for a Contractor on administrative leave due to any actions potentially in violation of the Standards of Conduct. Disqualifying information may include, but is not limited to:

    a. Conviction of a crime (felony offenses);

    b. A record of arrests for traffic offenses (especially DUI); and

    c. False information entered on suitability forms.

11. At no time will a Contractor's employees nor its subcontractor's employees make statements or represent themselves as government employees to include but not limited to, using social media.

C-19. USE OF SUBCONTRACTORS AND INDEPENDENT CONTRACTORS.
Contractor is permitted to use independent contractors and or subcontractors for services rendered under this contract unless debarred from government contracts. If Contractor deems it necessary to obtain the services of a subcontractor to fulfill its obligations under this SOW, the Contractor will notify the CO in writing of its intent to use subcontractors for particular positions. No approval is necessary for use of a subcontractor that is a subsidiary of the Prime Contractor or if the subcontractor was identified in the Prime Contractor's proposal in response to the RFP. Responsibility remains with the Prime Contractor for all subcontractor and independent Contractors. Any subcontractor utilized by the Prime Contractor will be held to the same standards as those required of the Prime Contractor. All staff working under this contract shall identify themselves as employees of the Contractor. The Prime Contractor will remain the sole point of contact for the government in all matters related to the delivery of services under this contract without exception. Any and all documentation, memos etc. submitted to the government will be identified as the product of the Prime Contractor.

C-20. SECURITY REQUIREMENTS.

GENERAL
The United States Immigration and Customs Enforcement (ICE) has determined that performance of the tasks as described in Contract 70CDCR18C0000002 requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor) have access to sensitive DHS information, and that the Contractor will adhere to the following.

C-20.1 PRELIMINARY DETERMINATION
ICE will exercise full control over granting; denying, withholding or terminating unescorted

government facility and/or sensitive Government information access for Contractor employees, based upon the results of a background investigation. ICE may, as it deems appropriate, authorize and make a favorable expedited pre-employment determination based on preliminary security checks. The expedited pre-employment determination will allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable pre-employment determination shall not be considered as assurance that a favorable full employment determination will follow as a result thereof. The granting of a favorable pre-employment determination or a full employment determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by ICE, at any time during the term of the contract. No employee of the Contractor shall be allowed to enter on duty and/or access sensitive information or systems without a favorable preliminary fitness determination or final fitness determination by the Office of Professional Responsibility, Personnel Security Unit (OPR-PSU). No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable pre-employment determination or full employment determination by the OPR-PSU. Contract employees are processed under the ICE Management Directive 6-8.0. The contractor shall comply with the pre-screening requirements specified in the DHS Special Security Requirement – Contractor Pre-Screening paragraph located in this contract, if HSAR clauses 3052.204-70, Security Requirements for Unclassified Information Technology (IT) Resources; and/or 3052.204-71, Contractor Employee Access are included in the Clause section of this contract.

C-20.2 BACKGROUND INVESTIGATIONS

Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. Background investigations will be processed through the Personnel Security Unit. Prospective Contractor employees, whether a replacement, addition, subcontractor employee, or vendor employee, shall submit the following security vetting documentation to OPR-PSU, in coordination with the Contracting Officer Representative (COR), within 10 days of notification by OPR-PSU of nomination by the COR and initiation of an Electronic Questionnaire for Investigation Processing (e-QIP) in the Office of Personnel Management (OPM) automated on-line system.

1. Standard Form 85P (Standard Form 85PS (With supplement to 85P required for armed positions)), "Questionnaire for Public Trust Positions" Form completed on-line and archived by applicant in their OPM e-QIP account.

2. Signature Release Forms (Three total) generated by OPM e-QIP upon completion of Questionnaire (e-signature recommended/acceptable – instructions provided to applicant by OPR-PSU). Completed on-line and archived by applicant in their OPM e-QIP account.

3. Two (2) SF 87 (Rev. March 2013) Fingerprint Cards. **(Two Original Cards sent via COR to OPR-PSU)**

4. Foreign National Relatives or Associates Statement. **(This document sent as an attachment in an e-mail to applicant from OPR-PSU – must be signed and archived into applicant's OPM e-QIP account prior to electronic "Release" of data via on-line account)**

5. DHS 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act" **(This document sent as an attachment in an e-mail to applicant from OPR-PSU – must be signed and archived into applicant's OPM e-QIP account prior to electronic "Release" of data via on-line account)**

6. Optional Form 306 Declaration for Federal Employment **(This document sent as an attachment in an e-mail to applicant from OPR-PSU – must be signed and archived into applicant's OPM e-QIP account prior to electronic "Release" of data via on-line account)**

7. Two additional documents may be applicable if applicant was born abroad and/or if work is in a Detention Environment. If applicable, additional form(s) and instructions will be provided to applicant.

Prospective Contractor employees who currently have an adequate, current investigation and security clearance issued by the Department of Defense Central Adjudications Facility (DoD CAF) or by another Federal Agency may not be required to submit a complete security packet. Information on record will be reviewed and considered for use under Contractor Fitness Reciprocity if applicable.

An adequate and current investigation is one where the investigation is not more than five years old, meets the contract risk level requirement, and applicant has not had a break in service of more than two years.

Required information for submission of security packet will be provided by OPR-PSU at the time of award of the contract. Only complete packages will be accepted by the OPR-PSU as notified via the COR.

Be advised that unless an applicant requiring access to sensitive information has resided in the US for three of the past five years, the Government may not be able to complete a satisfactory background investigation. In such cases, DHS retains the right to deem an applicant as ineligible due to insufficient background information.

The use of Non-U.S. citizens, including Lawful Permanent Residents (LPRs), is not permitted in the performance of this contract for any position that involves access to DHS /ICE IT systems and the information contained therein, to include, the development and / or maintenance of DHS/ICE IT systems; or access to information contained in and / or derived from any DHS/ICE IT system.

C-20.3 TRANSFERS FROM OTHER DHS CONTRACTS:

Personnel may transfer from other DHS Contracts provided they have an adequate and current investigation (see above). If the prospective employee does not have an adequate and current investigation an eQip Worksheet will be submitted to the Intake Team to initiate a new investigation.

Transfers will be submitted on the COR Transfer Form which will be provided by OPR-PSU along with other forms and instructions.

C-20.4 CONTINUED ELIGIBILITY

If a prospective employee is found to be ineligible for access to Government facilities or information, the COR will advise the Contractor that the employee shall not continue to work or to be assigned to work under the contract.

The OPR-PSU may require drug screening for probable cause at any time and/or when the contractor independently identifies, circumstances where probable cause exists.

The OPR-PSU will conduct reinvestigations every 5 years, or when derogatory information is received, to evaluate continued eligibility.

ICE reserves the right and prerogative to deny and/or restrict the facility and information access of any Contractor employee whose actions are in conflict with the standards of conduct, 5 CFR 2635, or whom ICE determines to present a risk of compromising sensitive Government information to which he or she would have access under this contract.

C-20.5 REQUIRED REPORTS:

The Contractor will notify OPR-PSU, via the COR, of terminations/resignations of contract employees under the contract within five days of occurrence. The Contractor will return any ICE issued identification cards and building passes, of terminated/ resigned employees to the COR. If an identification card or building pass is not available to be returned, a report must be submitted to the COR, referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card. The COR will return the identification cards and building passes to the responsible ID Unit.

The Contractor will report any adverse information coming to their attention concerning contract employees under the contract to the OPR-PSU, via the COR, as soon as possible. Reports based on rumor or innuendo should not be made. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report shall include the employees' name and social security number, along with the adverse information being reported.

The Contractor will provide, via the COR, a Quarterly Report containing the names of personnel who are active, pending hire, have departed within the quarter or have had a legal name change

(Submitted with documentation) . The list shall include the Name, Position and SSN (Last Four) and should be derived from system(s) used for contractor payroll/voucher processing to ensure accuracy.

CORs will submit reports to psu-industrial-security@ice.dhs.gov

C-20.6 EMPLOYMENT ELIGIBILITY

The contractor will agree that each employee working on this contract will successfully pass the DHS Employment Eligibility Verification (E-Verify) program operated by USCIS to establish work authorization.

The E-Verify system, formerly known as the Basic Pilot/Employment Eligibility verification Program, is an Internet-based system operated by DHS USCIS, in partnership with the Social Security Administration (SSA) that allows participating employers to electronically verify the employment eligibility of their newly hired employees. E-Verify represents the best means currently available for employers to verify the work authorization of their employees.

The Contractor must agree that each employee working on this contract will have a Social Security Card issued and approved by the Social Security Administration. The Contractor shall be responsible to the Government for acts and omissions of his own employees and for any Subcontractor(s) and their employees.

Subject to existing law, regulations and/ or other provisions of this contract, illegal or undocumented aliens will not be employed by the Contractor, or with this contract. The Contractor will ensure that this provision is expressly incorporated into any and all Subcontracts or subordinate agreements issued in support of this contract.

C-20.7 SECURITY MANAGEMENT

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with the OPR-PSU through the COR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the Contractor.

The COR and the OPR-PSU shall have the right to inspect the procedures, methods, and facilities utilized by the Contractor in complying with the security requirements under this contract. Should the COR determine that the Contractor is not complying with the security requirements of this contract, the Contractor will be informed in writing by the Contracting Officer of the proper action to be taken in order to effect compliance with such requirements.

The following computer security requirements apply to both Department of Homeland Security (DHS) U.S. Immigration and Customs Enforcement (ICE) operations and to the former Immigration and Naturalization Service operations (FINS). These entities are hereafter referred to as the Department.

C-20.8 INFORMATION TECHNOLOGY

When sensitive government information is processed on Department telecommunications and

automated information systems, the Contractor agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data as outlined in *DHS IT Security Program Publication DHS MD 4300.Pub. or its replacement.* Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

C-20.9 INFORMATION TECHNOLOGY SECURITY TRAINING AND OVERSIGHT
In accordance with Chief Information Office requirements and provisions, all contractor employees accessing Department IT systems or processing DHS sensitive data via an IT system will require an ICE issued/provisioned Personal Identity Verification (PIV) card. Additionally, Information Assurance Awareness Training (IAAT) will be required upon initial access and annually thereafter. IAAT training will be provided by the appropriate component agency of DHS.

Contractors, who are involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of the Department, shall receive periodic training at least annually in security awareness and accepted security practices and systems rules of behavior. Department contractors, with significant security responsibilities, shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

All personnel who access Department information systems will be continually evaluated while performing these duties. Supervisors should be aware of any unusual or inappropriate behavior by personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures should be reported to the local Security Office or Information System Security Officer (ISSO).

~~**C-20.1 PRELIMINARY DETERMINATION.** ICE will exercise full control over granting; denying, withholding or terminating unescorted government facility and/or sensitive Government information access for Contractor employees, based upon the results of a background investigation. ICE may, as it deems appropriate, authorize and make a favorable expedited pre-employment determination based on preliminary security checks. The expedited pre-employment determination will allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable pre-employment determination shall not be considered as assurance that a favorable full employment determination will follow as a result thereof. The granting of a favorable pre-employment determination or a full employment determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by ICE, at any time during the term of the contract. No employee of the Contractor shall be allowed to enter on duty and/or access sensitive information or systems~~

without a favorable preliminary fitness determination or final fitness determination by the Office of Professional Responsibility, Personnel Security Unit (OPR-PSU). No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable pre-employment determination or full employment determination by the OPR-PSU. Contract employees are processed under the ICE Management Directive 6-8.0. The contractor shall comply with the pre-screening requirements specified in the DHS Special Security Requirement – Contractor Pre-Screening paragraph located in this contract, if HSAR clauses 3052.204-70, Security Requirements for Unclassified Information Technology (IT) Resources; and/or 3052.204-71, Contractor Employee Access are included in the Clause section of this contract.

C-20.2 BACKGROUND INVESTIGATIONS. All Contractor personnel, including subcontractor personnel (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. Background investigations will be processed through the ICE Personnel Security Unit (PSU). Prospective Contractor employees shall submit the following completed forms to the Personnel Security Unit through the COR, no less than 35 days before the starting date of the contract or 5 days prior to the expected entry on duty of any employees, whether a replacement, addition, subcontractor employee, or Contractor :

1. Standard Form 85P "Questionnaire for Public Trust Positions" Form will be submitted via e-QIP (electronic Questionnaires for Investigation Processing) (Original and One Copy)

2. Three signed e-QIP Signature forms: Signature Page, Release of Information and Release of Medical Information (Originals and One Copy)

3. Two FD Form 258, "Fingerprint Card"

4. Foreign National Relatives or Associates Statement (Original and One Copy)

5. DHS 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act" (Original and One Copy)

6. Optional Form 306 Declaration for Federal Employment (applies to contractors as well) (Original and One Copy)

Prospective Contractor employees who currently have an adequate current investigation and security clearance issued by the Department of Defense Central Adjudications Facility (DoD CAF) or by another Federal Agency may, at the discretion of PSU, not be required to submit complete security packages, and the investigation will be accepted for adjudication under reciprocity.

An adequate and current investigation is one where the investigation is not more than five years old and the subject has not had a break in service of more than two years.

Required forms will be provided by ICE at the time of award of the contract. Only complete packages will be accepted by the OPR-PSU. Specific instructions on submission of packages will be provided upon award of the contract.

Be advised that unless an applicant requiring access to sensitive information has resided in the US for three of the past five years, the Government may not be able to complete a satisfactory background investigation. In such cases, DHS retains the right to deem an applicant as ineligible due to insufficient background information.

The use of Non-U.S. citizens, including Lawful Permanent Residents (LPRs), is not permitted in the performance of this contract for any position that involves access to DHS /ICE IT systems and the information contained therein, to include, the development and / or maintenance of DHS/ICE IT systems; or access to information contained in and / or derived from any DHS/ICE IT system.

C-20.3. TRANSFERS FROM OTHER DHS CONTRACTS. Personnel may transfer from other DHS Contracts provided they have an adequate and current investigation (see above). If the prospective employee does not have an adequate and current investigation an e-QIP Worksheet will be submitted to the Intake Team to initiate a new investigation.

Transfers will be submitted on the COR Transfer Form which will be provided by the Dallas PSU Office along with other forms and instructions.

C-20.4. CONTINUED ELIGIBILITY. If a prospective employee is found to be ineligible for access to Government facilities or information, the COR will advise the Contractor that the employee shall not continue to work or to be assigned to work under the contract.

The OPR-PSU may require drug screening for probable cause at any time and/ or when the contractor independently identifies, circumstances where probable cause exists.

The OPR-PSU will conduct reinvestigations every 5 years, or when derogatory information is received, to evaluate continued eligibility.
ICE reserves the right and prerogative to deny and/ or restrict the facility and information access of any Contractor employee whose actions are in conflict with the standards of conduct, 5 CFR 2635 and 5 CFR 3801, or whom ICE determines to present a risk of compromising sensitive Government information to which he or she would have access under this contract.

C-20.5. REQUIRED REPORTS. The Contractor will notify OPR-PSU through the COR, of all terminations/ resignations within five days of occurrence. The Contractor will return any expired ICE issued identification cards and building passes, or those of terminated employees to the COR. If an identification card or building pass is not available to be returned, a report must be submitted to the COR, referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card. The COR will return the identification cards and building passes to the responsible ID Unit.

The Contractor will report any adverse information coming to their attention concerning contract

employees under the contract to the OPR-PSU through the COR, as soon as possible. Reports based on rumor or innuendo should not be made. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report shall include the employees' name and social security number, along with the adverse information being reported.

The Contractor will provide, through the COR a Quarterly Report containing the names of personnel who are active, pending hire, have departed within the quarter or have had a legal name change (Submitted with documentation) . The list shall include the Name, Position and SSN (Last Four) and should be derived from system(s) used for contractor payroll/voucher processing to ensure accuracy.
Submit reports to the email address psu-industrial-security@ice.dhs.gov

C-20.6. EMPLOYMENT ELIGIBILITY. The Contractor will agree that each employee working on this contract will successfully pass the DHS Employment Eligibility Verification (E-Verify) program operated by USCIS to establish work authorization.

The E-Verify system, formerly known as the Basic Pilot/Employment Eligibility verification Program, is an Internet-based system operated by DHS USCIS, in partnership with the Social Security Administration (SSA) that allows participating employers to electronically verify the employment eligibility of their newly hired employees. E-Verify represents the best means currently available for employers to verify the work authorization of their employees.

The Contractor must agree that each employee working on this contract will have a Social Security Card issued and approved by the Social Security Administration. The Contractor shall be responsible to the Government for acts and omissions of his own employees and for any Subcontractor(s) and their employees.

Subject to existing law, regulations and/ or other provisions of this contract, illegal or undocumented aliens will not be employed by the Contractor, or with this contract. The Contractor will ensure that this provision is expressly incorporated into any and all Subcontracts or subordinate agreements issued in support of this contract.

C-20.7. SECURITY MANAGEMENT. The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with the OPR-PSU through the COR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the Contractor.

The COR and the OPR-PSU shall have the right to inspect the procedures, methods, and facilities utilized by the Contractor in complying with the security requirements under this contract. Should the COR determine that the Contractor is not complying with the security requirements of this contract, the Contractor will be informed in writing by the Contracting Officer of the proper action to be taken in order to effect compliance with such requirements.

The following computer security requirements apply to both Department of Homeland Security (DHS) U.S. Immigration and Customs Enforcement (ICE) operations and to the former Immigration and Naturalization Service operations (FINS). These entities are hereafter referred

to as the Department.

C-20.8. INFORMATION TECHNOLOGY. When sensitive government information is processed on Department telecommunications and automated information systems, the Contractor agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data as outlined in *DHS IT Security Program Publication DHS MD 4300.Pub. or its replacement. Con*tractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level. Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

C-20-9. INFORMATION TECHNOLOGY SECURITY TRAINING AND OVERSIGHT. In accordance with Chief Information Office requirements and provisions, all contractor employees accessing Department IT systems or processing DHS sensitive data via an IT system will require an ICE issued/provisioned Personal Identity Verification (PIV) card. Additionally, Information Assurance Awareness Training (IAAT) will be required upon initial access and annually thereafter. IAAT training will be provided by the appropriate component agency of DHS.

Contractors, who are involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of the Department, shall receive periodic training at least annually in security awareness and accepted security practices and systems rules of behavior. Department contractors, with significant security responsibilities, shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

All personnel who access Department information systems will be continually evaluated while performing these duties. Supervisors should be aware of any unusual or inappropriate behavior by personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures should be reported to the local Security Office or Information System Security Officer (ISSO).

C-21. EMPLOYMENT SCREENING REQUIREMENTS.

(a) The Contractor shall certify in writing to the Contracting Officer prior to commencement of work, that each employee performing under this Agreement who has access to ICE detainees, has successfully completed an employment screening that includes at a minimum a criminal history records check, employment reference checks, and a citizenship check. Screening criteria that will exclude applicants from consideration to perform under this agreement include:

1. Felony convictions (including felony drug convictions);
2. Conviction of a sex crime;