287(g) SERVICE AGREEMENT
BETWEEN THE
UNITED STATES DEPARTMENT OF HOMELAND SECURITY
U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
AND
GALVESTON COUNTY SHERIFF'S OFFICE

This Service Agreement (**"agreement"**) is entered into between United States (US) Department of Homeland Security (**"DHS"**), Immigration and Customs Enforcement (**"ICE"**), and **GALVESTON COUNTY SHERIFF'S OFFICE (D35JK3G2TMU7)** (**"service provider" or "contractor"**) for the purpose of receiving reimbursable costs incurred by the service provider in providing resources to joint operations (also referred to as "aliens" and "detainees"). The term "parties" is used in this agreement to refer jointly to ICE and the service provider.

Participating Law Enforcement Agencies will perform targeted enforcement actions on any case approved by Enforcement and Removal Operations (ERO) in advance of the enforcement action and/or any case specifically designated by ICE that was previously in Office of Refugee Resettlement custody, subsequently released, and unaccounted for.

The agreement will remain in effect for a period not to exceed 36 months unless extended by bilateral modification or terminated in writing by either party. Either party may terminate this agreement by providing written notice of intention to terminate the agreement, a minimum of 60 calendar days in advance of the effective date of termination, or the parties may agree to a shorter period. If this agreement is terminated by either party under this article, ICE will be under no financial obligation for any allowable costs after the date of termination. The service provider will only be paid for services provided to ICE up to and including the day of termination.

The period of performance for this agreement will be specified on Optional Form 347 (OF347).

The following documents constitute the complete agreement and are hereby incorporated directly or by reference:

- A. Optional Form (OF) 347
- B. 287(g) Agreement (This document)

Attachments

- Attachment 1 – Title 29, Part 4 Labor Standards for Federal Service Contracts
- Attachment 2 – Wage Determination Number (to be specified on OF347)
- Attachment 3 – Combatting Trafficking in Persons
- Attachment 4 – ICE Privacy, Records Management, and Safeguarding of Sensitive Information
- Attachment 5 – 287(g) Electronic Payment Request for Stipends

IN WITNESS WHEREOF, the undersigned, duly authorized officers, have subscribed their names on behalf of the Galveston County Sheriff's Office and the Department of Homeland Security, U.S. Immigration and Customs Enforcement. Only the service provider is authorized as a signatory for this agreement with full authority to sign and bind the service provider regarding this agreement. The authorized signatory must be a bona fide representative of the service provider (prime).

ACCEPTED:

U.S. Immigration and Customs Enforcement

Contracting Officer (CO)

Signature: _____

Date: _____

ACCEPTED:

Galveston County Sheriff's Office
Jimmy Fullen
Sheriff

Signature: _____

Date: 9-30-25

ACCEPTED:

Signature: _____
Galveston County Judge, Mark Henry

Date: October 13, 2025

Definitions

- Service Provider Operational Team – ICE immigration enforcement activities under this agreement follow a Task Force Model (TFM) approach. For the service provider's officers to qualify for any reimbursement in this agreement, the team will have two weeks from receipt of the targeted enforcement list from ICE to make an arrest. The arrest must be an individual from this list.

- Law Enforcement Agency (LEA) - Any agency with an active 287(g) Task Force Model (TFM) Memorandum of Agreement (MOA) signed by the Immigration and Customs Enforcement (ICE) director or designee.

- Task Force Officer (TFO) - Any officer, in good standing, employed by a LEA with an active TFM MOA who satisfactorily completed the required training and is in possession of valid TFM credentials (temporary or permanent).

- Targeted Enforcement Actions (TEA) - any case approved by Enforcement and Removal Operations (ERO) in advance of enforcement action.

- Unaccompanied Alien Children (UAC) - any case specifically designated by ICE that was previously in Office of Refugee Resettlement custody, subsequently released, and unaccounted for.

- TFM Participation Worksheet (TPW) - a paper or electronic document provided by the ERO Enforcement Division that collects information related to a LEO's enforcement action under the TFM MOA.

Article 1. Purpose

A. Purpose: The purpose of this service agreement is to establish an agreement between ICE and the service provider for specific enforcement actions as directed by ICE under the authority of Section 287(g) of the Immigration and Nationality Act (INA), codified at 8 U.S.C. § 1357(g), as amended by the Homeland Security Act of 2002, Public Law 107-296. Participation in the ICE/ERO 287(g) Program for reimbursement of items listed in this agreement, apply to participation and operational enforcement in ICE Task Force Model (TFM) only.

B. Responsibilities: This agreement sets forth the responsibilities of ICE and the service provider.

a. ICE

i. ERO shall provide the service provider with access to required Federal Law Enforcement Training Center (FLETC) e-course curriculum required for service provider candidates to become credentialed Task Force Model (TFM)/Task Force Officers (TFO) upon successful completion.

ii. ERO shall provide the service provider with an initial targeted enforcement list from ERO's ELITE data system, which will direct required immigration enforcement activities within a specific geographical area.

iii. ERO shall provide service provider with the "287(g) Service Provider Monthly Report" template. This template must be completed by the service provider monthly to detail TFO payroll (salary and overtime), benefits, and operational expenses related to targeted immigration enforcement activities performed on behalf of ICE, as well as LEA reimbursement requests for vehicles and equipment. This template shall be e-mailed to the designated ICE/ERO POC(s) at ERORPA-287g-TFM@ICE.dhs.gov no later than the 5th day of the corresponding month in which services were performed. This process may be updated with further requirements or automations at a later date.

iv. ERO Field Office shall verify and validate service provider salary, overtime, and benefits data incurred monthly by each operating team.

v. ERO Field Office shall verify and validate the service provider's targeting enforcement accomplishments against the provided ELITE list on a monthly basis, with disbursements to be paid quarterly

vi. The ERO 287(g) Program shall coordinate with ERO Field Offices on validated operational enforcement statistics using ERO systems of record and will confirm payment disbursements. Salary, overtime, and benefits payments will be disbursed monthly, and targeted enforcement incentive payments will be disbursed quarterly.

b. Service Provider

i. The service provider shall provide all personnel, management, equipment, supplies, and services necessary for performance of all targeted enforcement activities addressed in this agreement. Targeted enforcement activities will comply with the Memorandum of Agreement (MOA) 287(g) Task Force Model between the service provider and ICE. The MOA can be found here https://www.ice.gov/doclib/about/offices/ero/287g/moaFillableTFM.pdf.

ii. The service provider shall provide ERO with salary, overtime, and benefits package data for each TFO assigned to an operationalized team as indicated in Section B.a.iii above.

iii. The service provider shall attest to the truthfulness and accuracy of all salary, overtime, benefits, and operational information provided to ICE.

iv. The service provider shall provide ERO with targets located from the provided ELITE list and illegal alien disposition (arrest, transfer of custody to ICE, transfer of custody to CBP, or other)

v. The service provider shall provide ERO with hours spent performing ICE enforcement activities for adult and Unaccompanied Alien Children (UAC), for each TFO assigned to an operationalized team

vi. The service provider shall provide ERO with the manual form. This form may be updated to an automated process at a later date

vii. On all invoices, the service provider shall identify TFO participants by their ICE designated credential identification number (generated after completion of the ICE e-FLETC coursework

C. Rates: All rates are specified in the OF347 This is a fixed rate agreement, subject to the availability of funds

D. Order of Precedence: In instances where other policies conflict with ICE policy or standards, this agreement and/or the Memorandum of Agreement 287(g) Task Force Model between the provider and ICE will be the guiding document.

Article 2. Task Force Model Participation Verification

A. Points of Contact (POC)

The service provider shall provide a POC to the ERO field office with local operational control of the 287(g) program for participation notification purposes. The POC information shall include a name, title, office phone number, and official email address.

The ERO field office with local operational control of the 287(g) program shall provide a POC to the service provider for participation verification purposes. The local ERO office POC will provide the service provider POC with a name, title, office phone number, and official email address, or other electronic means of communication, for communicating and documenting participation activities.

B. Process

Service providers will only be eligible for reimbursement for TEA and UAC cases. TFOs will record all enforcement actions on the approved TPW, on which they will specify whether the case is TEA or UAC. TFOs will provide the TPW to their LEA POC at the end of their shift.

The LEA POC will create a process to save and track all TFO TPWs.

On the first day of each month, the service provider POC will send the ERO POC a list of all TFO enforcement actions along with copies of each TPW.

The ERO POC will reconcile the list of TFO enforcement actions against events recorded in ICE systems of record. Any unmatched records will be reviewed by the ERO POC to identify a cause and resolution. If a case cannot be resolved because it is not in an ICE system of record, then the ERO POC will notify the service provider POC the case has been rejected. If the service provider POC submits correct information and the case is located, then credit will be granted.

Disputes of participation verification will be handled between the ERO field office and service provider management.

Article 3. Employment Screening Requirements

General. The service provider shall certify to the Contracting Officer (CO) and CO Representative (COR) that any employees performing under this agreement, who have access to ICE detainees, will have successfully completed employment screening that includes at a minimum a criminal history records check, employment reference checks and a citizenship check.

Employment Eligibility. Each employee working on this contract shall successfully pass the DHS Employment Eligibility Verification (E-Verify) program operated by the United States Citizenship and Immigration Services (USCIS) to establish work authorization.

> The E-Verify system 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.
>
> Each employee working on this Agreement shall have a Social Security Card issued by the SSA. The service provider shall be responsible 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 shall not be employed by the service provider under this Agreement. The service provider shall ensure that this provision is expressly incorporated into any subcontracts or agreements issued in support of this Agreement.

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

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

Article 4. Incident Reporting

The COR shall be immediately notified in the event of all serious incidents. The COR will provide any additional contact information for outside working hours to the service provider at the time of the award.

Article 5. Administration

A. Commencement of Services: ICE is under no obligation to utilize the services identified herein until the need for services has been identified, and funding has been identified and made available.

B. Funding: The obligation of ICE to make payments to the service provider is contingent upon the availability of Federal funds. ICE will not direct the performance of any other services until ICE has appropriate funding. Service agreements will be established when specific requirements have been identified and funding obligated. Performance under this agreement is not authorized until the CO issues a specific service agreement to the designated service provider in writing. In the event of a Federal lapse of funding, please consult with the CO.

C. Consistent with Law: This agreement is permitted under applicable statutes, regulations, policies, and judicial mandates. Any provision of this agreement contrary to applicable statutes, regulation, policies, or judicial mandates is null and void and shall not necessarily affect the balance of the agreement.

Article 6. Adjusting the Agreement Rates

A. ICE will reimburse the service provider at the rates shown in the OF347, subject to the availability of funds, except as provided in Article 11. No rate adjustments are permitted under this service agreement unless initiated by ICE subject to the availability of funds.

Article 7. Modifications and Disputes

A. Modifications: Actions, other than those designated in this agreement, will not bind or incur liability on behalf of either party. Either party may request a modification to this agreement by submitting a written request to the other party. A modification will become a part of this agreement only after the CO has approved the modification in writing.

B. Disputes: In regard to this service agreement, the CO and the authorized signatory of the service provider will settle disputes, questions, and concerns arising from this agreement. Settlement of disputes will be memorialized in a written modification between the ICE CO and authorized signatory of the service provider. In the event a dispute is not able to be resolved between the service provider and the ICE CO, the ICE CO will make the final decision. If the service provider does not agree with the final decision, the matter may be appealed to the ICE HCA for resolution. The ICE HCA may employ all methods available to resolve the dispute including alternative dispute resolution techniques. The

service provider shall proceed diligently with performance of this agreement pending final resolution of any dispute.

Article 8. Enrollment, Invoicing, and Payment

A. Enrollment in Electronic Funds Transfer: The service provider shall provide ICE with the information needed to make payments by electronic funds transfer (EFT). The service provider shall identify their financial institution and related information on Standard Form 3881, Automated Clearing House (ACH) Vendor Miscellaneous Payment Enrollment Form https://www.gsa.gov/forms-library/ach-vendormiscellaneous-payment-enrollment. The service provider shall submit a completed SF 3881 to ICE payment office prior to submitting its initial request for payment under this agreement. If the EFT data changes, the service provider shall be responsible for providing updated information to the ICE payment office.

B. SAM Registration: The service provider shall maintain an active registration in System for Award Management (SAM) at the time of award and throughout the life of this agreement. The service provider shall be registered to receive "All Awards" in their SAM registration. The SAM website can be found at www.sam.gov.

C. Consolidated Invoicing: Service providers shall submit invoices for salary, overtime, and benefits by the 10th day of the subsequent month after the enforcement action is performed Service providers shall submit invoices for incentive payments by the 10th day after the end of the federal fiscal year quarter (Jan. 10th, Apr. 10th, Jul. 10th, Oct. 10th)

Article 9. Hold Harmless Provisions

Unless specifically addressed by the terms of this agreement, the parties agree to be responsible for the negligent or wrongful acts or omissions of their respective employees to the extent authorized under the applicable law.

A. Service Provider Held Harmless: ICE liability for any injury, damage or loss to persons or property caused by the negligent or tortuous conduct of its own officers, employees, and other persons provided coverage pursuant to Federal law is governed by the Federal Tort Claims Act, 28 USC 2691 *et seq.* (FTCA). Compensation for work related injuries for ICE's officers, employees and covered persons is governed by the Federal Employees Compensation Act (FECA). The service provider shall promptly notify ICE of any claims or lawsuits filed against any ICE employees of which the service provider is notified.

B. Federal Government Held Harmless: Service provider liability for any injury, damage or loss to persons or property arising out of the performance of this agreement and caused by the negligence of its own officers, employees, agents and representatives is governed by the applicable State and/or local law. ICE will promptly notify the service provider of any claims filed against any of the service provider's employees of which ICE is notified. The Federal Government will be held harmless for any injury, damage or loss to persons

or property caused by a service provider employee arising in the performance of this agreement.

A. Defense of Suit: In the event an ICE detained alien files suit against the service provider contesting the legality of the alien's ICE detention under this agreement and/or immigration/citizenship status, or an alien files suit as a result of an administrative error or omission of the Federal Government, ICE will request that the United States Department of Justice (DOJ), as appropriate, move either to have the service provider dismissed from such suit; to have ICE substituted as the proper party defendant; or to have the case removed to a court of proper jurisdiction. Regardless of the decision on any such motion, ICE will request that DOJ be responsible for the defense of any suit on these grounds. Nothing in this agreement limits the discretion of DOJ on any litigation matters.

B. ICE Recovery Right: The service provider shall do nothing to prejudice ICE's right to recover against third parties for any loss, destruction of, or damage to U.S. Government property. Upon request from the CO, the service provider shall furnish to ICE all reasonable assistance and cooperation, including assistance in the prosecution of suit and execution of the instruments of assignment in favor of ICE in obtaining recovery.

Article 10. Financial Records

A. Retention of Records: All supporting documents, arrest sheets, and other records pertinent to service agreements or subordinate agreements under this agreement shall be retained by the service provider in accordance with the NARA records schedule for purposes of federal examinations and audit. The retention period begins at the end of the first year of completion of service under the agreement. If any litigation, claim, negotiation, audit, or other action involving the records has been started before the expiration of the retention period, the records must be retained until completion of the action and resolution of all issues which arise from it or until the end of the regular NARA record retention period, whichever is later. Retention of records requirements can be found in Attachment 8.

B. Access to Records: ICE and the Comptroller General of the United States, or any of their authorized representatives, have the right of access to any pertinent books, documents, papers or other records of the service provider or its subcontractors, which are pertinent to the award, to make audits, examinations, excerpts, and transcripts. The rights of access must not be limited to the required retention period but shall last as long as the records are retained.

Article 11. Labor Standards and Wage Determination

A. The Service Contract Act, 41 U.S.C. 351 et seq., Title 29, Part 4 Labor Standards for Federal Service Contracts, is hereby incorporated as Attachment 1. These standards and provisions are included in every contract and service agreement entered by the United

States or the District of Columbia, in excess of $2,500, or in an indefinite amount, the principal purpose of which is to furnish services through the use of service employees.

B. Wage Determination: Each service employee employed in the performance of this agreement shall be paid not less than the minimum prevailing wages and shall be furnished fringe benefits in accordance with the wages and fringe benefits determined by the Secretary of Labor or authorized representative, as specified in any wage determination applicable under this agreement. The wage determination, issued under the Service Contract Labor Standards statute, by the Administrator, Wage and Hour Division, U.S. Department of Labor, will be updated on the annual anniversary of the service agreement with the most recent applicable wage determination.

C. The service provider shall notify the CO of any increase claimed within 30 calendar days after receiving a new wage determination unless this notification period is extended in writing by the CO. Requested increases shall only include the service provider's actual increase in applicable wages and fringe benefits to the extent the increase is made to comply with the new wage determination. Any adjustment will be limited to increases or decreases in wages and fringe benefits, and the accompanying increases or decreases in social security and unemployment taxes and workers' compensation insurance but shall not otherwise include any amount for general and administrative costs, overhead, or profit.

Article 12. Notification and Public Disclosures

A. Information obtained or developed because of this agreement is under the control of ICE and is subject to public disclosure only pursuant to the provisions of applicable Federal laws (such as FOIA), regulations, and Executive Orders or as ordered by a Court. The Service provider is prohibited from disclosing any information relating to ICE aliens pursuant to 8 C.F.R § 236.6. If the service provider receives a request for such information through, for example relevant State sunshine laws or another mechanism, the service provider shall promptly notify the ICE FOIA Officer and inform the requester to submit a FOIA request directly to the ICE FOIA Office. To the extent the service provider intends to release the agreement or any information relating to, or exchanged under, this agreement, the service provider agrees to coordinate with the ICE FOIA Officer prior to such release. The service provider may, at its discretion, communicate the substance of this agreement when requested. ICE understands that this agreement will become a public document when presented to the service provider's governing body for approval.

B. The service provider shall notify the ICE Office of Congressional Relations when a member of the United States Congress requests information, or the CO and the ICE Office of Congressional Relations when he/she makes a request to visit the facility. The service provider shall coordinate all public information related issues pertaining to ICE aliens with ICE. The service provider shall promptly make public announcements stating the facts of unusual or newsworthy incidents to local media. Examples of such events include, but are not limited to deaths, escapes from custody, and facility emergencies. All

press statements and releases shall be cleared, in advance, with the ICE Office of Public Affairs.

C. With respect to public announcements and press statements, the service provider shall ensure employees agree to use appropriate disclaimers clearly stating the employees' opinions do not reflect the position of the United States government in any public presentations they make or articles they write that relate to any aspect of performance or the facility operations.

Article 13. Privacy

A. The service provider shall comply with the Privacy Act of 1974 ("the Act") and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the agreement specifically identifies (i) the systems of records; and (ii) the design, development, or operation work that the service provider is to perform. The service provider shall also include the Privacy Act into all subcontracts when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and

B. In the event of violations of the act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For the purposes of the act, when the agreement is for the operation of a system of records on individuals to accomplish an agency function, the service provider is considered to be an employee of the Agency.

1. "Operation of a system of records," as used in this article, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

2. "Record," as used in this article, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

3. "System of records on individuals," as used in this article, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

Article 14. Quality Control

The service provider is responsible for management and quality control actions, including the actions of credentialed TFOs, necessary to meet the quality standards set forth in the agreement.

TITLE 29—LABOR

This attachment is updated as of June 2022. The standards for Title 29, Part 4, Subpart A can be found at https://www.ecfr.gov/current/title-29/subtitle-A/part-4/subpart-A.

PART 4 LABOR STANDARDS FOR FEDERAL SERVICE CONTRACTS

Subpart A Service Contract Labor Standards Provisions and Procedures

Sec. 4.6 Labor standards clauses for Federal service contracts exceeding $2,500.

The clauses set forth in the following paragraphs shall be included in full by the contracting agency in every contract entered into by the United States or the District of Columbia, in excess of $2,500, or in an indefinite amount, the principal purpose of which is to furnish services through the use of service employees:

(a) Service Contract Act of 1965, as amended: This contract is subject to the Service Contract Act of 1965, as amended (41 U.S.C. 351 et seq.) and is subject to the following provisions and to all other applicable provisions of the Act and regulations of the Secretary of Labor issued thereunder (29 CFR part 4).

(b)

(1) Each service employee employed in the performance of this contract by the contractor or any subcontractor shall be paid not less than the minimum monetary wages and shall be furnished fringe benefits in accordance with the wages and fringe benefits determined by the Secretary of Labor or authorized representative, as specified in any wage determination attached to this contract.

(2)

(i) If there is such a wage determination attached to this contract, the contracting officer shall require that any class of service employee which is not listed therein and which is to be employed under the contract (i.e., the work to be performed is not performed by any classification listed in the wage determination), be classified by the contractor so as to provide a reasonable relationship (i.e., appropriate level of skill comparison) between such unlisted classifications and the classifications listed in the wage determination. Such conformed class of employees shall be paid the monetary wages and furnished the fringe benefits as are determined pursuant to the procedures in this section.

(ii) Such conforming procedure shall be initiated by the contractor prior to the performance of contract work by such unlisted class of employee. A written report of the proposed conforming action, including information regarding the agreement or disagreement of the authorized representative of the employees involved or, where there is no authorized representative, the employees themselves, shall be submitted by the contractor to the contracting officer no later than 30 days after

such unlisted class of employees performs any contract work. The contracting officer shall review the proposed action and promptly submit a report of the action, together with the agency's recommendation and all pertinent information including the position of the contractor and the employees, to the Wage and Hour Division, U.S. Department of Labor, for review. The Wage and Hour Division will approve, modify, or disapprove the action or render a final determination in the event of disagreement within 30 days of receipt or will notify the contracting officer within 30 days of receipt that additional time is necessary.

(iii) The final determination of the conformance action by the Wage and Hour Division shall be transmitted to the contracting officer who shall promptly notify the contractor of the action taken. Each affected employee shall be furnished by the contractor with a written copy of such determination or it shall be posted as a part of the wage determination.

(iv)

(A) The process of establishing wage and fringe benefit rates that bear a reasonable relationship to those listed in a wage determination cannot be reduced to any single formula. The approach used may vary from wage determination to wage determination depending on the circumstances. Standard wage and salary administration practices which rank various job classifications by pay grade pursuant to point schemes or other job factors may, for example, be relied upon. Guidance may also be obtained from the way different jobs are rated under Federal pay systems (Federal Wage Board Pay System and the General Schedule) or from other wage determinations issued in the same locality. Basic to the establishment of any conformable wage rate(s) is the concept that a pay relationship should be maintained between job classifications based on the skill required and the duties performed.

(B) In the case of a contract modification, an exercise of an option or extension of an existing contract, or in any other case where a contractor succeeds a contract under which the classification in question was previously conformed pursuant to this section, a new conformed wage rate and fringe benefits may be assigned to such conformed classification by indexing (i.e., adjusting) the previous conformed rate and fringe benefits by an amount equal to the average (mean) percentage increase (or decrease, where appropriate) between the wages and fringe benefits specified for all classifications to be used on the contract which are listed in the current wage determination, and those specified for the corresponding classifications in the previously applicable wage determination. Where conforming actions are accomplished in accordance with this paragraph prior to the performance of contract work by the unlisted class of employees, the contractor shall advise the contracting officer of the action taken but the other procedures in paragraph (b)(2)(ii) of this section need not be followed.

(C) No employee engaged in performing work on this contract shall in any event be paid less than the currently applicable minimum wage specified under section 6(a)(1) of the Fair Labor Standards Act of 1938, as amended.

(v) The wage rate and fringe benefits finally determined pursuant to paragraphs (b)(2)(i) and (ii) of this section shall be paid to all employees performing in the classification from the first day on which contract work is performed by them in the classification. Failure to pay such unlisted employees the compensation agreed upon by the interested parties and/or finally determined by the Wage and Hour Division retroactive to the date such class of employees commenced contract work shall be a violation of the Act and this contract.

(vi) Upon discovery of failure to comply with paragraphs (b)(2)(i) through (v) of this section, the Wage and Hour Division shall make a final determination of conformed classification, wage rate, and/or fringe benefits which shall be retroactive to the date such class of employees commenced contract work.

(3) If, as authorized pursuant to section 4(d) of the Service Contract Act of 1965 as amended, the term of this contract is more than 1 year, the minimum monetary wages and fringe benefits required to be paid or furnished thereunder to service employees shall be subject to adjustment after 1 year and not less often than once every 2 years, pursuant to wage determinations to be issued by the Wage and Hour Division of the Department of Labor as provided in such Act.

(c) The contractor or subcontractor may discharge the obligation to furnish fringe benefits specified in the attachment or determined conformably thereto by furnishing any equivalent combinations of bona fide fringe benefits, or by making equivalent or differential payments in cash in accordance with the applicable rules set forth in subpart D of 29 CFR part 4, and not otherwise.

(d)

(1) In the absence of a minimum wage attachment for this contract, neither the contractor nor any subcontractor under this contract shall pay any person performing work under the contract (regardless of whether they are service employees) less than the minimum wage specified by section 6(a)(1) of the Fair Labor Standards Act of 1938. Nothing in this provision shall relieve the contractor or any subcontractor of any other obligation under law or contract for the payment of a higher wage to any employee.

(2) If this contract succeeds a contract, subject to the Service Contract Act of 1965 as amended, under which substantially the same services were furnished in the same locality and service employees were paid wages and fringe benefits provided for in a collective bargaining agreement, in the absence of the minimum wage attachment for this contract setting forth such collectively bargained wage rates and fringe benefits, neither the contractor nor any subcontractor under this contract shall pay any service employee performing any of the contract work (regardless of whether or not such employee was employed under the predecessor contract), less than the wages and

fringe benefits provided for in such collective bargaining agreements, to which such employee would have been entitled if employed under the predecessor contract, including accrued wages and fringe benefits and any prospective increases in wages and fringe benefits provided for under such agreement. No contractor or subcontractor under this contract may be relieved of the foregoing obligation unless the limitations of § 4.1b(b) of 29 CFR part 4 apply or unless the Secretary of Labor or his authorized representative finds, after a hearing as provided in § 4.10 of 29 CFR part 4 that the wages and/or fringe benefits provided for in such agreement are substantially at variance with those which prevail for services of a character similar in the locality, or determines, as provided in § 4.11 of 29 CFR part 4, that the collective bargaining agreement applicable to service employees employed under the predecessor contract was not entered into as a result of arm's-length negotiations. Where it is found in accordance with the review procedures provided in 29 CFR 4.10 and/or 4.11 and parts 6 and 8 that some or all of the wages and/or fringe benefits contained in a predecessor contractor's collective bargaining agreement are substantially at variance with those which prevail for services of a character similar in the locality, and/or that the collective bargaining agreement applicable to service employees employed under the predecessor contract was not entered into as a result of arm's-length negotiations, the Department will issue a new or revised wage determination setting forth the applicable wage rates and fringe benefits. Such determination shall be made part of the contract or subcontract, in accordance with the decision of the Administrator, the Administrative Law Judge, or the Administrative Review Board, as the case may be, irrespective of whether such issuance occurs prior to or after the award of a contract or subcontract. 53 Comp. Gen. 401 (1973). In the case of a wage determination issued solely as a result of a finding of substantial variance, such determination shall be effective as of the date of the final administrative decision.

(e) The contractor and any subcontractor under this contract shall notify each service employee commencing work on this contract of the minimum monetary wage and any fringe benefits required to be paid pursuant to this contract, or shall post the wage determination attached to this contract. The poster provided by the Department of Labor (Publication WH 1313) shall be posted in a prominent and accessible place at the worksite. Failure to comply with this requirement is a violation of section 2(a)(4) of the Act and of this contract.

(f) The contractor or subcontractor shall not permit any part of the services called for by this contract to be performed in buildings or surroundings or under working conditions provided by or under the control or supervision of the contractor or subcontractor which are unsanitary or hazardous or dangerous to the health or safety of service employees engaged to furnish these services, and the contractor or subcontractor shall comply with the safety and health standards applied under 29 CFR part 1925.

(g)

(1) The contractor and each subcontractor performing work subject to the Act shall make and maintain for 3 years from the completion of the work records containing the

information specified in paragraphs (g)(1)(i) through (vi) of this section for each employee subject to the Act and shall make them available for inspection and transcription by authorized representatives of the Wage and Hour Division of the U.S. Department of Labor:

(i) Name and address and social security number of each employee.
(ii) The correct work classification or classifications, rate or rates of monetary wages paid and fringe benefits provided, rate or rates of fringe benefit payments in lieu thereof, and total daily and weekly compensation of each employee.
(iii) The number of daily and weekly hours so worked by each employee.
(iv) Any deductions, rebates, or refunds from the total daily or weekly compensation of each employee.
(v) A list of monetary wages and fringe benefits for those classes of service employees not included in the wage determination attached to this contract but for which such wage rates or fringe benefits have been determined by the interested parties or by the Administrator or authorized representative pursuant to the labor standards clause in paragraph (b) of this section. A copy of the report required by the clause in paragraph (b)(2)(ii) of this section shall be deemed to be such a list.
(vi) Any list of the predecessor contractor's employees which had been furnished to the contractor pursuant to § 4.6(l)(2).

(2) The contractor shall also make available a copy of this contract for inspection or transcription by authorized representatives of the Wage and Hour Division.

(3) Failure to make and maintain or to make available such records for inspection and transcription shall be a violation of the regulations and this contract, and in the case of failure to produce such records, the contracting officer, upon direction of the Department of Labor and notification of the contractor, shall take action to cause suspension of any further payment or advance of funds until such violation ceases.

(4) The contractor shall permit authorized representatives of the Wage and Hour Division to conduct interviews with employees at the worksite during normal working hours.

(h) The contractor shall unconditionally pay to each employee subject to the Act all wages due free and clear and without subsequent deduction (except as otherwise provided by law or Regulations, 29 CFR part 4), rebate, or kickback on any account. Such payments shall be made no later than one pay period following the end of the regular pay period in which such wages were earned or accrued. A pay period under this Act may not be of any duration longer than semi-monthly.

(i) The contracting officer shall withhold or cause to be withheld from the Government prime contractor under this or any other Government contract with the prime contractor such sums as an appropriate official of the Department of Labor requests or such sums as the contracting officer decides may be necessary to pay underpaid employees employed by the contractor or subcontractor. In the event of failure to pay any employees subject to the Act all or part of the wages or fringe benefits due under the Act, the agency may, after authorization or by direction of the Department of Labor and written notification to the

contractor, take action to cause suspension of any further payment or advance of funds until such violations have ceased. Additionally, any failure to comply with the requirements of these clauses relating to the Service Contract Act of 1965, may be grounds for termination of the right to proceed with the contract work. In such event, the Government may enter into other contracts or arrangements for completion of the work, charging the contractor in default with any additional cost.

(j) The contractor agrees to insert these clauses in this section relating to the Service Contract Act of 1965 in all subcontracts subject to the Act. The term contractor as used in these clauses in any subcontract, shall be deemed to refer to the subcontractor, except in the term Government prime contractor.

(k)

(1) As used in these clauses, the term service employee means any person engaged in the performance of this contract other than any person employed in a bona fide executive, administrative, or professional capacity, as those terms are defined in part 541 of title 29, Code of Federal Regulations, as of July 30, 1976, and any subsequent revision of those regulations. The term service employee includes all such persons regardless of any contractual relationship that may be alleged to exist between a contractor or subcontractor and such persons.

(2) The following statement is included in contracts pursuant to section 2(a)(5) of the Act and is for informational purposes only:

The following classes of service employees expected to be employed under the contract with the Government would be subject, if employed by the contracting agency, to the provisions of 5 U.S.C. 5341 or 5 U.S.C. 5332 and would, if so employed, be paid not less than the following rates of wages and fringe benefits:

Employee Class	Monetary wage-fringe benefit

(l)

(1) If wages to be paid or fringe benefits to be furnished any service employees employed by the Government prime contractor or any subcontractor under the contract are provided for in a collective bargaining agreement which is or will be effective during any period in which the contract is being performed, the Government prime

contractor shall report such fact to the contracting officer, together with full information as to the application and accrual of such wages and fringe benefits, including any prospective increases, to service employees engaged in work on the contract, and a copy of the collective bargaining agreement. Such report shall be made upon commencing performance of the contract, in the case of collective bargaining agreements effective at such time, and in the case of such agreements or provisions or amendments thereof effective at a later time during the period of contract performance, such agreements shall be reported promptly after negotiation thereof.

(2) Not less than 10 days prior to completion of any contract being performed at a Federal facility where service employees may be retained in the performance of the succeeding contract and subject to a wage determination which contains vacation or other benefit provisions based upon length of service with a contractor (predecessor) or successor (§ 4.173 of Regulations, 29 CFR part 4), the incumbent prime contractor shall furnish to the contracting officer a certified list of the names of all service employees on the contractor's or subcontractor's payroll during the last month of contract performance. Such list shall also contain anniversary dates of employment on the contract either with the current or predecessor contractors of each such service employee. The contracting officer shall turn over such list to the successor contractor at the commencement of the succeeding contract.

(m) Rulings and interpretations of the Service Contract Act of 1965, as amended, are contained in Regulations, 29 CFR part 4.

(n)

(1) By entering into this contract, the contractor (and officials thereof) certifies that neither it (nor he or she) nor any person or firm who has a substantial interest in the contractor's firm is a person or firm ineligible to be awarded Government contracts by virtue of the sanctions imposed pursuant to section 5 of the Act.

(2) No part of this contract shall be subcontracted to any person or firm ineligible for award of a Government contract pursuant to section 5 of the Act.

(3) The penalty for making false statements is prescribed in the U.S. Criminal Code, 18 U.S.C. 1001.

(o) Notwithstanding any of the clauses in paragraphs (b) through (m) of this section relating to the Service Contract Act of 1965, the following employees may be employed in accordance with the following variations, tolerances, and exemptions, which the Secretary of Labor, pursuant to section 4(b) of the Act prior to its amendment by Public Law 92-473, found to be necessary and proper in the public interest or to avoid serious impairment of the conduct of Government business:

(1) Apprentices, student-learners, and workers whose earning capacity is impaired by age, physical, or mental deficiency or injury may be employed at wages lower than

the minimum wages otherwise required by section 2(a)(1) or 2(b)(1) of the Service Contract Act without diminishing any fringe benefits or cash payments in lieu thereof required under section 2(a)(2) of that Act, in accordance with the conditions and procedures prescribed for the employment of apprentices, student-learners, handicapped persons, and handicapped clients of sheltered workshops under section 14 of the Fair Labor Standards Act of 1938, in the regulations issued by the Administrator (29 CFR parts 520, 521, 524, and 525).

(2) The Administrator will issue certificates under the Service Contract Act for the employment of apprentices, student-learners, handicapped persons, or handicapped clients of sheltered workshops not subject to the Fair Labor Standards Act of 1938, or subject to different minimum rates of pay under the two acts, authorizing appropriate rates of minimum wages (but without changing requirements concerning fringe benefits or supplementary cash payments in lieu thereof), applying procedures prescribed by the applicable regulations issued under the Fair Labor Standards Act of 1938 (29 CFR parts 520, 521, 524, and 525).

(3) The Administrator will also withdraw, annul, or cancel such certificates in accordance with the regulations in parts 525 and 528 of title 29 of the Code of Federal Regulations.

(p) Apprentices will be permitted to work at less than the predetermined rate for the work they perform when they are employed and individually registered in a bona fide apprenticeship program registered with a State Apprenticeship Agency which is recognized by the U.S. Department of Labor, or if no such recognized agency exists in a State, under a program registered with the Bureau of Apprenticeship and Training, Employment and Training Administration, U.S. Department of Labor. Any employee who is not registered as an apprentice in an approved program shall be paid the wage rate and fringe benefits contained in the applicable wage determination for the journeyman classification of work actually performed. The wage rates paid apprentices shall not be less than the wage rate for their level of progress set forth in the registered program, expressed as the appropriate percentage of the journeyman's rate contained in the applicable wage determination. The allowable ratio of apprentices to journeymen employed on the contract work in any craft classification shall not be greater than the ratio permitted to the contractor as to his entire work force under the registered program.

(q) Where an employee engaged in an occupation in which he or she customarily and regularly receives more than $30 a month in tips, the amount of tips received by the employee may be credited by the employer against the minimum wage required by Section 2(a)(1) or 2(b)(1) of the Act to the extent permitted by section 3(m) of the Fair Labor Standards Act and Regulations, 29 CFR part 531. To utilize this proviso:

(1) The employer must inform tipped employees about this tip credit allowance before the credit is utilized;

(2) The employees must be allowed to retain all tips (individually or through a pooling arrangement and regardless of whether the employer elects to take a credit for tips received);

(3) The employer must be able to show by records that the employee receives at least the applicable Service Contract Act minimum wage through the combination of direct wages and tip credit;

(4) The use of such tip credit must have been permitted under any predecessor collective bargaining agreement applicable by virtue of section 4(c) of the Act.

(r) Disputes concerning labor standards. Disputes arising out of the labor standards provisions of this contract shall not be subject to the general disputes clause of this contract. Such disputes shall be resolved in accordance with the procedures of the Department of Labor set forth in 29 CFR parts 4, 6, and 8. Disputes within the meaning of this clause include disputes between the contractor (or any of its subcontractors) and the contracting agency, the U.S. Department of Labor, or the employees or their representatives.

Paragraph	OMB Control No.
(b)(2)(iv)-(iv)	1235-0007
(e)	1235-0007
(g)(1)(i)-(iv)	1235-0007
	1235-0018
(g)(1)(v)-(vi)	1235-0007
(l)(1),(2)	1235-0007
(q)(3)	1235-0007

[48 FR 49762, Oct. 27, 1983; 48 FR 50529, Nov. 2, 1983, as amended at 61 FR 68663, Dec. 30, 1996; 82 FR 2224, Jan. 9, 2017]

Combating Trafficking in Persons

(a) *Definitions*. As used in the below article—

"Agent" means any individual, including a director, an officer, an employee, or an independent contractor, authorized to act on behalf of the organization.

"Coercion" means—

(1) Threats of serious harm to or physical restraint against any person;

(2) Any scheme, plan, or pattern intended to cause a person to believe that failure to perform an act would result in serious harm to or physical restraint against any person; or

(3) The abuse or threatened abuse of the legal process.

"Commercial sex act" means any sex act on account of which anything of value is given to or received by any person.

"Commercially available off-the-shelf (COTS) item" means –

(1) Any item of supply (including construction material) that is-

(i) A commercial item (as defined in paragraph (1) of the definition at FAR 2.101);

(ii) Sold in substantial quantities in the commercial marketplace; and

(iii) Offered to the Government, under a contract, agreement, or subcontract at any tier, without modification, in the same form in which it is sold in the commercial marketplace; and

(2) Does not include bulk cargo, as defined in 46 U.S.C. 40102(4), such as agricultural products and petroleum products.

"Debt bondage" means the status or condition of a debtor arising from a pledge by the debtor of his or her personal services or of those of a person under his or her control as a security for debt if the value of those services as reasonably assessed is not applied toward the liquidation of the debt or the length and nature of those services are not respectively limited and defined.

"Employee" means an employee of the service provider directly engaged in the performance of work under the agreement who has other than a minimal impact or involvement in performance.

"Forced Labor" means knowingly providing or obtaining the labor or services of a person—

(1) By threats of serious harm to, or physical restraint against, that person or another person;

(2) By means of any scheme, plan, or pattern intended to cause the person to believe that, if the person did not perform such labor or services, that person or another person would suffer serious harm or physical restraint; or

(3) By means of the abuse or threatened abuse of law or the legal process.

"Involuntary servitude" includes a condition of servitude induced by means of—

(1) Any scheme, plan, or pattern intended to cause a person to believe that, if the person did not enter into or continue in such conditions, that person or another person would suffer serious harm or physical restraint; or

(2) The abuse or threatened abuse of the legal process.

Recruitment fees means fees of any type, including charges, costs, assessments, or other financial obligations, which are associated with the recruiting process, regardless of the time, manner, or location of imposition or collection of the fee.

(1) Recruitment fees include, but are not limited to, the following fees (when they are associated with the recruiting process) for-

(i) Soliciting, identifying, considering, interviewing, referring, retaining, transferring, selecting, training, providing orientation to, skills testing, recommending, or placing employees or potential employees;

(ii) Advertising

(iii) Obtaining permanent or temporary labor certification, including any associated fees;

(iv) Processing applications and petitions;

(v) Acquiring visas, including any associated fees;

(vi) Acquiring photographs and identity or immigration documents, such as passports, including any associated fees;

(vii) Accessing the job opportunity, including required medical examinations and immunizations; background, reference, and security clearance checks and examinations; and additional certifications;

(viii) An employer's recruiters, agents or attorneys, or other notary or legal fees;

(ix) Language interpretation or translation, arranging for or accompanying on travel, or providing other advice to employees or potential employees;

(x) Government-mandated fees, such as border crossing fees, levies, or worker welfare funds;

(xi) Transportation and subsistence costs-

(A) While in transit, including, but not limited to, airfare or costs of other modes of transportation, terminal fees, and travel taxes associated with travel from the country of origin to the country of performance and the return journey upon the end of employment; and

(B) From the airport or disembarkation point to the worksite;

(xii) Security deposits, bonds, and insurance; and

(xiii) Equipment charges.

(2) A recruitment fee, as described in the introductory text of this definition, is a recruitment fee, regardless of whether the payment is-

(i) Paid in property or money;

(ii) Deducted from wages;

(iii) Paid back in wage or benefit concessions;

(iv) Paid back as a kickback, bribe, in-kind payment, free labor, tip, or tribute; or

(v) Collected by an employer or a third party, whether licensed or unlicensed, including, but not limited to-

(A) Agents;
(B) Labor brokers;
(C) Recruiters;
(D) Staffing firms (including private employment and placement firms);
(E) Subsidiaries/affiliates of the employer;
(F) Any agent or employee of such entities; and
(G) Subcontractors at all tiers.

"Severe forms of trafficking in persons" means—

(1) Sex trafficking in which a commercial sex act is induced by force, fraud, or coercion, or in which the person induced to perform such act has not attained 18 years of age; or

(2) The recruitment, harboring, transportation, provision, or obtaining of a person for labor or services, through the use of force, fraud, or coercion for the purpose of subjection to involuntary servitude, peonage, debt bondage, or slavery.

"Sex trafficking" means the recruitment, harboring, transportation, provision, or obtaining of a person for the purpose of a commercial sex act.

Subcontract means any contract entered into by a subcontractor to furnish supplies or services for performance of a prime contract, agreement, or a subcontract.

Subcontractor means any supplier, distributor, vendor, or firm that furnishes supplies or services to or for a service provider or another subcontractor.

United States means the 50 States, the District of Columbia, and outlying areas.

(b) *Policy.* The United States Government has adopted a zero-tolerance policy regarding trafficking in persons. The service provider and service provider employees shall not—

(1) Engage in severe forms of trafficking in persons during the period of performance of the agreement;

(2) Procure commercial sex acts during the period of performance of the agreement; or

(3) Use forced labor in the performance of the agreement.

(4) Destroy, conceal, confiscate, or otherwise deny access by an employee to the employee's identity or immigration documents, such as passports or drivers' licenses, regardless of issuing authority;

(5) (i) Use misleading or fraudulent practices during the recruitment of employees or offering of employment, such as failing to disclose, in a format and language understood by the employee or potential employee, basic information or making material misrepresentations during the recruitment of employees regarding the key terms and conditions of employment, including wages and fringe benefits, the location of work, the living conditions, housing and associated costs (if employer or agent provided or arranged), any significant costs to be charged to the employee or potential employee, and, if applicable, the hazardous nature of the work;

(ii) Use recruiters that do not comply with local labor laws of the country in which the recruiting takes place;

(6) Charge employees or potential employees recruitment fees;

(7) (i) Fail to provide return transportation or pay for the cost of return transportation upon the end of employment-

(A) For an employee who is not a national of the country in which the work is taking place and who was brought into that country for the purpose of working on a U.S. Government contract, agreement, or subcontract (for portions of contracts performed outside the United States); or

(B) For an employee who is not a United States national and who was brought into the United States for the purpose of working on a U.S. Government contract, agreement, or subcontract, if the payment of such costs is required under existing temporary worker programs or pursuant to a written agreement with the employee (for portions of contracts performed inside the United States); except that-

(ii) The requirements of paragraphs (b)(7)(i) of this Article shall not apply to an employee who is-

(A) Legally permitted to remain in the country of employment and who chooses to do so; or

(B) Exempted by an authorized official of the contracting agency from the requirement to provide return transportation or pay for the cost of return transportation;

(iii) The requirements of paragraph (b)(7)(i) of this Article are modified for a victim of trafficking in persons who is seeking victim services or legal redress in the country of employment, or for a witness in an enforcement action related to trafficking in persons. The service provider shall provide the return transportation or pay the cost of return transportation in a way that does not obstruct the victim services, legal redress, or witness activity. For example, the service provider shall not only offer return transportation to a witness at a time

when the witness is still needed to testify. This paragraph does not apply when the exemptions at paragraph (b)(7)(ii) of this Article apply.

(8) Provide or arrange housing that fails to meet the host country housing and safety standards; or

(9) If required by law, contract, or agreement, fail to provide an employment contract, recruitment agreement, or other required work document in writing. Such written work document shall be in a language the employee understands. If the employee must relocate to perform the work, the work document shall be provided to the employee at least 5 calendar days prior to the employee relocating. The employee's work document shall include, but is not limited to, details about work description, wages, prohibition on charging recruitment fees, work location(s), living accommodations and associated costs, time off, roundtrip transportation arrangements, grievance process, and the content of applicable laws and regulations that prohibit trafficking in persons.

(c) *Service Provider Requirements.* The service provider shall—

(1) Notify its employees of—

(i) The United States Government's policy prohibiting trafficking in persons, described in paragraph (b) of this Article; and (ii) The actions that will be taken against employees for violations of this policy. Such actions may include, but are not limited to, removal from the agreement, reduction in benefits, or termination of employment; and
(2) Take appropriate action, up to and including termination, against employees or subcontractors that violate the policy in paragraph (b) of this Article.

(d) *Notification.* The service provider shall inform the CO immediately of—

(1) (i)Any credible information it receives from any source (including host country law enforcement) that alleges a service provider employee, subcontractor, subcontractor employee, or their agent has engaged in conduct that violates the policy in paragraph (b) of this Article (see also 18 U.S.C. 1351, Fraud in Foreign Labor Contracting, and 52.203-13(b)(3)(i)(A), if that Article is included in the solicitation or contract, which requires disclosure to the agency Office of the Inspector General when the service provider has credible evidence of fraud); and (ii)Any actions taken against service provider employees, subcontractors, or subcontractor employees pursuant to this Article.

(2) If the allegation may be associated with more than one contract, the service provider shall inform the CO for the contract with the highest dollar value.

(e) *Remedies.* In addition to other remedies available to the Government, the service provider's failure to comply with the requirements of paragraphs (c), (d), or (f) of this Article may result in—

(1) Requiring the service provider to remove a service provider employee or employees from the performance of the agreement;
(2) Requiring the service provider to terminate a subcontract;
(3) Suspension of contract payments until the service provider has taken appropriate remedial action;
(4) Loss of award fee, consistent with the award fee plan, for the performance period in which the Government determined service provider non-compliance;

(5) Declining to exercise available options under the agreement;
(6) Termination of the agreement for default or cause, in accordance with the termination Article of this contract; or
(7) Suspension or debarment.

(f) *Mitigating Factor.*

When determining remedies, the CO may consider the following:

(1) Mitigating factors. The service provider had a Trafficking in Persons compliance plan or an awareness program at the time of the violation, was in compliance with the plan, and has taken appropriate remedial actions for the violation, which may include reparation to victims for such violations.

(2) Aggravating factors. The service provider failed to abate an alleged violation or enforce the requirements of a compliance plan, when directed by the CO to do so.

(g) *Full cooperation.* (1) The service provider shall, at a minimum-

(i) Disclose to the agency Inspector General information sufficient to identify the nature and extent of an offense and the individuals responsible for the conduct;

(ii) Provide timely and complete responses to Government auditors' and investigators' requests for documents;

(iii) Cooperate fully in providing reasonable access to its facilities and staff (both inside and outside the U.S.) to allow contracting agencies and other responsible Federal agencies to conduct audits, investigations, or other actions to ascertain compliance with the Trafficking Victims Protection Act of 2000 (22 U.S.C. chapter 78), E.O. 13627, or any other applicable law or regulation establishing restrictions on trafficking in persons, the procurement of commercial sex acts, or the use of forced labor; and

(iv) Protect all employees suspected of being victims of or witnesses to prohibited activities, prior to returning to the country from which the employee was recruited and shall not prevent or hinder the ability of these employees from cooperating fully with Government authorities.

(2) The requirement for full cooperation does not foreclose any service provider rights arising in law, the FAR, or the terms of the agreement. It does not-

(i) Require the service provider to waive its attorney-client privilege or the protections afforded by the attorney work product doctrine;

(ii) Require any officer, director, owner, employee, or agent of the service provider, including a sole proprietor, to waive his or her attorney client privilege or Fifth Amendment rights; or

(iii) Restrict the service provider from-

(A) Conducting an internal investigation; or
(B) Defending a proceeding or dispute arising under the agreement or related to a potential or disclosed violation.

(h) *Compliance plan.* (1) This paragraph (h) applies to any portion of the agreement that-

(i) Is for supplies, other than commercially available off-the-shelf items, acquired outside the United States, or services to be performed outside the United States; and

(ii) Has an estimated value that exceeds $550,000.

(2) The service provider shall maintain a compliance plan during the performance of the agreement that is appropriate-

(i) To the size and complexity of the agreement; and

(ii) To the nature and scope of the activities to be performed for the Government, including the number of non-United States citizens expected to be employed and the risk that the contract or subcontract will involve services or supplies susceptible to trafficking in persons.

(3) Minimum requirements. The compliance plan must include, at a minimum, the following.

(i) An awareness program to inform service provider employees about the Government's policy prohibiting trafficking-related activities described in paragraph (b) of this Article, the activities prohibited, and the actions that will be taken against the employee for violations. Additional information about Trafficking in Persons and examples of awareness programs can be found at the website for the Department of State's Office to Monitor and Combat Trafficking in Persons at http://www.state.gov/j/tip/.

(ii) A process for employees to report, without fear of retaliation, activity inconsistent with the policy prohibiting trafficking in persons, including a means to make available to all employees the hotline phone number of the Global Human Trafficking Hotline at 1-844-888-FREE and its email address at help@befree.org.

(iii) A recruitment and wage plan that only permits the use of recruitment companies with trained employees, prohibits charging recruitment fees to the employees or potential employees and ensures that wages meet applicable host-country legal requirements or explains any variance.

(iv) A housing plan, if the service provider or subcontractor intends to provide or arrange housing, that ensures that the housing meets host-country housing and safety standards.

(v) Procedures to prevent agents and subcontractors at any tier and at any dollar value from engaging in trafficking in persons (including activities in paragraph (b) of this Article) and to monitor, detect, and terminate any agents, subcontracts, or subcontractor employees that have engaged in such activities.

(4) Posting. (i) The service provider shall post the relevant contents of the compliance plan, no later than the initiation of contract performance, at the workplace (unless the work is to be performed in the field or not in a fixed location) and on the service provider's Web site (if one is maintained). If posting at the workplace or on the Web site is impracticable, the service provider shall provide the relevant contents of the compliance plan to each worker in writing.

(ii) The service provider shall provide the compliance plan to the CO upon request.

(5) Certification. Annually after receiving an award, the service provider shall submit a certification to the CO that-

(i) It has implemented a compliance plan to prevent any prohibited activities identified at paragraph (b) of this Article and to monitor, detect, and terminate any agent, subcontract or subcontractor employee engaging in prohibited activities; and

(ii) After having conducted due diligence, either-

(A) To the best of the service provider's knowledge and belief, neither it nor any of its agents, subcontractors, or their agents is engaged in any such activities; or

(B) If abuses relating to any of the prohibited activities identified in paragraph (b) of this Article have been found, the service provider or subcontractor has taken the appropriate remedial and referral actions.

(i) *Subcontracts.* (1) The service provider shall include the substance of this article, including this paragraph (i), in all subcontracts and in all contracts with agents. The requirements in paragraph (h) of this Article apply only to any portion of the subcontract that-

(i) Is for supplies, other than commercially available off-the-shelf items, acquired outside the United States, or services to be performed outside the United States; and

(ii) Has an estimated value that exceeds $550,000.

(2) If any subcontractor is required by this Article to submit a certification, the service provider shall require submission prior to the award of the subcontract and annually thereafter. The certification shall cover the items in paragraph (h)(5) of this Article.

A. Information Governance and Privacy

PRIVACY REQUIREMENTS FOR CONTRACTOR AND PERSONNEL

In addition to FAR 52.224-1 Privacy Act Notification (APR 1984), 52.224-2 Privacy Act (APR 1984), FAR 52.224-3 Privacy Training (JAN 2017), and HSAR Clauses, the following instructions must be included in their entirety in all contracts.

Limiting Access to Privacy Act and Other Sensitive Information

In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984), and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires contractor personnel to have access to information protected by the Privacy Act of 1974, the contractor is advised that the relevant DHS system of records notices (SORNs) applicable to this Privacy Act information may be found at https://www.dhs.gov/system-records-notices-sorns. Applicable SORNS of other agencies may be accessed through the agencies' websites or by searching GovInfo, available at https://www.govinfo.gov that replaced the FDsys website in December 2018. SORNs may be updated at any time.

Prohibition on Performing Work Outside a Government Facility/Network/Equipment

The contractor shall perform all tasks on authorized Government networks, using Government-furnished IT and other equipment and/or Workplace as a Service (WaaS) if WaaS is authorized by the statement of work. Government information shall remain within the confines of authorized Government networks at all times. Except where telework is specifically authorized within this contract, the contractor shall perform all tasks described in this document at authorized Government facilities; the contractor is prohibited from performing these tasks at or removing Government-furnished information to any other facility; and Government information shall remain within the confines of authorized Government facilities at all times. Contractors may only access classified materials on government furnished equipment in authorized government owned facilities regardless of telework authorizations.

Prior Approval Required to Hire Subcontractors

The contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (Subcontractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under or relating to this contract. The contractor (and any Subcontractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

Separation Checklist for Contractor Employees

Contractor shall complete a separation checklist before any employee or Subcontractor employee terminates working on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposal of sensitive personally identifiable information (PII), in paper or electronic form, in the custody of the employee or Subcontractor employee including the sanitization of data on any computer systems or media as appropriate; and

(3) termination of any technological access to the contractor's facilities or systems that would permit the terminated employee's access to sensitive PII.

In the event of adverse job actions resulting in the dismissal of an employee or Subcontractor employee, the contractor shall notify the Contracting Officer's Representative (COR) within 24 hours. For normal separations, the contractor shall submit the checklist on the last day of employment or work on the contract.

As requested, contractors shall assist the ICE Point of Contact (ICE/POC), Contracting Officer, or COR with completing ICE Form 50-005/Contractor Employee Separation Clearance Checklist by returning all Government-furnished property including but not limited to computer equipment, media, credentials and passports, smart cards, mobile devices, PIV cards, calling cards, and keys and terminating access to all user accounts and systems.

Contractor's Commercial License Agreement and Government Electronic Information Rights

Except as stated in the Performance Work Statement and, where applicable, the contractor's Commercial License Agreement, the Government Agency owns the rights to all electronic information (electronic data, electronic information systems or electronic databases) and all supporting documentation and associated metadata created as part of this contract. All deliverables (including all data and records) under the contract are the property of the U.S. Government and are considered federal records, for which the Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

Privacy Lead Requirements

If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy documentation, the contractor shall assign or procure a Privacy Lead, to be listed under the SOW or PWS's required Contractor Personnel section. The Privacy Lead shall be responsible for providing adequate support to DHS to ensure DHS can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance. The Privacy Lead shall work with personnel from the program office, the ICE Privacy Unit, the Office of the Chief Information Officer, and the Records and Data Management Unit to ensure that the privacy documentation is kept on schedule, that the answers to questions in the PIA are thorough and complete, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.

The Privacy Lead:

- Must have excellent writing skills, the ability to explain technology clearly for a non-technical audience, and the ability to synthesize information from a variety of sources.
- Must have excellent verbal communication and organizational skills.
- Must have experience writing PIAs. Ideally the candidate would have experience writing PIAs for DHS.
- Must be knowledgeable about the Privacy Act of 1974 and the E-Government Act of 2002.
- Must be able to work well with others.

If a Privacy Lead is already in place with the program office and the contract involves IT system builds or substantial changes that may require privacy documentation, the requirement for a separate Private Lead specifically assigned under this contract may be waived provided the contractor agrees to have the existing Privacy Lead coordinate with and support the ICE Privacy POC to ensure privacy concerns are proactively reviewed and so ICE can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance if required. The contractor shall work with personnel from the program office, the ICE Office of Information Governance and Privacy, and the Office of the Chief Information Officer to ensure that the privacy documentation is kept on schedule, that the answers to questions in any privacy documents are thorough and complete, that all records management requirements are met, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.

Privacy Expectations

Government contractor employees do not have a right, nor should they have an expectation, of privacy while using Government provided devices at any time, including accessing the Internet and using e-mail and voice communications. To the extent that employees wish that their private activities remain private, they should avoid using the Government provided device for limited personal use. By acceptance of the government provided device, employees imply their consent to disclosing and/or monitoring of device usage, including the contents of any files or information maintained or passed -through that device.

B. Data Ownership

1. **Accessibility of Government-owned Data**
   All stored program data associated with this acquisition shall be owned by the Government. As such, it shall be made accessible to the Government in accordance with the Minimum Data Access Capability described below. This accessibility is required to allow full data transparency, flexibility in performing data analytics, and integration with data from other government programs.

   In addition to the Minimum Data Access Capability, the Government prefers, but does not require, that program data be accessible via Enhanced Access Capabilities as described below.

   Definition of **"program data"**: Program Data refers to any data resulting from ICE and DHS organizational activity. Examples of such data include but are not limited to administrative data resulting from human resource, management, and financial actions, as well as operational data resulting from performance of the ICE mission.

   Definition of "**associated with this acquisition"**: Program Data is associated with an acquisition if it is created by DHS organizational activity that is facilitated by the contractor. Examples of how a contractor might facilitate organizational activity follow:
   - Program data is stored by contractor personnel
   - Program data is stored by software that is managed, developed, or used by the contractor

- Program data is stored in a repository that is managed, developed, or used by the contractor

2. Minimum Data Access Capability

- The current version of all Program Data is accessible to the Government within 24 hours of request, as well as on any pre-defined schedule as required by the Government.

  Data access can occur by various means, provided that Government security requirements are met, and data is accessible in a format that is acceptable to the Government. Examples include but are not limited to APIs that are consumable by the Government, files made available for Government download (e.g., Excel Spreadsheets), or direct database query by federal or contractor personnel.

- The contractor shall format program data accessed by the Government to anticipate the maximum file size of any data to be accessed. File size shall be small enough to assure rapid processing by government applications.

- The contractor shall provide the means for the Government to interpret accessible Program Data as follows:

  - Data elements and groupings of data elements shall be clearly identifiable by labels embedded in the data itself, or by a separate schema or file layout which allows such elements and groupings to be identified.
    In the case of a relational database schema defined through Data Definition Language (DDL), data elements would be represented as columns, and groupings of data would be represented as tables. In addition, relationships between tables would be described as foreign key relations.
  - Labels or names used to identify data elements and groupings of data elements shall be approved by the Government. In addition, each label or name shall be associated with a government approved definition which describes the content of data held therein.
  - Program data delivered to the Government shall conform to the Government approved definition for each data element and grouping of data elements.
  - All data accessible by the Government shall be both machine readable and human-readable in plain text.
  - All reference data associated with Program Data also needs to be accessible to the Government. Such reference data is required to provide complete understanding of a record.

    Reference Data Example: Program data may include a city code which uniquely identifies a city. Reference data associated with a city code may include its name, geographic boundaries, population, median income, etc. This example is provided for clarification of the meaning of reference data and may or may not apply to this specific acquisition. Examples of other reference data codes would include codes representing eye color, gender, country of origin, etc.

3. **Enhanced Access Capabilities**

The Government prefers that sharing of program data take place via an Application Programming Interface (API) or multiple APIs. APIs allow the Government to efficiently consume data via a widely recognized standard where the data has been completely abstracted from the technology platform that produces it.

In addition, the Government prefers that sharing of program data take place using techniques that enhance efficiency, such as Change Data Capture (CDC). CDC enhances efficiency of data transfer by providing only incremental updates to program data as opposed to providing all program data each time data is shared.

C. Records Management

REC: 1.1: Required DHS Basic Records Management Training: The contractor shall provide DHS basic records management training for all Government contractor employees and Subcontractors at the outset of their work on the contract and every year thereafter. A hardcopy of the training will be provided as vendors will not have access to ICE systems The contractor shall maintain copies of certificates as a record of compliance. The contractor must submit an annual e-mail notification to the Contracting Officer's Representative that the required training has been completed for all the contractor's employees and Subcontractors.

REC 1.2: Federal Records are the Property of the U.S. Government: The contractor shall treat all federal records (as defined in 44 U.S.C. § 3301) under the contract as the property of the U.S. Government for which the Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. Any records containing information regarding detainees are considered Federal records and the contractor shall comply with 8 C.F.R. §236.6. The contractor shall not retain, use, sell, or disseminate copies of any deliverable without the expressed permission of the Contracting Officer or Contracting Officer's Representative. As consistent with Federal records schedules and the terms of this contract, the contractor shall certify in writing the destruction or return of all Government data at the conclusion of the contract or at a time otherwise specified in the contract. Prior to any destruction, the contractor shall consult with the Contracting Officer or Contracting Officer's Representative to ensure any such destruction follows the governing National Archives and Records Administration (NARA) records control schedule. The Agency owns the rights to all information and records produced as part of this contract.

REC 1.3: Contractor Shall Not Create or Maintain Unauthorized Records: The contractor shall not create or maintain any records that are not specifically tied to or authorized by the contract using Government IT equipment and/or Government records. The contractor shall not create or maintain any records containing any Government agency data that are not specifically tied to or authorized by the contract.

REC 1.4: Agency Owns Rights to Electronic Information: The Government Agency owns the rights to all electronic information (electronic data, electronic information systems or electronic databases) and all supporting documentation created as part of this contract. The contractor must deliver sufficient technical documentation with all data deliverables to permit the Agency to use the data.

REC 1.5: Comply With All Records Management Requirements: The contractor agrees to comply with Federal records management laws, regulations, and Agency policies, including those associated with the safeguarding of records covered by the Privacy Act of 1974, 44 U.S. Code Chapter 31 (Records Management By Federal Agencies), and CFR Title 36 Chapter XII Subchapter B (Records Management). These include the preservation of all records created or received regardless of format, mode of transmission, or state of completion.

REC 1.6: No Disposition of Documents without Prior Written Consent: No disposition of documents will be allowed without the prior written consent of the Contracting Officer. The Agency and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. Records may not be removed from the legal custody of the Agency or destroyed without regard to the provisions of the governing NARA records control schedules. The contractor must report any unlawful or accidental removal, defacing, alteration, or destruction of records to the COR immediately upon discovery.

REC 1.7: Return of all Federal and Agency Records: Upon termination or expiration of the contract, the Contractor must return all Federal and Agency records created or maintained as part of the contract. These records must be returned to the Contracting Officer, Contracting Officer's Representative, or other Designated Agency Representative in a format that ensures they are accessible to the Agency without the use of proprietary software that requires the Agency to engage in additional acquisition or procurement actions.

REC 1.8: Submission of a Records Plan: Prior to the start of the contract, the contractor must submit a Records Plan outlining how it will maintain ICE records throughout the duration of the contract period. The plan must include the following items:

a. A statement acknowledging awareness of relevant General Records Schedules (GRS); DHS records schedules; and ICE records schedules and their intent to comply with the applicable retention requirements. (ICE records schedules can be found at the following link: Records Control Schedules | National Archives)
b. A summary of recordkeeping activities it plans to undertake to ensure all records are properly maintained during the entire records lifecycle (e.g., creation, disposition, etc.). This summary must include where and how ICE records will be stored in an acceptable climate-controlled environment.
c. A summary of electronic recordkeeping activities it plans to undertake to ensure compliance with electronic records management (ERM) practices that are currently underway in ICE (e.g., cloud storage, metadata management, etc.). The plan must include details regarding any video/audio records it creates or uses and how they will be stored during lengthy periods of time.
d. A point of contact for addressing recordkeeping issues and rectifying any discrepancies noted during a records assessment and/or inspection.

The Records Plan must be approved by the ICE Records Officer no sooner 30 days before the start of the contract period.

D. Compliance with DHS Security Policy Terms and Conditions:

All hardware, software, and services provided under this task order must be compliant with DHS 4300A DHS Sensitive System Policy and DHS 4300A Sensitive Systems Handbook.

E. Security Review Terms and Conditions

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford ICE, including the organization of ICE Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer Representative (COR), and other government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor will contact ICE Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to ICE. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of ICE data or the function of computer system operated on behalf of ICE, and to preserve evidence of computer crime.

F. Contractor Employee Access (July 2023)

(a) *Controlled Unclassified Information (CUI)* is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. This definition includes the following CUI categories and subcategories of information:

(1) Chemical-terrorism Vulnerability Information (CVI) as defined in 6 CFR part 27, "Chemical Facility Anti-Terrorism Standards," and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual "Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information" dated September 2008);

(2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through Pub. L. 116–283), PCII's implementing regulations (6 CFR part 29), the PCII Program Procedures Manual, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security, the PCII Program Manager, or a PCII Program Manager Designee;

(3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, "Protection of Sensitive Security Information," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or designee), including Department of Homeland Security MD 11056.1, "Sensitive Security Information (SSI)" and, within the Transportation Security Administration, TSA MD 2810.1, "SSI Program";

(4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local, Tribal, territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015;

(5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;

(6) International Agreement Information means information the Department of Homeland Security receives that is required to be protected by an information sharing agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization;

(7) Information Systems Vulnerability Information (ISVI) means:

> (i) Department of Homeland Security information technology (IT) systems data revealing infrastructure used for servers, desktops, and networks; applications name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission or business use/need. Examples of ISVI are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526 will be classified as appropriate; and/or
>
> (ii) Information regarding developing or current technology, the release of which could hinder the objectives of the Department, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system;

(8) Operations Security Information means Department of Homeland Security information that could be collected, analyzed, and exploited by a foreign adversary to identify intentions, capabilities, operations, and vulnerabilities that threaten operational security for the missions of the Department;

(9) Personnel Security Information means information that could result in physical risk to Department of Homeland Security personnel or other individuals whom the Department is responsible for protecting;

(10) Physical Security Information means reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of Federal buildings, grounds, or property. For example, threat assessments, system security plans,

contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation;

(11) Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or trace an individual's identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(ii) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(A) Truncated SSN (such as last 4 digits);
(B) Date of birth (month, day, and year);
(C) Citizenship or immigration status;
(D) Ethnic or religious affiliation;
(E) Sexual orientation;
(F) Criminal history;
(G) Medical information; and
(H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(iii) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

(b) *Information Resources* means information and related resources, such as personnel, equipment, funds, and information technology.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted or subject to other investigations as required. All Contractor employees requiring recurring access to government facilities or access to CUI or information resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to CUI. The Contractor shall access and use CUI only for the purpose of furnishing advice or assistance directly to the Government in support of the Government's activities, and shall not disclose, orally or in writing, CUI for any other purpose to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized to access CUI, the Contractor shall ensure that these persons receive initial and refresher training concerning the protection and disclosure of CUI. Initial training shall be completed within 60 days of contract award and refresher training shall be completed every 2 years thereafter.

(f) The Contractor shall include this clause in all subcontracts at any tier where the subcontractor may have access to government facilities, CUI, or information resources.

Alternate II (JULY 2023)

When the Department has determined contract employee access to controlled unclassified information or Government facilities must be limited to U.S. citizens and lawful permanent residents, but the contract will not require access to information resources, add the following paragraphs:

(g) Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident Card (USCIS I-551). Any exceptions must be approved by the Department's Chief Security Officer or designee.

(h) Contractors shall identify in their proposals, the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the Contracting Officer.

G. Safeguarding of Controlled Unclassified Information (July 2023)

(a) *Definitions*. As used in this clause—

Adequate Security means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.

Controlled Unclassified Information (CUI) is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. This definition includes the following CUI categories and subcategories of information:

(1) Chemical-terrorism Vulnerability Information (CVI) as defined in 6 CFR part 27, "Chemical Facility Anti-Terrorism Standards," and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual "Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information" dated September 2008);

(2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through Pub. L. 116–283), PCII's implementing regulations (6 CFR part 29), the PCII Program Procedures Manual, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security, the PCII Program Manager, or a PCII Program Manager Designee;

(3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, "Protection of Sensitive Security Information," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or designee), including Department of Homeland Security MD 11056.1, "Sensitive Security Information (SSI)" and, within the Transportation Security Administration, TSA MD 2810.1, "SSI Program";

(4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local, Tribal, territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015;

(5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;

(6) International Agreement Information means information the Department of Homeland Security receives that is required to be protected by an information sharing agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization;

(7) Information Systems Vulnerability Information (ISVI) means:

(i) Department of Homeland Security information technology (IT) systems data revealing infrastructure used for servers, desktops, and networks; applications name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission or business use/need. Examples of ISVI are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526 will be classified as appropriate; and/or

(ii) Information regarding developing or current technology, the release of which could hinder the objectives of the Department, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system;

(8) Operations Security Information means Department of Homeland Security information that could be collected, analyzed, and exploited by a foreign adversary to identify intentions, capabilities, operations, and vulnerabilities that threaten operational security for the missions of the Department;

(9) Personnel Security Information means information that could result in physical risk to Department of Homeland Security personnel or other individuals whom the Department is responsible for protecting;

(10) Physical Security Information means reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of Federal buildings, grounds, or property. For example, threat assessments, system security plans, contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation;

(11) Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or trace an individual's identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, the DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an

individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(ii) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(A) Truncated SSN (such as last 4 digits);
(B) Date of birth (month, day, and year);
(C) Citizenship or immigration status;
(D) Ethnic or religious affiliation;
(E) Sexual orientation;
(F) Criminal history;
(G) Medical information; and
(H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(iii) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

Federal information means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

Federal information system means an information system used or operated by an agency or by a Contractor of an agency or by another organization on behalf of an agency.

Handling means any use of controlled unclassified information, including but not limited to marking, safeguarding, transporting, disseminating, re-using, storing, capturing, and disposing of the information.

Incident means an occurrence that—

(1) Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

(2) Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Information Resources means information and related resources, such as personnel, equipment, funds, and information technology.

Information Security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(1) Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

(2) Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(3) Availability, which means ensuring timely and reliable access to and use of information.

Information System means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

(b) *Handling of Controlled Unclassified Information.*

(1) Contractors and subcontractors must provide adequate security to protect CUI from unauthorized access and disclosure. Adequate security includes compliance with DHS policies and procedures in effect at the time of contract award. These policies and procedures are accessible at *https://www.dhs.gov/dhs-security-and-training-requirements-contractors*.

(2) The Contractor shall not use or redistribute any CUI handled, collected, processed, stored, or transmitted by the Contractor except as specified in the contract.

(3) The Contractor shall not maintain SPII in its invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions. It is acceptable to maintain in these systems the names, titles, and contact information for the Contracting Officer's Representative (COR) or other government personnel associated with the administration of the contract, as needed.

(4) Any government data provided, developed, or obtained under the contract, or otherwise under the control of the Contractor, shall not become part of the bankruptcy estate in the event a Contractor and/or subcontractor enters bankruptcy proceedings.

(c) *Incident Reporting Requirements.*

(1) Contractors and subcontractors shall report all known or suspected incidents to the Component Security Operations Center (SOC) in accordance with Attachment F, *Incident Response*, to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems*. If the Component SOC is not

available, the Contractor shall report to the DHS Enterprise SOC. Contact information for the DHS Enterprise SOC is accessible at *https://www.dhs.gov/dhs-security-and-training-requirements-contractors.* Subcontractors are required to notify the prime Contractor that it has reported a known or suspected incident to the Department. Lower tier subcontractors are required to likewise notify their higher tier subcontractor, until the prime contractor is reached. The Contractor shall also notify the Contracting Officer and COR using the contact information identified in the contract. If the report is made by phone, or the email address for the Contracting Officer or COR is not immediately available, the Contractor shall contact the Contracting Officer and COR immediately after reporting to the Component or DHS Enterprise SOC.

(2) All known or suspected incidents involving PII or SPII shall be reported within 1 hour of discovery. All other incidents shall be reported within 8 hours of discovery.

(3) CUI transmitted via email shall be protected by encryption or transmitted within secure communications systems. CUI shall be transmitted using a *FIPS 140-2/140-3 Security Requirements for Cryptographic Modules* validated cryptographic module identified on *https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules*. When this is impractical or unavailable, for Federal information systems only, CUI may be transmitted over regular email channels. When using regular email channels, Contractors and subcontractors shall not include any CUI in the subject or body of any email. The CUI shall be included as a password-protected attachment with the password provided under separate cover, including as a separate email. Recipients of CUI information will comply with any email restrictions imposed by the originator.

(4) An incident shall not, by itself, be interpreted as evidence that the Contractor or Subcontractor has failed to provide adequate information security safeguards for CUI or has otherwise failed to meet the requirements of the contract.

(5) If an incident involves PII or SPII, in addition to the incident reporting guidelines in Attachment F, *Incident Response*, to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Unique Entity Identifier (UEI);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime Contractor location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, and email);
(v) Contracting Officer POC (address, telephone, and email);

(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms, or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where CUI resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the government PII or SPII contained within the system; and
(xiii) Any additional information relevant to the incident.

(d) *Incident Response Requirements.*

(1) All determinations by the Department related to incidents, including response activities, will be made in writing by the Contracting Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(i) Inspections;
(ii) Investigations;
(iii) Forensic reviews;
(iv) Data analyses and processing; and
(v) Revocation of the Authority to Operate (ATO), if applicable.

(4) The Contractor shall immediately preserve and protect images of known affected information systems and all available monitoring/packet capture data. The monitoring/packet capture data shall be retained for at least 180 days from submission of the incident report to allow DHS to request the media or decline interest.

(5) The Government, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(e) *Certificate of Sanitization of Government and Government-Activity-Related Files and Information.* Upon the conclusion of the contract by expiration, termination, cancellation, or as otherwise indicated in the contract, the Contractor shall return all CUI to DHS and/or destroy it physically and/or logically as identified in the contract unless the contract states that return and/or destruction of CUI is not required. Destruction shall conform to the guidelines for media sanitization contained in NIST SP 800–88, *Guidelines for Media Sanitization.* The Contractor shall certify and confirm the sanitization of all government and government-activity related files and

information. The Contractor shall submit the certification to the COR and Contracting Officer following the template provided in NIST SP 800–88, *Guidelines for Media Sanitization*, Appendix G.

(f) *Other Reporting Requirements.* Incident reporting required by this clause in no way rescinds the Contractor's responsibility for other incident reporting pertaining to its unclassified information systems under other clauses that may apply to its contract(s), or as a result of other applicable statutory or regulatory requirements, or other U.S. Government requirements.

(g) *Subcontracts.* The Contractor shall insert this clause in all subcontracts and require subcontractors to include this clause in all lower tier subcontracts when subcontractor employees will have access to CUI; CUI will be collected or maintained on behalf of the agency by a subcontractor; or a subcontractor information system(s) will be used to process, store, or transmit CUI.

(End of clause)

ALTERNATE I (JULY 2023)

(h) *Authority to Operate*. The Contractor shall not collect, process, store, or transmit CUI within a Federal information system until an ATO has been granted by the Component or Headquarters CIO, or designee. Once the ATO has been granted by the Government, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. Unless otherwise specified in the ATO letter, the ATO is valid for 3 years. An ATO is granted at the sole discretion of the Government and can be revoked at any time. Contractor receipt of an ATO does not create any contractual right of access or entitlement. The Government's grant of an ATO does not alleviate the Contractor's responsibility to ensure the information system controls are implemented and operating effectively.

(1) *Complete the Security Authorization process.* The Security Authorization (SA) process shall proceed according to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems* (Version 13.3, February 13, 2023), or any successor publication; and the *Security Authorization Process Guide*, including templates. These policies and templates are accessible at *https://www.dhs.gov/dhs-security-and-training-requirements-contractors*.

(i) *Security Authorization Package*. The SA package shall be developed using the government-provided Security Requirements Traceability Matrix and SA templates. The SA package consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). The Contractor shall submit a signed copy of the SA package, validated by an independent third party, to the COR for review and approval by the Component or Headquarters CIO, or designee, at least 30 days prior to the date of operation of the information system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of modified documents.

(ii) *Independent Assessment*. Contractors shall have an independent third party validate the security and privacy controls in place for the information system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in NIST SP 800–53, *Security and Privacy Controls for Information Systems and Organizations*, or successor publication, accessible at *https://csrc.nist.gov/publications/sp*. The Contractor shall address all deficiencies before submitting the SA package to the COR for review.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the Contractor shall renew the ATO every 3 years. The Contractor is required to update its SA package as part of the ATO renewal process for review and verification of security controls. Review and verification of security controls is independent of the system production date and may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place. The updated SA package shall be submitted for review and approval by the Component or Headquarters CIO, or designee, at least 90 days before the ATO expiration date. The Contractor shall update its SA package by one of the following methods:

(i) Updating the SA package in the DHS Information Assurance Compliance System; or

(ii) Submitting the updated SA package directly to the COR.

(3) *Security Review.* The Government may elect to conduct periodic reviews to ensure that the security requirements contained in the contract are being implemented and enforced. The Government, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in security review activities. The Contractor shall afford DHS, the Office of the Inspector General, other government organizations, and Contractors working in support of the Government access to the Contractor's facilities, installations, operations, documentation, databases, networks, systems, and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Component or Headquarters CIO, or designee, to coordinate and participate in review and inspection activity by government organizations external to DHS. Access shall be provided, to the extent necessary as determined by the Government (including providing all requested images), for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Federal Reporting and Continuous Monitoring Requirements.* Contractors operating information systems on behalf of the Government shall comply with Federal reporting and information system continuous monitoring requirements. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2015 DHS Information Security Performance Plan, or successor publication, accessible at *https://www.dhs.gov/dhs-security-and-training-requirements-contractors*. The plan is updated on an annual basis.

Annual, quarterly, and monthly data collection will be coordinated by the Government. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for information systems. The Contractor shall provide the COR with requested information within 3 business days of receipt of the request. Unless otherwise specified in the contract, monthly continuous monitoring data shall be stored at the Contractor's location for a period not less than 1 year from the date the data are created. The Government may elect to perform information system continuous monitoring and IT security scanning of information systems from government tools and infrastructure.

(End of clause)

Notification of Credit Monitoring Requirements for Personally Identifiable Information Incidents (July 2023)

(a) *Definitions.* Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or trace an individual's identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, the DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(1) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(2) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(i) Truncated SSN (such as last 4 digits);
(ii) Date of birth (month, day, and year);
(iii) Citizenship or immigration status;
(iv) Ethnic or religious affiliation;
(v)Sexual orientation;
(vi) Criminal history;
(vii) Medical information; and
(viii) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(3) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

(b) *PII and SPII Notification Requirements.*

(1) No later than 5 business days after being directed by the Contracting Officer, or as otherwise required by applicable law, the Contractor shall notify any individual whose PII or SPII was either under the control of the Contractor or resided in an information system under control of the Contractor at the time the incident occurred. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by, the Contracting Officer. The Contractor shall not proceed with notification unless directed in writing by the Contracting Officer.

(2) All determinations by the Department related to notifications to affected individuals and/or Federal agencies and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer.

(3) Subject to government analysis of the incident and direction to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first-class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;
(ii) A description of the types of PII or SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;
(v) What the Contractor and/or the Government are doing to investigate the incident, mitigate the incident, and protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(c) *Credit Monitoring Requirements.* The Contracting Officer may direct the Contractor to:

(1) Provide notification to affected individuals as described in paragraph (b).

(2) Provide credit monitoring services to individuals whose PII or SPII was under the control of the Contractor or resided in the information system at the time of the incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;
(ii) Daily customer service;

(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts.

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized Frequently Asked Questions, approved in writing by the Contracting Officer in coordination with the Component or Headquarters Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(End of clause)

Information Technology Security Awareness Training (July 2023)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Security Training Requirements.*

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable

for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually, and the COR will provide notification when a review is required.

(End of clause)

Privacy Training – Alternate I (DEVIATION)(July 2023)

(a) *Definition.* As used in this clause, personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) Circular A–130, Managing Federal Information as a Strategic Resource).

(b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who—

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or

(3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.1 and 39.105).

(c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract. Contractor employees shall satisfy this requirement by completing *Privacy at DHS: Protecting Personal Information* accessible at *http://www.dhs.gov/dhs-security-and-training-requirements-contractors*. Training shall be completed within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year.

(d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.

(e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.

(f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will—

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information; or

(3) Design, develop, maintain, or operate a system of records.

(End of clause)

287(g) ERO - Electronic Payment Request

Requisition Number:	N/A
ALC:	**70-19-1512**
Date:	
Appropriation Remarks 1 (Bank's Name):	
Appropriation Remarks 2 (Street Address):	
Appropriation Remarks 3 (City, State, Zip):	
Appropriation Remarks 4 (POC Name and Phone #):	
Beneficiary (Agency) Name:	
Beneficiary Bank:	
Depositor Account Number (Receiving Bank):	
Receiving Bank ABA:	
Product Code (BTR/CTR):	CTR
RFB (Please submit incoming wire transfer fee):	
Beneficiary Bank ABA:	
BBK Remarks:	OBI
Payee Remarks 1:	N/A
Payee Remarks 2:	N/A
Payment Amount (Stipend Amount Only):	
Type Code:	**10**
Payee ID/TIN:	**432000174**
OI POC This Request:	Akeem Nugent
ACCS Funding String:	

If **no seizure** is tied to the case, please include funding string to be used above depending on which category the case falls under (Example: National Security, Financial, or Smuggling/Public Safety Investigation). **If there **is a seizure** tied to the case, I will fill in the ACCS funding string.

ICE 287(g) Service Provider Monthly Report

FORM SUBMISSION	
EMAIL TO:	**ERO287g@ice.dhs.gov**
SUBJECT:	EXAMPLE COUNTY OH 287g Report SEP 2025

SERVICE PROVIDER REFERENCE INFORMATION	
AOR:	(ICE will complete)
Service Provider:	Example County Sheriff's Office
Street Address:	123 Main Street
City/State/Zip:	Anytown, OH 00123
POC Name:	Sheriff Doe
POC Email:	sheriff.doe@email.com
MOA Number:	ICE12345678
SAM Registration No. (UEI):	
IRS TIN/EIN:	
COR:	Benjamin Buchta
COR Email Address:	benjamin.buchta@ice.dhs.gov
ACOR:	Lisa Perdue
ACOR Email Address:	lisa.perdue@ice.dhs.gov

INVOICE INFORMATION	
Invoice Start Date:	9/1/2025
Invoice End Date:	9/30/2025
Days in Period:	30
Invoice Number:	00001
Invoice Date:	10/5/2025

TOTAL REQUEST SUMMARY		
Officer Salary:		
Officer Overtime:		
Officer Benefits:		
Operational Expenses:	$	107,500.00
Total Cost:	$	107,500.00

ICE 287(g) Operational Expenses

Officer Name	287(g) Credential Number	Expense Category
DOE, JOHN	123456789	Equipment Package (One Time)
N/A	N/A	Vehicle (One Time)

Operational Expenses can be used to input:
Vehicle Reimbursement (up to $100k, one-time)
Equipment package (up to $7500, one-time per officer).
Do not fill out Officer Name/Credential Number for Vehicle.