Performance Work Statement
Detention Services

(Non-IHSC-Staffed Facility)

June 2026

DRAFT

1. Objective 1
2. Background and Mission 1
3. Scope of Work 1
4. Detention Site Standards and Accreditations 2
5. Facility Inspection Schedule 4
6. Spatial Requirements 4
7. Physical Plant 4
8. Business Permits and Licenses 5
9. ICE Administrative Space 6
10. Environmental Health 10
11. Sanitation and Hygienic Living Conditions 10
12. Maintain Institutional Emergency Readiness 10
13. Armed Transportation Services 11
14. On-call Guard Services 15
15. Virtual Attorney Visitation Capability and Operation 16
16. Notice to Proceed 17
17. Federal Facility Security and Control 17
18. Alien Rights 18
19. Unauthorized Access 18
20. Direct Supervision of Aliens 18
21. Video Surveillance 18
22. Mail Processing 28
23. Detention Management System 28
24. Logbooks 28
25. Reports 29
26. Daily Inspections 29
27. Deviation from Prescribed Schedule Assignments 30
28. Suicide Prevention 30
29. Escapes 30
30. Evacuation Plan 30
31. Injury, Illness, and Reports 31
32. Food Service 31
33. Health Services 31
34. Manage a Detainee Death 50
35. Facility Requirements for Infectious Disease Prevention, Management, and Screening 50
36. Environmental Health 52
37. Medical Quality Assurance (QA) Program 52
38. Immediate Jeopardy 53
39. Detainee Reporting Requirements 56
40. Health Records Requests and Physical Access 57
41. Detainee Medical Records 57

DRAFT

42. Electronic Health Record (EHR) Requirement Interoperability: 58
43. NEW O&M Task 62
44. General Cyber Security Contract Requirements 67
45. DHS FAR Class Deviation 17-03 – Revision 1 85
46. Cloud Services Contract Requirements 86
47. Encryption Compliance 99
48. Detention Services 100
49. Detention Facility ERO Case Processing Specialists Position Description 105
50. Robotics Process Automation (RPA) Contract Requirement 107
51. Notification and Public Disclosures 107
52. Records, Visits, and Disclaimers 108
53. ICE/ERO Control Over Facility Access 109
54. Federal Judiciary 110
55. Quality Control Plan (QCP) 110
56. Quality Assurance Surveillance Plan (QASP) 110
57. Contractor's Failure to Perform Required Services 111
58. Performance Evaluation Meetings 111
59. Organizational Chart 111
60. Personnel and Staffing 111
61. Health and Medical Care Policies 129
62. Federal Facility Requirements for Infectious Disease Screening 129
63. Airborne Precautions 129
64. Required Administration and Management Services 129
65. Property Accountability 134
66. Firearms/Body Armor 135
67. Personnel Background Security Requirements 139
68. Security Management 144
69. Data Ownership Contract Requirements 145
70. Transition 147
71. Glossary 148

DRAFT

1.Objective

The objective of this contract is to obtain comprehensive detention, transportation, food services, and operations and maintenance (O&M) services for U.S. Immigration and Customs Enforcement (ICE) detainees in ICE Enforcement and Removal Operations (ERO) custody as detailed below and as described within this document. The Contractor shall furnish the federal facility and provide all services inclusive of a trained and qualified management staff, supervision, manpower, relief officers, uniforms, equipment, vehicles, and supplies (which includes firearms, ammunition, body restraints, non-lethal devices, body armor, radios, and cellular telephones) to provide support seven (7) days per week, twenty-four (24) hours per day. In this document, "facility" and "federal facility" are used interchangeably. Service provider and contractor are also used interchangeably.

2.Background and Mission

ICE is responsible for the detention, health, welfare, transportation, and deportation of aliens in removal proceedings, and those subject to a final order of removal from the United States.

The mission of ICE ERO is to identify, arrest, and remove aliens, who present a danger to national security or are a risk to public safety, as well as those who enter the U.S. illegally or otherwise undermine the integrity of immigration laws and border control efforts.

In implementing its mission, ERO is responsible for carrying out all orders for the securing and departure activities of aliens who are designated in removal proceedings and for arranging for the detention of aliens when such becomes necessary and prescribed by law.

3.Scope of Work

The contractor shall provide safe and secure conditions of confinement based on the individual characteristics of a diverse population, including threat to the community, risk of flight, type and status of immigration proceeding, community ties, medical and behavioral health issues. The federal detention facility shall provide easy access to legal services; abundant natural light throughout the federal detention facility; ample indoor and outdoor recreation shall be offered at a reasonable time of day. Weather permitting, each detainee shall have access for at least one hour per day, five days per week; or, six or more hours per week, at least four days per week that allows for vigorous aerobic exercise with extended hours of availability - a minimum of four hours per day of outdoor recreation; private showers and restrooms (where practicable); cafeteria style meal service or satellite feeding; non-institutional alien clothing; contact visitation (if applicable), including special arrangements for visiting families, with extended hours including nights and weekends; private areas for attorney-client visits, with video teleconferencing capabilities; noise control; enhanced, but controlled freedom of movement (although the manner and degree of implementation may vary based on security levels); enhanced law library and legal resources (including computers with limited web access to accommodate the ICE provided online law library via the ICE Portal); and enhanced programming, including religious services and social programs and dedicated space for religious services.

DRAFT

In addition to comprehensive detention services, the Contractor shall provide comprehensive operations and maintenance (O&M) services including ongoing preventive and corrective maintenance, facility operations, post-closing services, and compliance with safety, environmental, medical, IT/communications, accessibility, pest control, and security requirements. All work shall be performed in accordance with ICE National Detention Standards (NDS), applicable codes, and regulatory requirements.

4.Detention Site Standards and Accreditations

Detention services shall be performed in accordance with the most current version of the National Detention Standards (NDS). The current version is NDS 2026 available at ice.gov. In addition to conforming with the requirements of NDS 2026, the Contractor shall also ensure the facility conforms with the Architectural Barriers Act of 1968, as amended, Section 504 of the Rehabilitation Act of 1973, and the March 7, 2014, Department of Homeland Security (DHS) regulation under the Prison Rape Elimination Act of 2003 (PREA; P.L. 108-79), *Standards to Prevent, Detect, and Respond to Sexual Abuse and Assault in Confinement Facilities* (DHS PREA Standards) available at https://www.gpo.gov/fdsys/pkg/FR-2014-03-07/pdf/2014-04675.pdf. The contractor shall be responsible for obtaining and maintaining American Correctional Association (ACA) Adult Local Detention Facilities (ALDF) accreditation. Conformance with the ACA ALDF Standards is required on the first day of contract performance and accreditation shall be obtained within seven (7) months of the contract award. If the federal facility is already accredited, reaccreditation shall occur as required by ACA.

The federal facility shall meet, at a minimum, all ACA ALDF requirements and NDS 2026 requirements.

The Contractor shall furnish all personnel, management, equipment, supplies, training, certification, accreditation, and services necessary for the performance of all aspects of the contract. Unless explicitly stated otherwise, the contractor is responsible for all costs associated with and incurred as part of providing the services outlined in this contract. Unless explicitly stated otherwise, the contractor is responsible for all costs associated with and incurred in providing the services specified in this contract.

The Contractor shall provide fully operational radios assigned to each detention officer (including relief officers).
The contractor will maintain a serviceable, in stock, backup quantity of radios that are adequate for all staff and enough to cover backup staff and/or repairs and downtime.

The Contractor will provide for the secure custody, care, and safekeeping of aliens in accordance with the federal laws, standards, policies, procedures for firearms requirements, or court orders applicable to the operations of the federal facility.

The contractor shall enforce disciplinary actions against any alien who is not in compliance with the rules and procedures of the federal facility in accordance with applicable NDS 2026 and applicable ICE policy.

The federal facility shall include a special management unit(s) for administrative and discipline segregation.

DRAFT

If any conflicts between federal, state, or local laws or rules arise, the federal rules shall be followed. Nothing in this performance work statement, is intended to, or shall be construed to be, a waiver of federal supremacy or the immunity of the Government or its contractor, the contractor. Otherwise, applicable or more stringent state or local laws or regulations shall not apply to the performance under this contract when they would directly or indirectly regulate, dictate, or control the contractor's performance under these standards.

In the event a lawsuit is filed against the contractor, in which any claim or allegation contests the legality or propriety of the contractor's performance of its obligations under the agreement or a lawsuit is filed as a result of an alleged administrative error, omission, or intentional act of the Federal Government, ICE, if it determines the contractor abided by the terms of this Agreement during the activity alleged in such lawsuit, will promptly request, and use reasonable efforts to endorse, and recommend that the United States Department of Justice (DOJ), as appropriate, should, but is not limited to, move to either have the contractor dismissed from such suit; have ICE substituted as the proper party defendant; or to have the case removed to a court of proper jurisdiction. ICE will request, endorse, and use reasonable efforts to recommend that DOJ assume responsibility for the defense of any lawsuit described above. The parties acknowledge DOJ assuming responsibility for the defense of any lawsuit arising from the contractor's performance under this agreement is solely at the discretion of DOJ and nothing in this agreement limits the discretion of DOJ on any litigation matters. The parties further acknowledge that nothing in this Agreement provides that the contractor or its employees acting under this Agreement are employees of the Government for wrongful acts or omissions committed by the contractor or its employees. Consistent with federal law including statutes of limitations, the Defense of Suit as outlined in this paragraph will apply even after the contract concludes, in cases where a lawsuit is filed against the contractor for services performed under this contract.

No ICE official other than the CO has the authority to modify the stated terms of the contract or approve any action that would result in additional charges to the government beyond what is stated in the contract line-item number schedule. The Contracting Officer (CO) shall make all modifications in writing.

The contractor does not have a right of refusal and shall take all referrals from ICE. Exceptions may be allowed as determined by the COR or ICE designated official. For example: any alien found to have a medical condition that requires medical care beyond the scope of the contractor's health care provider. In the case of an alien already at the federal facility, the contractor shall notify the ICE designee and COR and request transfer of the alien from the federal facility. The contractor shall permit ICE reasonable time to make alternative arrangements for the alien.

DHS, ICE, federal entities, and ICE-approved third-party inspectors (e.g., contracted support for conducting inspections) will conduct scheduled and unscheduled audits and inspections of performance to ensure contract compliance. Approved inspectors shall always have full access to the federal facility and in all areas of performance. The contractor shall provide full and complete cooperation for all requests related to detention oversight or investigation conducted by the government or approved third-party inspectors on behalf of the government.

DRAFT

Aliens are classified as High (Level 4 - Red), Medium-High (Level 3 - Orange), Medium-Low (Level 2 - Green) or Low-Risk (Level 1 - Blue). Upon discovery that an alien may be a juvenile, the contractor shall immediately notify the COR or ICE designee and follow the instructions of the COR or ICE designee.

The contractor will not house any non-ICE population at the federal facility without the express prior written approval of the CO.

ICE will review and approve all design documents and maintain approval of final inspection of the federal facility before occupancy.

Should a change in the applicable standards and laws identified in this contract result in a documentable financial impact on the contractor, the contractor must notify the CO within 30 calendar days of receipt of the change and both contractor and Government will negotiate best course of action, either 1) a waiver to the Standards or, 2) to negotiate a prospective change in the bed day or other rates. Please note, any change in compensation rate will be prospective, beginning on the date the change is effective.

5.Facility Inspection Schedule

For safety, security, and sanitation purposes, an inspection of housing areas shall be conducted by a supervisor at a minimum of once per shift. The inspection shall be logged into the security logbook and available for review by the COR and/or ICE official. All locks, windows, walls, floors, ventilators, covers, access panels, and doors shall be checked daily for operational wear and tampering. The Contractor shall take immediate action to repair all defective equipment.

The federal facility shall be subject to periodic and random inspections by the COR, an ICE official, or other federal government officials to ensure compliance with ICE Standards.

6.Spatial Requirements

The Contractor shall provide for ICE processing/holding space operated in accordance with ICE policy 11087.2 Operations of ERO Holding Facilities: located at https://icegov.sharepoint.com/sites/inSight-ero/policy/SitePages/Policy%20Statements/11087-2.aspx.

7.Physical Plant

The federal facility operation and maintenance shall ensure that aliens are housed in a safe, secure, and humane manner. All equipment, supplies, and services shall be Contractor-furnished and in operating condition, except as otherwise noted.

The federal facility, whether expansion or an existing physical plant, shall be operated, and maintained in accordance with all applicable federal laws, regulations, codes, guidelines, and policies.

The federal facility shall provide housing configurations commensurate with the security needs of the population.

The federal facility, whether expansion or existing physical plant, shall comply with the building code under which it was permitted at the time of original construction. Any

DRAFT

expansion or renovation of the federal facility shall be subject to the existing and applicable building codes at the time of the expansion or renovation.

The federal facility, whether expansion or existing physical plant, shall comply with the requirements in effect at the time of the original federal facility construction of the *Architectural Barriers Act of 1968* as amended and the *Rehabilitation Act of 1973* as amended. The standards for federal facility accessibility by physically handicapped persons as set forth in "Uniform Federal Accessibility Standards/Fed Std. - 795 4/01/88 Edition" (UFAS) shall apply. All areas of the buildings and site shall meet these requirements.

A safety program shall be maintained in compliance with all applicable Federal laws, statutes, regulations, and codes. The Contractor shall comply with the requirements of the OSHA and all codes and regulations associated with 29 CFR §§ 1910 and 1926 with respect to the Contractor's employees.

Fire alarm systems and equipment – all fire detection, communication, alarm, annunciation, suppression, and related equipment shall be operated, inspected, maintained, and tested in accordance with the edition of the applicable national electrical code and life safety codes under which the federal facility was permitted at the time of original construction. Any changes to the fire alarm systems or equipment shall be subject to the existing and applicable codes at the time of the changes.

The Contractor will provide exterior outdoor lighting, which is enough to illuminate the entire facility federal facility and secure perimeter, subject to ICE's visual inspection and approval.

Promptly after the occurrence of any physical damage to the federal facility (including disturbances), the Contractor will report such damage to the COR and ICE official. It shall be the responsibility of the Contractor to repair such damage, to rebuild or restore the institution.

Government staff will be on-site to monitor contract performance and manage other government interests associated with the operation of the federal facility. Government staff will have full access to all areas of the federal facility. Contractor access to the government required space must be pre-approved by the COR. In case of emergency the Contractor shall notify the COR promptly.

8. Business Permits and Licenses

Throughout the term of this contract, the contactor shall maintain current permits/business licenses and make copies available for Government inspection. The contractor shall comply with all applicable federal laws and all applicable Occupational Safety and Health Administration (OSHA) standards.

ICE/IHSC will review and approve all design documents and conduct final inspections of the federal facility before occupancy. The Contractor should also review Attachment 12 – EOIR Design Standards, and Attachment 13 – Contract Detention Federal Facility Design Standards, and Structured Cable Plant Standard and comply as applicable. The Contractor should also review ICE Health Services Design Standards for all administrative and medical space requirements.

DRAFT

9.ICE Administrative Space

1. Administrative and support space for ICE staff of approximately xx employees **(TO BE UPDATED DEPENDING ON FACILITY – EXAMPLE FOR 60 EMPLOYEES BELOW)**.

Including approximately:

a) 24 Offices – Deportation Officers (DO) (8x8)

b) 4 Offices – Supervisory Detention and Deportation Officers (SDDO) (100 sq ft)

c) 2 Offices – Assistant Field Office Director (AFOD) (100 sq ft)

d) 1 Office – MPA/COR (100 sq ft)

e) 1 Office – DSM (8x8)

f) 1 Office – IT (8x8)

g) 1 Office – Intelligence Officer (8x8)

h) 1 Office – FOD/DFOD drop office (100 sq ft)

i) 1 Office – PIV room (100 sq ft)

j) 2 Offices – Travel (8x8)

k) 1 Secure Contact Window for visitors

l) 1 Waiting Room

m) 1 File room with rolling file shelves

n) 1 Storage Room

o) 1 Supply Room

p) 2 Open areas for Copier/fax/printer/shredder and tables for working with files

q) 8 Workstations – Enforcement and Removal Assistants (ERA) (8x8)

r) 22 workstations – Case Processing Specialists and other visitors assisting ICE (8x8)

s) Employee break room with kitchenette (i.e. small food storage/preparation area including a refrigerator, microwave and sink and garbage disposal at a minimum) - within the ERO area.

t) IT computer support rooms including specialized requirements for climate-controlled IT equipment

DRAFT

u) Conference room (with video teleconferencing (VTC) capability)

v) Secure file room – with safes

w) Male restroom with two stalls, two urinals, and lockers (not used/shared with aliens)

x) Female restroom with three stalls and lockers (not used/shared with aliens)

y) Training room – adjacent to or within ICE space

z) Employee fitness center/weight room that includes male/female showers and lockers in separate rooms – for ERO employees only

aa) Employee firearms lockers that meet NDS standards

bb) Consulate affairs room

cc) Lactation room with running water, refrigerator, and comfortable furniture that is washable. The Contractor is required to provide an ICE office and support space immediately adjacent to the detention federal facility.

All office, administrative, support, and multiple use space shall be complete with appropriate electrical, communication, and phone/fax/VTC connections. VTC connections will use a primary rate interface T1 connection, at a minimum.

All ICE administrative, support, and multiple use spaces shall be clean, free from mold, climate controlled, with Heating, Ventilation, and Air Conditioning (HVAC) thermostat located outside a private office (within open space) controlling no more than 1,500 square feet. The ICE administrative space shall be separate from, but accessible to, housing units and the centralized visiting area. The ICE administrative space shall be secure and inaccessible to Contractor staff, except when specific permission is granted by on-site ICE staff. The Contractor shall be responsible for all maintenance, security, and janitorial costs associated with the ICE administrative space, to include painting the walls and replacing the carpeting every five years. Every other year, the carpet should be cleaned at least once per year or at the direction of the COR and touch-up painting should be done as needed. All ICE administrative and support space shall be cleaned daily (between the hours of 8 a.m. and 4 p.m.) by government cleared Contractor janitorial staff. The Contractor is responsible for coordinating clearance activities for their janitorial staff with the government and for costs associated with clearance. Cleaning services to be performed every day include but are not limited to dusting all surfaces within the open spaces and offices upon request, emptying all trashcans and replacing liners, vacuuming all carpeting, and sweeping and mopping all floors that are not carpeted, cleaning and disinfecting all common touch items such as door handles, countertops, sinks, toilets, and tables.

Stairwells are to be cleaned weekly to include sweeping, mopping, and cleaning the railings.

1. Additional Requirements for ICE Administrative Office Space

All furniture and case goods will be furnished by the Contractor, throughout the length of the contract, and be in good working order with no damage. Any systems furniture,

DRAFT

such as cubicles, shall be electrically hardwired to the building electrical support by the Contractor, and have bottom raceways for data and telecommunications. The systems furniture must have knockouts within the bottom raceways as well as numerous grommets within the work surface. The systems furniture must have some universal requirements for a workspace to include a desk, chair, desk storage, overhead storage (with locking flipper doors) and lighting capacity under the overhead storage. All chairs are to be replaced every 2-3 years or as needed based on condition. All other case goods should be replaced every 5-7 years or as needed. Cubicles will be standard size with a minimum of 64 usable square feet, unless otherwise authorized by the COR. The government will provide and install IT equipment for government office spaces. The Contractor is responsible for providing phone/fax/Internet/VTC services and responsible for the costs for such services.

ICE will provide and install IT equipment in office spaces for ICE personnel only, including CPUs, screens, printers, fax machines, and copiers.

2. **Office of the Principal Legal Advisor (OPLA) Space**
OPLA Space Requirements: Refer to ICE/OPLA Design Standards for specific office and workstation number and sizes as well as specific furnishing and utility requirements to meet ICE's mandated bed capacity for the subject facility. All furniture and case goods shall be furnished by the contractor, throughout the life of the contract, in accordance with ICE/OPLA Design Standards. **(NUMBERS TO BE UPDATED DEPENDING ON FACILITY – EXAMPLE FOR AN APPROXIMATELY 1600 BED FACILITY BELOW)**

The standards include but are not limited to the following:

a) 1 - Office – Supervisory Attorney (100 sq ft)

b) 20 - Offices – Attorneys (8x8)

c) 8 - Workstations – Legal Technician workstations (8x8)

d) 2 - Workstations – Mail/File Clerk (8x8)

e) 1 - Conference room/Law Library

f) 1 - Break room

g) 1 - Supply room

h) 1 - Storage/Copier room

i) 1 - Support workstation for fax/scanner/network printer

j) Separate entrance for OPLA staff is requested with access to the parking lot, which must be ADA compliant

k) OPLA Support Space must be provided per the ICE/OPLA Design Standards

DRAFT

l) OPLA space shall be contiguous

3. **U.S. Citizenship and Immigration Services (USCIS) Space** **(NUMBERS TO BE UPDATED DEPENDING ON FACILITY – EXAMPLE FOR AN APPROXIMATELY 1600 BED FACILITY BELOW)**
Administrative and support space for approximately 8 employees including approximately 4 offices and 4 workstations. Offices must provide complete privacy (i.e. sound proofing) for asylum officers to conduct interviews.

4. **Executive Office for Immigration Review (EOIR) Space**
Refer to ICE/EOIR design standards for specific office and workstation sizes and specific furnishing requirements based on the number of beds at the facility. All furniture shall be furnished by the Contractor in accordance with ICE/EOIR design standards. **(NUMBERS TO BE UPDATED DEPENDING ON FACILITY – EXAMPLE FOR AN APPROXIMATELY 1,600 BED FACILITY BELOW):**

Support space includes:

a. 5 courtrooms - Each courtroom will have the capability to hold live court as well as via video teleconferencing.

b. 5 Courtroom Sub-Lobbies

c. Secure Judge's corridor

d. Public/detainee secure corridors

e. 5 Judges Chambers (hard walled office) (100 sq ft)

f. 2 Court Administrator offices (8x8)

g. 15 Offices (hard walled) (8x8)

h. 15 Workstations (8x8)

i. 1 Visitation space (pro-bono room) must be provided to meet the ACA and NDS standards

j. EOIR Support Space must be provided per the ICE/EOIR Design Standards

k. EOIR space shall be contiguous

5. A separate, Americans with Disabilities Act (ADA) compliant, entrance for judges and staff is required with complete security system and access to parking lot.

For further EOIR space requirements, please see *US Department of Homeland Security, US Immigration and Customs Enforcement, Office of Enforcement and Removal Operations, Contract Detention Federal facility and Intergovernmental Service*

DRAFT

Agreement, Design Standards for Executive Office for Immigration Review, Jun 2011

For further ICE and OPLA space requirements, please see *Contract Detention Facility (CDF) Design Standards for Immigration and Customs Enforcement (ICE), May 14, 2007; addendums: ICE Cabling Standards; Phone Specifications.*

6. Parking Spaces at the Contracted Detention Federal Facility

The Contractor shall provide hard surface (concrete or asphalt) parking for all ICE employees and visitors at no additional cost. A minimum of 150 secured surface parking spaces on-site at the federal facility exclusively for Government employees and ICE visitors' parking spaces shall be reserved for ICE, USCIS, OPLA, and EOIR. The Contractor must provide ICE employee parking on a secure surface (concrete or asphalt) striped parking lot. The ICE employee parking area shall be well lit, shall have privacy mesh on the fencing, and shall drain well. The ICE employee parking spaces shall be striped and have reserved spaces, all spaces shall be painted at least once per year and as directed by the COR or designated ICE official. The ICE employee parking lot shall have an automated entrance and exit gate, operated by the Contractor-provided building access badge system.

The Contractor shall provide an on-site hard surface (concrete or asphalt) parking lot for visitors. Street parking for ICE visitors is not acceptable.

10. Environmental Health

The Contractor shall implement all general housekeeping, environmental cleaning, and disinfection in areas where medical, dental, mental and behavioral health, and intake medical screening services are provided. This includes routine and terminal cleaning of medical housing and medical isolation units. The Contractor submits the implementation plan to the ICE COR.

11. Sanitation and Hygienic Living Conditions

The Contractor shall comply with the requirements of the OSHA and all codes and regulations associated with 29 CFR 1910 and 1926. The Contractor shall comply with all applicable ICE, federal laws, statutes, regulations, and codes.

12. Maintain Institutional Emergency Readiness

The Contractor shall submit an institutional emergency plan that will be operational prior to the end of the transition period, in accordance with NDS 2026, Standard 1.2 Environmental Health and Safety. The emergency plan shall include provisions for two or more disturbance control teams consisting of at least 12 people on each team. The Contractor shall provide protective clothing and equipment for each team member and 20 percent of all additional federal facility detention officers shall be maintained in a secure location outside the perimeter of the federal facility. The plan shall receive the concurrence of the COR prior to implementation and shall not be modified without the further written concurrence of the CO.

The contractor shall contact appropriate state and local authorities to make requests for

DRAFT

assistance in the event of any emergency incident that would adversely affect the community. The contractor shall notify ICE if state and/or local authorities decline to assist during an emergency.

Any decision by ICE or other federal agencies to provide and/or direct emergency assistance will be at the discretion of the government. The Contractor shall reimburse the government for all expenses incurred in providing such assistance.

The Contractor shall submit to the COR a proposed inventory of intervention equipment (e.g., weapons, munitions, chemical agents) intended for use during the performance of this contract. The COR, prior to the end of the transition period, shall provide a concurrence of the intervention equipment. The approved intervention equipment inventory shall not be modified without prior written concurrence of the CO.

13. Armed Transportation Services

The contractor shall provide all such ground transportation services as may be required to transport detainees securely, in a timely manner, to locations as directed by the COR or ICE Designated Service Official, including the transportation of detainees to various appointments. Regular transportation to key sites shall be provided as necessary and additional transportation requirements as requested by the COR or ICE Designated Service Official. When transportation staff are not providing transportation services, the contactor shall assign the employees to supplement security duties, or other activities as approved by the COR. However, the primary function of these staff is transportation. Duties performed by these officers shall not incur any additional expenses to the Government.

The contractor shall assign, at a minimum, two-person teams of armed transportation officers whenever necessary throughout a 24-hour period, seven days a week, including weekends and holidays. The number of two-person transportation teams shall be determined by the COR. When transporting detainees of the opposite sex, assigned transportation staff shall call in their time of departure and odometer reading; and then do so again upon arrival at their destination. A single transportation staff member may transport a single alien only in emergency situations, and only when that transportation member is of the same sex as the alien. Further, if there is an expectation that a pat search will occur during transport, an assigned transportation staff member of the same sex as the detainee(s) must be present to conduct the pat search.

The COR may direct the contractor to transport detainees to any specified location within approximately 250 miles, as required by the contract. Vehicles and transportation officers must meet applicable state and federal DOT and firearm laws. Locations outside the 250-mile radius require advance written approval from the COR, in accordance with the contract requirements. When the COR or ICE Designated Service Official provides documents to the contractor concerning the detainee(s) to be transported and/or escorted, the contractor shall deliver these documents only to the named authorized recipients or his or her designee. The contractor shall ensure the material is kept confidential and not viewed by any person other than the authorized recipient.

DRAFT

The contractor shall comply with all federal and state laws regarding inspections, licensing, and registration for all vehicles used for transportation. The contractor shall provide fully operational radios to each contract staff (including relief staff). The contractor shall maintain a serviceable, in stock, back-up quantity of radios that are adequate for all staff and enough to cover backup staff and/or repairs and downtime. Additionally, the contractor will have staff to monitor the radio traffic in real time and take appropriate action when needed.

The contractor shall transport a detainee to the hospital in an urgent medical situation and for medical appointments. Contract staff shall keep the detainee under constant supervision 24 hours per day until the detainee is released from the hospital or at the end of a medical appointment. The contractor shall transport the detainee back to the detention facility upon release.

ICE anticipates normal transportation requirements other than hospital visits and local needs. In addition to unspecified or miscellaneous locations, the facility must support transportation to and from locations as directed by ICE COR or ICE Designated Service Official. Transportation requirements will include facility transfers and movement of detainees to the flight line.

The contractor shall furnish suitable vehicles in good condition, approved by the government and in accordance with the most current version of NDS, or any modified version published by ICE. The contractor shall provide parking spaces at the facility for the transportation vehicles.

The contractor is not restricted from acquiring additional vehicles as deemed necessary; however, the acquisition of additional vehicles by the contractor shall be at no cost to the government. The contractor shall not allow employees to use their privately-owned vehicles to transport aliens. The contractor shall furnish vehicles equipped with interior security features in accordance with the most current version of NDS, or any modified version published by ICE. Vehicles furnished by the contractor shall be equipped with interior security features such as, but not limited to door lock controls, window locks, a wire cage with acrylic panel between the driver seat and the rear passenger seats and provide physical separation of aliens from transportation officers. The contractor shall provide the interior security specification of the vehicles to ICE for review and approval prior to installation or utilization. For vehicles with a capacity of 15 passengers (including the driver), or more, the driver shall operate the vehicle in accordance with the Commercial Drivers' License (CDL) manual or the highest prevailing standard and must always maintain complete control of the vehicle, obeying all posted traffic signs (including speed limits) and exercising extreme caution, reduced speed, and common sense when negotiating a steep grade or driving in inclement weather or hazardous road conditions.

Personnel provided for transportation services shall be of the same qualifications, receive the same training, complete the same background checks, and wear the same uniforms as other contractor detention officer personnel. Transportation officers shall have the requisite state licenses for commercial drivers with the proper endorsement limited to vehicles with automatic transmission and meet the federal and state licensing requirements.

DRAFT

All transportation detention officers shall be armed. Accordingly, all armed personnel must meet applicable Federal, State, and local firearm laws for every destination requested by ICE.

The contractor shall supply and maintain restraint equipment, per NDS 2025 Standard 1.2 “Transportation by Land.” ICE personnel reserve the right to approve such restraint equipment, as well as the right to inspect such equipment.

Contractor tour of duties will comply with all applicable laws and ICE standards including, but is not limited to, the Federal Motor Carrier Safety Administration, CFR 395.5 - Maximum driving time and maximum on duty time for passenger-carrying vehicles (Hours of Service for Motor Carriers of Passengers | FMCSA (dot.gov)). Overnight lodging resulting from transportation services shall be approved in advance by the COR or ICE Designated Service Official; overnight lodging expenses shall be billed at rates not to exceed the applicable General Services Administration (GSA) per diem rates. Transportation shall be accomplished in the most economic manner and in accordance with the applicable GSA per diem rates. All travel shall occur in accordance with the Federal Travel regulation (FTR) and approved in advance by the COR or will not be reimbursed

The transport of detainees to and from various destinations by the contractor shall be performed by the most economical and direct means, using traditional highways while being cognizant of local traffic conditions. Estimated anticipated routes and/or mileage will be provided to the COR for this requirement. Routes are for informational purposes only and do not in any means dictate future routes or frequencies. Refer to CLIN structure for tracking mileage. Mileage to and from vendor’s depot will not be invoiced or reportable.

The contractor shall establish a fully operational communication system compatible with ICE communication equipment that has direct and immediate contact with all transportation vehicles and post assignments. The contractor shall provide a secondary form of communication in the event the primary form of communication becomes inoperable while in transit.

The transporting of aliens shall not be limited to any specific classification level and may potentially include juveniles and family units as part of support provided to local ICE field offices.

The contractor shall submit a monthly report to ICE Transport Analysis & Support (TRPAS) to include, at a minimum, the information required for every trip as indicated in the G-391 and a copy of the COR monthly report above. See Deliverables section. The G-391 Excel Upload Template and accompanying report will be emailed directly to the TRPAS office with a copy to the COR monthly within 5 business days post invoice acceptance by the COR for transportation services. The Government reserves the right to update the G-391 Upload Template or to provide updated means of uploading transportation data to fix issues, expand capabilities, and improve performance of the worksheet.

If ICE authorizes the contractor to use government furnished vehicles, the following requirements apply to this contract.

DRAFT

a. ICE will provide the contractor with government vehicles and government fleet cards (for the purchase of fuel) for the purpose of transporting aliens to and from ICE designated facilities, or alternative transportation sites. The vehicles assigned for this purpose will remain the property of the government, and all costs associated with the operation and use of the vehicles, such as, but not limited to, vehicle maintenance and fuel, will be covered by the government's Fleet Management Program.

b. The contractor agrees to be responsible for reimbursing ICE for any damage sustained by the vehicles because of any act or omission on the part of the contractor, its employees and or persons acting on behalf of the contractor. The contractor shall be responsible for promptly reporting any accidents or damage to the government vehicles in accordance with any ICE policies that pertain to reporting such damage. The contractor agrees to fully cooperate and assist ICE in making any claims against a third party at fault for causing the property damage to the government vehicles.

In addition, the contractor agrees to hold harmless, indemnify, and assume financial responsibility for any claims or litigations filed by persons sustaining personal injuries or property damage for incidents or accidents caused by the negligent acts or omissions of the contractor, agents, or other persons acting on behalf of the contractor. The contractor agrees to fully cooperate and assist ICE in the defense of any claims made against ICE, and in the event of a settlement or judgment entered against ICE for the negligent acts or omissions of the contractor employees or agents, the contractor agrees to reimburse ICE for said settlement or adverse judgment.

d. For ICE to maintain accurate fleet records of the transportation services, the contractor shall complete specific documentation that will be provided by ICE, to record the times of vehicle usage for proper hourly guard reimbursement, and to record the inspection of the vehicles for damage each time the vehicles are used.

e. The COR will provide forms to the contractor to request and authorize routine maintenance of vehicles.

f. The contractor shall be responsible for any costs or expenses associated with the return of the vehicles, to include towing charges, title replacement fees, or licensing expenses made necessary by the loss of any paperwork associated with the vehicles.

At least one vehicle used to transport detainees must be ADA equipped to safely and humanely transport detainees with disabilities.

The transporting officers shall comply with all local, State and Federal motor vehicle regulations (including DOT, Interstate Commerce Commission, and Environmental Protection Agency), including, but not limited to:

• Wearing a seat belt when the vehicle is moving;

• Holding a valid CDL;

DRAFT

• Inspecting the vehicle, using a government-approved checklist and noting any defect that could render the vehicle unsafe or inoperable;

• Transporting detainees in a safe and humane manner;

• Verifying individual identities and checking documentation when transferring or receiving detainees;

• Driving defensively, taking care to protect the vehicle and occupants; and immediately reporting damage or accidents;

• Driving under the influence of drugs or alcohol is prohibited.

• Alcohol may NOT be consumed eight (8) hours immediately before any shift;

• Maximum driving time (time on the road) is governed by USDOT.

The transportation requirements included in this contract are subject to change at any time based on changes in operational tempo, strategic priorities, or other factors. The Government will make an effort to provide as much advance notice as possible to the contractor regarding changes in transportation requirements, but the Government reserves the right to increase, decrease, or otherwise adjust the required transportation scope as mission needs dictate. If transportation requirements change to the degree that necessitates adjustments to transportation scope and/or contract structure, the contractor will be provided sufficient time to provide an updated price proposal.

14. On-call Guard Services

The Contractor shall provide on-call guard services as requested by the COR and/or ICE designated official and shall include, but is not limited to, escorting and guarding detainees to medical or doctor appointments; hearings; ICE interviews; and any other remote location requested by the COR and designated ICE official. On-call stationary guard services are for detainees housed at the facility only, and only for locations where facility detainees are temporarily located. Contractor shall provide sufficient staff to escort detainees within the facility for routine appointments. Qualified guard personnel employed by the Contractor under their policies, procedures, and practices will perform such services. The Contractor agrees to augment such practices as may be requested by ICE to enhance specific requirements for security, detainee monitoring, visitation, and contraband control. Upon the order of the COR and designated ICE official or in an emergency, the Contractor shall provide an officer to safeguard the detainee(s) at a medical federal facility while undergoing medical examination or treatment as either inpatient or outpatient care. Such assignments may include but are not restricted to medical appointments of detainees. The detainee shall be kept under constant supervision. Public contact is prohibited unless authorized in advance by the COR.

The numbers and frequency of these services shall vary, but to the extent possible, the COR and ICE designated officials shall notify the Contractor 48 hours in advance of such need and four hours of a schedule for the remote post to be manned. One guard shall be authorized for such a post unless the COR specifies additional guards are required. For safeguarding of detainees at secured community Long Term Care and

DRAFT

Inpatient Behavioral Health Facilities, one unarmed guard shall be authorized for such posts unless COR specifies additional guards are required

The following notes are applicable to the above posts:

a) All on-call posts require at least one guard that is of the same sex as the detainee.

b) Additional officers for each post assignment may be required at the direction of the COR and ICE Supervisor when operationally necessary.

c) All necessary meals shall be provided by the Contractor when the detainees(s) are in custody of the Contractor.

d) COR shall follow Contract requirements for each on-call post directed.

e) The Contractor remains responsible for providing security and preventing escapes. The itemized monthly invoice for such on-call guard services shall state the number of hours being billed, the duration of the billing (times and dates to include travel to and from location being guarded) and the names and A-numbers of the detainees who were guarded. Such services shall be denoted as a separate item on submitted invoices. ICE agrees to reimburse the Contractor for actual on-call guard services provided at the negotiated rate.

15. Virtual Attorney Visitation Capability and Operation

a. Space and Technical Requirements:

Virtual attorney visitation is a facility protocol that allows attorneys (or legal representatives) to contact the facility
and schedule VTC visitation with their alien client(s) at least 24 hours in advance of the desired teleconference (at no cost to the attorney or alien).

The facility plant layout and design will accommodate virtual attorney visitation with a ratio of one booth per 100 detainees. The utilized space/room/booths must be private, allowing for confidential attorney-client conversations, and be equipped with video teleconference equipment and/or tablet(s) permitting both visual and audio communications. Phone booths should be soundproofed to at least the 30-35 decibel (dB) level to keep VAV conversations private.

The room/booths must also have a windowed door or other mechanism that allows observation.

b. Operational Requirements:

While the designated space and equipment can be utilized for other purposes, it is expected that virtual attorney visitation will be made available for at least eight (8) hours each day on weekdays and four (4) hours per day on weekends and holidays. See Attachment 01h – Virtual Attorney Visitation for all related requirements.

c. Virtual Court Hearings Capability

DRAFT

When not being utilized for legal visitation, the contractor shall also use the virtual attorney visitation rooms/booths
to facilitate virtual asylum interviews, credible fear interviews, forensic competency evaluations, and/or DOJ EOIR Immigration Judge hearings (i.e., these rooms/booths should be set up to serve these multiple functions). If VAV rooms/booths are to supplement as additional court spaces, they must be in areas that can accommodate different sexes and/or classification levels. VAV court rooms/booths, accommodating up to 1 detained alien, may make up
to half of the required court space with a ratio of one court space per one hundred and fifty (150) detainees. See 5.7 - Executive Office for Immigration Review (EOIR) Space.

16. Notice to Proceed

It is essential that the Contractor is fully prepared to accept responsibility for performing the requirements of the contract. Therefore, ICE may perform required assessments to ensure contract compliance prior to issuance of the Notice to Proceed (NTP). If ICE determines that the Contractor can accept detainees, the NTP will be issued by the Contracting Officer. The Contractor shall be prepared to begin performance and accept detainees immediately upon issuance of the NTP. Performance may begin with staged capacity or open with full capacity, as stated in the NTP. Performance includes, but is not limited to, preliminary fitness determination and training documentation for an adequate number of federal facility staff. Preliminary fitness determinations may take up to 30 days on average to be adjudicated and depend upon the federal facility providing proper initiation documentation and individuals completing the required application and fingerprints once initiated. If proper initiation documentation and fingerprints are not completed and returned timely, the applicant will be discontinued and will have to start the process again to be considered.

The Contractor shall submit in writing a Quality Control Plan (QCP) and all other plans, policies, and procedures, including those identified in the NDS 2026 and ACA standards to the COR for review and concurrence prior to issuance of the NTP. Once written concurrence has been granted by the COR, these plans, policies, and procedures shall not be modified without the prior written approval of the COR. The Contractor's operational and/or corporate policies that do not impact on ICE operations (i.e. policies on employee sick days, vacation days, etc.) do not have to be reviewed or approved by ICE.

17. Federal Facility Security and Control

Security and Control (General)

The Contractor shall maintain a copy of federal facility post orders for employee review within the areas of assignment and shall initiate responses to any incidents as outlined in the post orders.

Contractor employees shall write reports of incidents as outlined in the post orders.

The Contractor will operate and control all designated points of ingress and egress on the site, such as housing units, courtrooms, medical facilities, and hold rooms. The

DRAFT

Contractor shall inspect all packages in accordance with ICE procedures. The Contractor shall comply with ICE security plans.

The Contractor shall adhere to local operating procedures within each federal facility.

The Contractor shall provide, install, and maintain a building access control system in all ICE and/or DOJ administrative space. The Contractor shall provide the government with administrative access and oversight role for system. The Contractor shall comply with ICE security plans.

18. Alien Rights

The Contractor will supervise, observe, and protect aliens from sexual abuse, discrimination, corporal punishment, personal injury, property damage, harassment, or violation of aliens' civil rights. The Contractor shall have a zero-tolerance policy for incidents of sexual abuse or assault.

Aliens have the right to be free from discrimination for any reason, including race, religion, national origin, sex, sexual orientation, sexual presentation, expression, or perception thereof, physical ability, mental ability, or political beliefs.

19. Unauthorized Access

The Contractor shall attempt to detect anyone attempting to gain unauthorized access to the site(s) identified in this contract and notify both ICE and local law enforcement.

20. Direct Supervision of Aliens

The Contractor will provide supervision of all aliens in all areas, including supervision in medical, housing, and activity areas, to permit detention officers to hear and respond promptly to emergencies. This shall include providing medical housing unit security officer with video surveillance unit to view all patients rooms. The Contractor shall have direct supervision of each housing unit. This direct supervision position(s) (determined by the COR based on the size of the housing unit) is separate from the housing control post.

The Contractor shall comply with the requirements applicable to detention facilities contained in Subpart A of the DHS PREA Standards, specifically §115.13, including the development of alien supervision guidelines that are reviewed annually, as outlined in Attachment 10, Prison Rape Elimination Act Regulations.

21. Video Surveillance

1. Installation

The contractor shall ensure video surveillance of hallways, exits, and common areas. Additionally, surveillance systems shall be installed and updated in accordance with DHS PREA §115.18(b). The system shall have a network time protocol (NTP) Server, like Time Machines TM-1000, as an element of the VSS solution to ensure system timing accuracy. All network devices shall be set to periodically communicate with the NTP server to adjust for timing inaccuracies. The contractor shall provide and install a minimum of an 8-hour emergency

DRAFT

power solution for all video surveillance system (VSS) hardware. The power solution can be provided using batteries, emergency generators, UPS, or a combination thereof to meet the requirements. If emergency power is available, via generator, a battery backup must be provided to cover transfer time, minimum of 30 minutes. Network video recorder (NVR) hard disk drives used for video storage, such as the Western Digital ITB-10TB (a.k.a. Purple Surveillance Storage), must be built to withstand continuous read/write activity.

The contractor will determine the storage capacity of the NVR(s) based on the following criteria:

- Quantity of cameras
- Period of motion activated recording per camera
- Frames-per-Second (fps) for each camera
- A minimum of 90 days of storage for each camera
- NVR servers shall have failover capabilities and redundancy to ensure continuous function in the event an NVR experiences a failure
- Workstations to export video evidence in open format such as audio-video interleave or QuickTime Movie (e.g. avi or mov) and provide chain of custody
- H.265 or better compression

2. **Camera Resolution**

Cameras should capture video with a minimum resolution of 40 pixels-per-foot (PPF) at the target distance. Cameras must provide 100% coverage of perimeter, detention and high-security areas. In detention holding cells, cameras will be mounted such that video is not seen or recorded in the toilet/privacy area. All cameras will have 2-megapixel or better resolution. ICE may designate a select number of cameras covering high security or critical areas as 5-megapixel or better to identify a person (facial recognition) or object (license plate recognition) with enough detail for courtroom quality. All exterior cameras shall have an infrared (IR) cut-filter and/or IR night time illuminator either built in or added as an accessory. All exterior cameras shall be environmentally protected based on the prevailing weather conditions for the geographical area and as prescribed by the camera manufacturer. Fixed, pan-tilt-zoom (PTZ), 180-degree and 360-degree panoramic or multi-head cameras are acceptable. PTZ cameras shall not be programmed on an area tour to provide 100% coverage. These cameras shall only be utilized for additional monitoring capability. Cameras shall be positioned to prevent tampering which includes installing in fixed, tamper and vandal resistant enclosures. Cameras installed in detention areas (housing area, holding, etc.) will be detention grade.

DRAFT

Monitors shall have the appropriate built-in video and management ports based on the VSS system design requirements and shall not have any wireless connection (Wi-Fi, Bluetooth etc.) capability enabled. Wall mounted monitors shall be installed using a premium type full-motion wall bracket to provide tilt, swivel and arm extension capabilities, unless specified differently by ICE. For multiple monitor installations videos shall be organized for security personnel to easily follow movement through the facility from one camera to the next in a smooth flowing fashion without having to bounce back and forth among monitors. VSS workstations and decoders shall not exceed the manufacture's recommended number of displayed cameras or connected monitors.

All monitors shall be capable of viewing the specified number of camera views listed below at 30 fps (real time) with no lag:

- Monitors for general area observation shall be capable of 16 camera views per monitor.

- A minimum of 27-32" monitors shall be utilized for guard stations and other areas where size restrictions will not allow 42-50" monitors. Monitors shall be capable of 8 camera views per monitor

- 22-26" monitors shall be utilized for VSS workstations, alarm call-up, or specific spot area monitors.
  Monitors shall be capable of 1-4 camera views per monitor.

All AC voltage powered devices shall be connected to a centrally located uninterruptable power supply (UPS) in the designated IT/LAN equipment and frame/closet rooms. Each equipment room will contain a building-grounded, grounding buss bar which will be utilized for equipment rack and panel grounding connectivity. As part of the VSS package, the contractor shall provide a rack mount keyboard-video-mouse (KVM) console with appropriate cabling for connection to each NVR and matrix (if used), or properly configured network client with remote access (on the dedicated VSS network), for video and software management and maintenance.

Man-down and duress system for officer safety shall be integrated with VSS.

3. Warranty

The contractor shall have warranty all contractor supplied components, workmanship and/or systems for a (minimum) period of 12 months from the date of Government acceptance. After the one-year base warranty period the contractor shall include four one-year option periods for technical services, support, testing, maintenance and repair of the system and components installed in this PWS. This includes coordination with ICE and other Government offices providing support to the ICE facilities.

In the event any contractor-supplied equipment, component, part fails within the specified warranty period; the contractor shall immediately replace or repair the item within 24 hours at no additional cost to the Government. If the contractor is

DRAFT

unable to rectify the issue(s) within the allotted time, the contractor shall be liable for all costs incurred by the Government to correct the issue(s).

4. **Maintenance**

The contractor shall perform maintenance related tasks, including asset management and inventory services (provide inventory), Preventative Maintenance (PM), upgrades and repairs, equipment disposal, integrated support services, and other maintenance and service-related tasks on all Video Surveillance Systems (VSS).

The contractor is responsible for the scheduling and execution of preventive maintenance on all ICE VSS electronic security equipment and systems. Critical components are those required to provide security (IDS, VSS, access control, etc.) for a perimeter access point or critical area. The contractor shall implement a maintenance program for all security systems. Any critical component that becomes inoperable must be replaced or repaired. (See table for repair times.)

The contractor shall conduct quarterly, semi-annual, and annual maintenance at the facility. The primary purpose of maintenance is to reduce component down time and optimize the equipment life cycle.

Quarterly:

- Software updates
- Firmware updates
- Patches

Semi-Annually:

- Preventive maintenance
- Camera cleaning
- Head-end rack equipment cleaning (Racks, Workstations, Servers, PoE switch, UPS)

Annually:

- Equipment functionality testing of all equipment and devices

Testing and Maintenance. Prior to testing any VSS equipment the contractor shall notify the ICE OPR Point of Contact. The ICE point of contact is the Governments designated person that will be on the project site when needed to discuss matters with the contractor.

The contractor shall perform on-site functional evaluations of existing security systems at the identified ICE facility per manufacturer's specifications, and if necessary, shall recommend methods of remediation to make the system fully operational per manufacturer and DHS/ICE specifications. The contractor shall be solely responsible for conducting any repair or replacement

DRAFT

work required to maintain the systems in the condition prescribed by the original equipment manufacturer's recommended guidelines and/or warranty requirements (where the warranty remains in force).

If any components are found to need repair or replacement, the contractor shall be responsible for following all procedures listed in this PWS. Failure to follow any procedures listed in this PWS shall be done at the contractor's risk. The contractor shall perform a complete inspection and functional test of the VSS System, verifying 100% functionality, per manufacturers and DHS/ICE standards, of all system capabilities to include, but not limited to: pan, tilt, tilt, zoom features, recorders, monitors, controllers, fiber optic transceivers, and connections associated with the system.

Scheduling of Routine Maintenance. Maintenance shall be performed at each location semi-annually. Maintenance visits shall be scheduled no less than 90 calendar days apart.

Quarterly Maintenance. The contractor shall provide on-site software maintenance support, software and firmware upgrades, software patches, virus protection, and system configuration changes, as necessary. This support shall start upon successful completion of the Substantial Completion Inspection (SCI) and include support for the Video Management Software System components. The contractor SHALL NOT use Remote Desktop connections, (e.g., Microsoft's Remote Desktop Protocol (RDP), without the use of an authentication method that employs secure authentication (two-factor, encrypted, key exchange). Use of removable media for maintenance purposes shall adhere to the policies and procedures established by the System Owners.

The contractor shall maintain an incident log as part of the software maintenance program, recording therein all deviations from normative operations, and all corrective actions taken. The incident log shall be submitted to ICE/OPR upon detection of anomalies, quarterly, and at the end of the contract period.

Semi-Annual Preventive Maintenance/Cleaning. The contractor shall perform preventative maintenance on all VSS equipment as specified by ICE and the manufacturers and DHS/ICE specifications and industry best practices. Preventative maintenance functions shall include but are not limited to, focusing and back-focusing of cameras, cleaning of recording devices (servers, NVRs, DVRs), switches and verification of controller programming.

Annual Maintenance and Testing. Use Appendix F for Performance Standards. The contractor shall verify the video transmission system, and that any signal or control cabling has been installed, tested, and approved as specified by the manufacturer's specifications. The contractor shall verify that the remote devices are operationally functional per the manufacturer's specifications and interface with the designated security center and perform all functions of which the system was designed and installed.

DRAFT

Contractor shall verify the switcher is fully functional and that the switcher software has been programmed for specific site configuration. The contractor shall verify switcher software is functioning correctly by manufacturer's specifications. All software functions shall be exercised. The contractor shall operate all electrical and mechanical switcher controls and verify that these controls perform as per the manufacturer's designed function.

Contractor shall verify that all video sources and video outputs provide a full bandwidth signal compliant with Electronic Industries Association (EIA) 170 for all video inputs. The contractor shall verify all video signals are terminated according to manufacturer's specifications. The contractor shall consult with ICE/OPR that all cameras are aimed and focused properly. The contractor shall conduct a walk test of the area covered by each camera to verify field of view. The contractor shall ensure that cameras remain properly oriented so that the picture is not degraded by any obstruction that prohibits the desired field of view. This could include, but not limited to the rising or setting sun, foliage, shrubs, and trees.

The contractor shall verify night assessment capabilities to ensure night mode functionality of the system is fully functional per the manufacturer and DHS/ICE specifications.

Contractor shall verify all cameras are synchronized and the picture does not roll when cameras are switched. All cameras shall be fully operational and functional per manufacturers and DHS/ICE specifications. When PTZ mounts are used on a system, contractor shall verify the limit stops have been set within manufacturer specifications. Verify all controls for pan/tilt or zoom mechanisms are operative and the controls perform the desired function as specified in the user's manual.

If pre-position controls are used, contractor shall verify all home positions have been set according to the ICE/OPR directions and have been tested for auto home function and correct home position. The contractor shall deliver a report describing results of functional tests, diagnostics, and calibrations to ICE/OPR.

If repairs or replacements are discovered during testing & maintenance, the contractor shall contact the ICE/OPR and only after the ICE/OPR's acceptance of the contractor provided quotation and written approval shall those repairs or replacements be completed. The contractor shall fully complete these repairs & replacements if possible while on-site. If the ICE/OPR POC determines the delay of the repair or replacement could significantly harm the security posture of the facility, the ICE/OPR may authorize the repair or replacement as an emergency. The contractor shall make necessary repairs and/or replacement of equipment upon the approval and funding from ICE. See Section 2.0 for Repair and Replacement Procedures.

The contractor shall perform preventative scheduled maintenance on VSS. The contractor shall provide a detailed description of all preventative services

DRAFT

performed to ensure reliability of the system performance and optimal functionality per manufacturers and DHS/ICE specified capabilities. The contractor shall include in the O&M manual a copy of all manufacturer warranties, terms, and conditions.

The contractor shall provide a Performance Test and Acceptance Plan (PTAP) to the ICE/OPR POC no later than five (5) business days after each annual preventative maintenance session for review and approval. The plan shall be developed in accordance with all manufacturer specifications and design standards and address all systems and components. The PTAP shall be used to verify the performance of all installed equipment and systems. The plan shall detail the steps the contractor will use to test the performance of each system and its related components. The plan shall include a system acceptance form designated as a checklist for each of the major subsystems identified by the contractor and verified by the ICE/OPR POC. The acceptance form shall be signed by the ICE COR for the invoice to be paid for the service. Copies of all signed forms shall be given to the ICE/OPR POC.

The PTAP shall include, at a minimum, the following: an updated installed equipment list highlighting changes from the most recently approved plan; location of each piece of equipment; equipment to be identified by make, model and serial number for VSS components that are not encased in some camera enclosures; tests conducted; results of each test; recommendations; date and time of testing; name, position, signature of person conducting testing; status of current equipment, based on a scaled status (1 being poor to 5 being excellent.) The exact scaled status is up to the discretion of the contractor; a brief explanation of failures and corrective actions; and notes to include any concerns or upcoming issues.

5. **Repair and Replacement**

The contractor shall install all replacement parts required to maintain, repair, and keep all VSS systems fully operational and free of deficiencies per the manufacturers and DHS/ICE specifications. Additionally, the contractor may be required to alter, install, interface, improve and/or overhaul equipment, which, when completed, shall modify and/or enhance the aesthetics, operation, performance, reliability, safety etc. of the systems beyond existing levels. No alterations or improvements to equipment shall be made without written authorization from the ICE/OPR POC.

For repairs, replacement and/or addition of equipment, the contractor shall prepare a cost estimate to correct the problem prior to commencing work. This cost estimate shall include costs for parts and materials needed to restore the system. If the cost for the corrective action is equal to or less than $3,500.00, the contractor shall coordinate with the ICE/OPR and proceed with the work as a minor repair or replacement; if the cost for corrective action is greater than $3,500.00, the work is considered a major repair or replacement, and advance approval shall be given by the ICE/OPR POC prior to the contractor proceeding

DRAFT

with the work.

Repair work shall not exceed $3,500.00. The contractor shall notify the ICE/OPR POC if at any time 85% of the dollars for the CLIN have been expended. The Government reserves the right to perform or supplement performance of contract functions with Government personnel or other contractors for major repairs, replacement and/or if the Government considers the contractor's estimate to be unreasonable.

If during any 30-calendar day period more than 20% of the installed VSS equipment has been repaired or replaced, ICE reserves the right to disallow any further repairs and will determine the long-term cost effectiveness of any further repairs as opposed to replacing the entire system. If it is determined by the ICE/OPR POC that the entire system in any building shall be replaced, the replacement shall be subject to competition.

If during any 60-calendar day period more than 40% of the installed VSS equipment has been repaired or replaced, ICE reserves the right to disallow any further repairs and will determine the long-term cost effectiveness of any further repairs as opposed to replacing the entire system. If it is determined by the ICE/OPR POC that the entire system in any building shall be replaced, the replacement shall be subject to competition.

All replacement units shall be technically equivalent, compatible with the existing system and NDAA-compliant. Where applicable, devices shall be configured using Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) configurations in accordance with DHS 4300A Sensitive Systems Policy.

Service Request Timeframes. Repair or replacement service shall be performed seven days a week, 24 hours a day. The on-site completion times will be adhered to according to the table below. The repair completion time shall begin when ICE is notified by the contractor of the need and the contractor provided quotation is received and confirmed by the ICE/OPR POC. ICE will then either give written or verbal approval of the quotation to the Program Manager to complete the repair or replacement.

If the contractor is unable to meet the service response times or fails to repair the equipment correctly due to technical reasons (inability or incompetence to troubleshoot), the Government shall deduct a penalty of $550.00 per day the repair and replacement is not completed that exceeds the Standard Service or Emergency Service Completion timeframes, reference Section 3.0.1.

These response times shall not be deviated from. The responsibility of meeting these response times shall be completely on the contractor. At no time shall the contractor wait to complete repairs or replacements for regularly scheduled testing & maintenance periods for the contractor’s convenience. The response is dependent on the Facility Security Level (FSL). If the contractor is unable to meet the service response times or fails to repair the equipment correctly due to

DRAFT

technical reasons (inability or incompetence to troubleshoot), the Government shall deduct a penalty of $550.00 per day the repair and/or replacement is not completed that exceeds the listed service completion timeframes below.

FSL	Quotation Response	Standard Service Completion	Emergency Service Completion
1	0-24 hours	72 hours	36 hours
2	0-24 hours	72 hours	36 hours
3	0-12 hours	24 hours	12 hours
4	0-12 hours	24 hours	12 hours

Standard Service Request. The contractor shall provide a written quotation for any non-emergent repairs or replacements within 12 hours of notification. After reviewing the contractor-provided quotation, ICE will accept or reject the repair or replacement. The Standard Service Completion time will begin upon acceptance by the ICE/OPR POC of the contractor-provided quotation.

Service Response Times. If the contractor is unable to meet the service response times or fails to repair the equipment correctly due to technical reasons (inability or incompetence to troubleshoot), the Government shall deduct a penalty of $550.00 per day, through a contract deficiency report, the repair and replacement is not completed that exceeds the Standard Service or Emergency Service Completion timeframes. See above table in E.6.31.

Emergency Service Request. The same procedures shall be used for an Emergency Service Request as the Standard Service Request. A quotation shall be provided within 12 hours of being notified of the service request. The ICE/OPR POC will give authorization to complete the repair or replacement, at the ICE/OPR POC's discretion. If this procedure is not followed, the contractor shall not receive payment for the repair or replacement. The emergency service completion time will begin upon acceptance by the ICE/OPR POC of the contractor provided quotation.

Special Considerations. Delays such as the ordering of replacement equipment that will take longer than the allotted repair completion times shall be communicated to the ICE/OPR POC verbally, and in writing.
To accompany this communication shall be the contractor's estimated timeframe for deliverables and scheduled plan of actions. The ICE/OPR POC shall have the right to approve or disapprove these special considerations.

Outdated Equipment. For the equipment that is outdated and no longer commercially offered, a technically equivalent and compatible piece of

DRAFT

equipment shall be offered by the contractor. The ICE/OPR POC still has final rights to approve or discuss the contractor offered equivalent and compatible equipment. No loaner equipment shall be used.

Quotation Specifications. In the contractor-provided quotation, the contractor shall clearly indicate what piece of equipment is being repaired or replaced per the equipment lists provided by the contractor. This quotation shall be sent via email to ICE.

Invoicing Specifications. Testing and Maintenance invoices shall be submitted only after acceptance by the ICE/OPR POC of the PTAPs and updated Equipment Lists and Inventories (after the end of each quarter). The invoice should be in Excel format and sent as an attachment by email.

Repair and Replacement invoices shall be submitted monthly. All completed work will be invoiced at the end of the month.

6. **Maintain and Operate the Video Surveillance Program**
A qualified individual shall be responsible for monitoring this system inside and outside the building. Considering that the videos will be recording residents who may be seeking asylum or other considerations under U.S. immigration law, the contractor is required to maintain the recordings and may not release them to anyone, unless approved by the CO in accordance with applicable Federal laws and regulations. All video/audio recordings are considered federal records and must be retained in accordance with ICE schedules. Any Video/audio recordings by law enforcement personnel and contractors performing law enforcement activities on behalf of the agency during the performance of their duties determined to have no evidentiary value, must be retained for 60 days. However, video/audio surveillance that is determined to have evidentiary value or have a high likelihood to become evidentiary in criminal, civil, administrative, or other legal proceedings (e.g., assault, use of force, etc.) must be retained for 3 years, if it is not associated with a case file. If the video becomes part of an investigation it is maintained in accordance with that schedule. NARA Records Schedule Number: DAA-0567-2023-0002.

Health Insurance Portability and Accountability Act (HIPAA) does not explicitly mention "video recordings," its rules for Protected Health Information (PHI) and Electronic PHI (ePHI) would still apply, for example, facilities should use technology to pixelate or blur sensitive information, such as computer monitors displaying patient records, whenever releasing recordings for non-medical requests.

7. **Body Worn Cameras**
To augment stationary cameras, the vendor shall propose a body-worn camera program to document detention guard interactions with detainees during periods of heightened risk (e.g. during transport, use of force activities, periods of unrest or disturbance, etc.).

DRAFT

22. Mail Processing

The contractor shall utilize advanced scanning technologies to detect prohibited materials in special correspondence mail without opening it, through imaging, chemical analysis, and other methods. The contractor's technology shall both detect and identify hazardous materials at trace levels. The contractor shall develop, implement, and maintain processes and policies related to the safe handling of mail and hazardous materials.

The contractor shall establish and follow procedures to ensure that all facility staff use appropriate personal protective equipment (PPE) during the handling of incoming mail and hazardous materials. The contractor shall provide initial and recurring staff training on mail processing, including the identification and proper handling of hazardous materials.

23. Detention Management System

The contractor shall procure, install, and maintain an information system capable of electronically tracking and securely reporting to the ICE system of record in real time:

- Facility census to include but not limited to encumbered and available bed capacity,
- Detainee movements (i.e. intra-facility movements, book-ins/book-outs, and external movements including transportation, etc.),
- All records related to detainee management and housing including but not limited to detainee grievances and requests, detainee housing assignments, detainee classification, medical requests, appointments, segregated housing placements, use of force incidents, and other updates as requested by the COR.

The design of this system and contractor policies and activities shall abide by ICE system security, records management requirements (including record retention schedules) and detention management data requirements as directed by ICE Office of the Chief Information Officer (OCIO) / Law Enforcement Systems and Analysis (LESA) through the CO or COR.

24. Logbooks

The Contractor shall be responsible for completion and documentation of the following information in the logbooks, for each shift:

a) Activities that have an impact on the population (e.g., counts, shakedowns, movement, and escorts to and from court).

b) Shift activities (e.g., security checks, meals, recreation, religious services, property lockers, medical visits).

c) Entry and exit of vehicles and individuals other than aliens, ICE staff, or Contractor staff (e.g., attorneys and other visitors).

DRAFT

d) Fire drills and unusual occurrences.

e) Recreation time.

25. Reports

The Contractor shall furnish, daily, a manifest of all aliens currently detained in the federal facility. The manifest shall contain the following information for each alien: "A" File Number (system of numbering supplied by ICE); office received from; name; date of birth; sex; nationality; date of arrival; number of days the alien has been in the federal facility; and type of release, if applicable. The manifest shall be transmitted in a Microsoft Excel format, unless otherwise directed by ICE. The Contractor shall conduct a daily reconciliation of the ICE detention manifest and the Contractor manifest to ensure accuracy. Any discrepancies in the reports shall be the responsibility of the Contractor to immediately rectify and bring to the attention of ICE.

The Contractor shall provide monthly status reports to the COR and ICE officials. Such reports will include a monthly key indicator report, which indicates the key personnel positions of the federal facility (e.g., position title, name of the employee, vacancies and length of vacancies, dates of service, and additional comments). These monthly reports shall be submitted to the COR and ICE officials by the fifth of each month for the previous month's activities and staffing.

The Contractor shall prepare required orders, instructions, and reports of accidents, security violations, fires, and bomb threats. The reports shall be maintained on file, concerning all activities in connection with duties and responsibilities for the services performed under this contract. All such records shall be kept using a system with a written policy, which allows the reports to be made available to the government for inspection.

The Contractor shall, at the request of ICE, prepare any special or other reports, or issue further orders and instructions and may be required in support of work within the scope of this contract. The distribution, format, and time elements for these reports shall be directed by government requirements.

26. Daily Inspections

Staff will check all bars, locks, windows, walls, floors, ventilation covers, glass panels, access plates, protective screens, doors, lights, and equipment for operational wear and alien tampering. Staff shall also report slippery floor surfaces. This documentation will be made daily in a logbook. Problems discovered during these inspections shall be clearly identified in the documentation.

The Contractor shall also notify the COR of any abnormalities or problems. The Contractor shall immediately notify the COR and ICE officials of any physical federal facility damage. Written documentation of any problem areas shall be submitted to the COR by the end of the shift.

DRAFT

27. Deviation from Prescribed Schedule Assignments

The Contractor is authorized to deviate from the scheduled assignment when unusual conditions or circumstances so demand, and if prior approval is received from the COR. All deviations shall be recorded in the daily logbook. When the COR is not available, the Contractor shall notify the ICE official immediately or as soon as is practicably possible.

28. Suicide Prevention

The Contractor shall develop and implement a comprehensive suicide prevention and intervention program in accordance with ICE policy and standards. This program shall include staff training and protocols for managing aliens who require placement on suicide watch. This must include security officers documented monitoring every 15 minutes or more frequently if necessary per NDS standards. Clinical staff must perform welfare checks every 8 hours.

29. Escapes

The Contractor shall take all appropriate measures to prevent escapes. The Contractor shall notify the COR and ICE official immediately if an escape or an attempted escape has occurred. The Contractor shall provide the COR and ICE officials with a written report prior to the end of the shift. The Contractor shall be held to the following standards concerning escapes:

a) The Contractor assumes absolute liability for the escape of any alien in its control.

b) The Contractor shall provide written policies and procedures regarding the actions to be taken in the event of an escape. This document must include reporting requirements for all contract employees, escorts, supervisors, and management personnel. These procedures will meet with the approval of the COR, be reviewed at least annually, and updated as necessary.

c) Escapes shall be grounds for removing the responsible Contractor employee(s) from duty if the Contractor employee(s) is/are determined by the Contractor or the COR to be negligent, reckless, or intentionally responsible for the escape. Notice of removal shall be provided to the CO.

d) Corrective actions to prevent future escapes or attempted escapes shall be taken immediately and communicated to the COR for approval. A written report of the remedial action shall be due to the COR within 24 hours of an escape or attempted escape.

e) An escape is deemed an egregious incident and subject to the expedited processing of a contract discrepancy report resulting in a deduction or withholding for any applicable standards violations.

30. Evacuation Plan

The contractor shall furnish emergency evacuation diagrams showing exit routes as well as 24-hour emergency evacuation procedures.

DRAFT

31. Injury, Illness, and Reports

The Contractor shall immediately assist employees, aliens, or others on the premises in need of immediate help or those who are injured or ill. Contractor employees shall provide first aid and CPR when necessary

32. Food Service

Manage Food Service Program in a Safe and Sanitary Environment

The Contractor shall provide aliens with nutritious, adequately varied meals, prepared in a sanitary manner while identifying, developing, and managing resources to meet the operational needs of the food service program.

The Contractor shall provide a sack meal for aliens in custody, those who are absent during any meal, planning for departure, or for aliens on certain travel routes (upon order by the ICE COR and/or designated official). Further, the Contractor will provide alien sack meals as requested by ICE staff. The contents of the sack meals must be approved by COR and ICE official.

At the COR's request, the Contractor shall provide sack meals for aliens in ICE custody, but not yet on the Contractor's premises.

Minimum Daily Calories

The contractor shall follow U.S. Department of Health & Human Services Dietary Guidelines for Americans (www.dietaryguidelines.gov). The menus must be certified as exceeding minimum daily nutritional requirements, meeting or exceeding U.S. recommended daily allowances (RDAs).

33. Health Services

33.1. Facility Care Levels:

Facility Care Levels are based on the level of care required by ICE. The definition for all IHSC Levels and Baseline Clinical Capabilities requirements will be provided by ICE/ERO/IHSC. As designated by ICE ERO/IHSC, the Contractor will ensure adequate medical and behavioral health staff, as well as facilities and equipment to provide the following services at a minimum:

- Facility Care Level 4: Facilities at this level shall provide medical management for individuals with complex, chronic medical conditions that require frequent clinical interactions to maintain control or stability of the condition, including assistance with activities of daily living (e.g., feeding, toileting, bathing, and hygiene). Such facilities are intended to prevent hospitalization or further medical complications. For behavioral health, Care Level 4 facilities shall be inpatient facilities.

- Facility Care level 3: Facilities at this level shall provide medical management for stable patients who are suitable for outpatient care but require regular clinical interventions and clinician evaluations at intervals ranging from monthly to every three months. These facilities must have access to enhanced medical resources, including consultations with

DRAFT

specialty services provided by medical specialists in the local community.

- Facility Care Level 2: Facilities at this level shall provide medical management for stable chronic conditions across all age groups (e.g., diabetes, hypertension, asthma).

- Facility Care Level 1: Facilities at this level shall provide medical management for detainees under 60 years of age who are otherwise healthy.

33.2. Space Requirements:

The Contractor shall provide adequate space for health services, to include office and support space within the medical clinic. The facility must include sufficient space for services such as infectious disease screening and treatment; emergent, acute and chronic care; on-site sick call; medical housing (infirmary), dental services; mental health services; and an on-site pharmacy. Space provided shall be adequate to account for the needs of the full anticipated population.

Medical staff shall have space available for secure storage of medical records. Spatial and equipment requirements for medical record storage rooms shall comply with the IHSC Design Standards.

33.3. Medical Area

The Contractor shall maintain uniform procedures for the safe handling and disposal of sharp objects to prevent injury and transmission of infectious diseases, especially the hepatitis B virus (HBV) and the human immunodeficiency virus (HIV).

- Inventory control shall maintain a perpetual inventory of sharp instruments (needles, syringes, scissors, etc.). Inventory shall be reconciled weekly by the Health Services Administrator (HSA) or designee.
- Handling and used sharps shall be placed immediately, without removal of needles or replacement of covers, into the National Institute for Occupational Safety and Health (NIOSH)-approved biohazard containers.
- Disposal containers shall be labeled “Infectious Waste” or with biohazard symbol. Sharps are disposed through a licensed commercial Contractor in compliance with federal and local infectious and hazardous waste regulations.

In the event of accidental exposure, a written exposure-control plan shall be followed in all needle-stick incidents.

33.4. Health Services Overview

The Contractor is responsible for providing all medical services for this contract.

The Contractor shall furnish 24/7 on-site health care as defined by the Facility Local Health Authority (usually the Health Administrator). The Contractor shall not charge

DRAFT

any ICE detainee a fee or co-payment for medical services or treatment provided at the facility. In accordance with 18 USC 4006(b)(1), the Contractor shall not charge the government more than would be paid "for the provision of similar health care items and services under the Medicare program under title XVIII of the Social Security Act." The Contractor shall ensure that ICE detainees receive no lower level of onsite medical care and services than those spelled out in the current applicable ICE detention standards or any modified version of it published by ICE and based on community standards of care.

The Contractor shall be responsible for providing both culturally competent and trauma-informed health care services for all ICE detainees at the facility in accordance with the applicable ICE detention standards, ACA standards, and any other accreditation standards, which refers to formal certification by authorized organizations confirming compliance with established health care service standards that are in place at the time of award of this contract or incorporated through modification.

The Contractor shall provide detainees with access to medical services, preferably on-site, or via telemedicine, with minimal wait times for community providers. Telehealth shall not be utilized for daily mental health treatment for patients on suicide watch. Tele-Behavioral Health shall not be utilized to remove or change suicide precautions. Additionally, all mental health providers shall have the highest-level clinical certification and/or license in their profession within the state where the provider is practicing, except as otherwise provided herein. Services provided shall include but are not limited to, intake arrival screening; infectious disease screening and treatment; emergent, urgent, acute, chronic, and emergency care; on-site sick call; treatment of minor injuries; treatment of special needs; providing mental health services; dental services to include dental health assessments; participating in quality improvement and risk management activities; and provision of over the counter and prescription medications:

a. On-site health care personnel shall perform initial medical screening within 12 hours of arrival to the facility. Each detainee shall be given an opportunity to shower and shall be issued clean clothing, bedding, towels, and personal hygiene items. Arrival screening shall include, at a minimum, testing for TB infection and/or disease, and the elicitation and recording of past and present medical history (mental and physical, dental, pregnancy, lactation or post-partum status, history of substance abuse, screening questions for other infectious disease, and current health status including any physical or developmental disabilities or impairments):

    1) The Contractor shall elicit a medical history and provide recommended vaccinations for ICE detainees pursuant to Centers for Disease Control and Prevention (CDC) and the Advisory Committee for Immunization Practices (ACIP) or state health department recommendations. This requirement applies, at a minimum, to populations at highest risk (e.g., individuals with diabetes, HIV, cancer, seizure disorders, heart disease, asthma, cancer and over the age of fifty (50), pregnant females, and other special populations), as well as those necessary to address pandemic events in accordance with ICE guidance and CDC recommendations.

    2) Measurement of height, weight, and a complete set of vital signs (BP, P, R,

and T) shall be completed during initial screening. Blood sugar and pulse oximeter O2 readings may be necessary dependent upon specified diagnosis or current medical concern exhibited or verbalized by the detainee and observed by medical provider; and detainee responding in the affirmative shall be sent for evaluation to a qualified, licensed health care practitioner as quickly as possible, but no later than two calendar days.

3) Pregnancy screening shall be completed during initial screening to ensure all female detainees/residents ages 10-56 complete a pregnancy test. The FOD shall be notified immediately regarding females determined to be pregnant, but no later than 72 hours after such determination. The Field Medical Coordinator (FMC) and other IHSC personnel shall coordinate with the Assistant FOD and /or FOD in ensuring that detention facility staff are aware of these notification requirements pursuant to ICE Directive 11032.4: Identification and Monitoring of Pregnant, Postpartum, or Nursing Individuals.

b. A comprehensive health assessment to include a history and physical examination shall be completed within the first 14 days of an adult detainee arrival unless the clinical situation dictates an earlier evaluation. Detainees with chronic medical, dental, and/or mental health conditions shall receive prescribed treatment and follow-up care with the appropriate level of provider and in accordance with the ICE detention standards, ACA standards, and any other accreditation standards, which refers to formal certification by authorized organizations confirming compliance with established health care service standards.

c. The Contractor shall utilize the following IHSC-developed screening tools: Intake, comprehensive health assessment (i.e., 14-day physical examination), Mental Health Assessment, or equivalent:

1) The Contractor shall offer the following discretionary mental health screening tools to direct patient care providers: Columbia-Suicide Severity Rating Scale (C-SSRS), Patient Health Questionnaire (PHQ)-9, General Anxiety Disorder (GAD)-7 , Mini Montreal Cognitive Assessment (MoCA), full MoCA, World Health Organization (WHO) Disability Assessment; Additional evidence-based screening tools can also be used at the discretion of the Contractor;

2) The Contractor shall add a data-field to relevant screening and assessment forms indicating that a qualified mental health provider (QMHP) has reviewed available medical records and will document which records specifically have been reviewed;

3) Within the electronic health record (EHR), the Contractor shall implement a built-in prompt, or equivalent, to auto-refer a non-citizen for a Mental Health Assessment following a positive intake screening or comprehensive health assessment;

4) Contractors operating in Arizona, California, and Washington, shall add an EHR data field requiring the QMHP to indicate whether the non-citizen

DRAFT

meets designated medical criteria (see section, Serious Mental Illness) after each mental health visit. If the QMHP determines the non-citizen does not meet the designated medical criteria, the QMHP will document the rationale.

d. The Contractor shall ensure that its healthcare system/employees solicit and triage detainees' requests for healthcare (sick call) daily and that this is tracked through a written system of accountability and within the health record with care delivered per current ICE detention standards, ACA standards, and any other accreditation standards, which refers to formal certification by authorized organizations confirming compliance with established health care service standards.

e. Upon receipt of an authorization to transfer a detainee from ICE/ERO to another facility, the medical provider shall prepare and provide a Medical Transfer Summary or equivalent form that includes at minimum: current medications, current diagnoses, scheduled and/or medically indicated appointments and consultations (to include any referred community specialty care appointments), and medical equipment for continuity of care. (IHSC Form 849).

    1) Transporting Officer: the transporting officer shall review the Medical Transfer Summary, or equivalent form for completeness and to make sure he or she has the supplies required to provide any in-transit care that is indicated. The Transporting Officer is responsible for delivering the Medical Transfer Summary or equivalent to the medical provider at the receiving facility and shall advise them of any medical interventions provided to the detainee in transit.

f. The facility mental health program shall include appropriate group counseling, individual talk therapy, peer-support groups, and psychiatric services to meet the needs of the population. The facility will provide adequate spacing for group counseling and other behavioral health groups. The Contractor shall furnish mental health evaluations as determined by the Facility Local Health Authority and in accordance with the current applicable ICE detention standards, ACA standards, and any other accreditation standards, which refers to formal certification by authorized organizations confirming compliance with established health care service standards. The FMC and Behavioral Health Case Manager (BHCM) will review policies as a part of the annual site visit to ensure the policies align with the detention standards and IHSC's expectations for optimal patient care and services.

g. The Contractor is required to provide prescribed medications. The Contractor may acquire medications not included among the stock medications kept in the facility pharmacy through an IHSC network pharmacy. Prescribed medications include formulary medications per the current IHSC Formulary and approved nonformulary medications (e.g., IHSC Form 943 or equivalent). Formulary medications include approved vaccinations. All travel medications must be provided per ICE policies. ICE will only cover cost associated with medications provided by IHSC network pharmacies.

In accordance with detention standards, the Contractor may approve a list of nonprescription medications available to detainees outside of health services (e.g., sold

DRAFT

in commissary). IHSC does not reimburse for nonprescription medication services outside of health services. Facility Care Levels are based on the level of care required by ICE.

33.5. Certified/ Licensed Health Care Personnel

The Contractor shall ensure that all health care personnel employed under this agreement to provide care to ICE detainees shall be licensed and/or certified as required by the State in which the designated facility covered under this agreement resides. At no time shall unlicensed, uncertified and/or inactive status health care personnel provide care to ICE detainees. The Contractor shall ensure that all health care providers utilized for the care of ICE detainees are credentialed, to include: primary source verification, current licensure, certifications, and/or registrations within the State and/or City where they treat the detained population, and inquiry regarding sanctions or disciplinary actions (i.e., National Practitioner Data Bank).

33.6. Staffing Levels

The Contractor shall have a staffing plan to effectively staff the facility in a safe and secure manner. The number, type, and distribution of health care personnel as described in the approved staffing plan shall be maintained throughout the term of the agreement.

Written requests to change the number, type, or distribution of healthcare personnel must be submitted to the Contracting Officer (CO) and Contracting Officer's Representative (COR) for approval prior to implementation and incorporation into this agreement.

Staffing levels shall not fall below a monthly average of 85% for all health care position categories, including direct-care clinical health services personnel, and all other departments, calculated in the aggregate, as outlined in the approved staffing plan. The Contractor shall retain, at a minimum, health care staffing levels as approved by IHSC at the time of implementation.

33.7. Key Personnel (Medical)

The Contracting Officer (CO) shall provide written approval before any employee is assigned as key medical personnel to perform duties under this contract. The Contractor shall have key personnel employed and available for duty before the Contractor can begin contract performance. Any subsequent changes to key personnel shall meet these criteria and be approved in writing by the CO. The following are considered key personnel for the contract (position descriptions below): Health Services Administrator; Clinical Director; Nurse Manager, Behavioral Health Supervisor/Lead, Behavioral Health Providers, Psychiatrist, Psychiatric Nurse Practitioner/PA, and Behavioral Health Program Manager. The Contractor may use other titles. The Contractor shall provide a contract manager who shall be responsible for the performance of the work. The name of this person and an alternate who shall act for the Contractor when the contract manager is absent shall be designated in writing to the CO. The contract manager or alternate shall have full authority to act for the Contractor on all contract matters relating to the daily operation

DRAFT

of this contract. The contract manager or alternate shall be available 24/7/365.

Health Services Administrator. The Health Services Administrator (HSA) shall have a minimum of an accredited bachelor's degree in a health-related field of study (master's degree preferred). The HSA shall have three years of leadership experience, and two years management of programs and services experience. The HSA shall maintain the Basic Life Support (BLS) for Healthcare Providers certification through the American Heart Association and if the HSA holds a clinical license, it is their responsibility to fulfill the obligations of their licensing or certifying body to ensure continued status. This is an onsite fulltime position.

Clinical Director. The Clinical Director shall have a Doctor of Medicine or Doctor of Osteopathic Medicine from a university in the United States or from a foreign medical school that provides education and medical knowledge equivalent to accredited schools in the United States or any of its territories as established by the National Committee on Foreign Medical Education and Accreditation and permanent certification by the Educational Commission for Foreign Medical Graduates. The Clinical Director shall have a minimum of six years' post residency experience providing direct patient care as a board-certified/eligible physician in Family Medicine, Internal Medicine, Emergency Medicine, or Preventive Health as well as a minimum of three years' experience in the provision of clinical supervision and leadership to other medical professionals and ancillary clinic staff. The Clinical Director shall maintain the current, full, and unrestricted licensure to practice medicine for the entirety of the employment term in the state in which the duty station is located. The Clinical Director shall also maintain the Basic Life Support (BLS) for Healthcare Providers certification through the American Heart Association. This is an onsite fulltime position.

Nurse Manager. The Nurse Manager shall be, at minimum, a bachelor's degree trained registered nurse (RN) and have current and documented professional licensure to be an RN. The Nurse Manager shall have a minimum of six years of professional nursing experience and shall also maintain the Basic Life Support (BLS) for Healthcare Providers certification through the American Heart Association as well as any professional credentials/certification appropriate to the job specialty. This is an onsite fulltime position.

Behavioral Health Supervisor, Behavioral Health Program Manager, & Mental Health Providers. Mental Health Providers shall only consist of Psychiatrists, Psychiatric Advanced Practice Providers, Clinical/Counseling Psychologist, Licensed Clinical Social Workers (LCSWs), or Licensed Professional Clinical Counselors/Licensed Clinical Professional Counselors/Licensed Clinical Mental Health Counselors (LPC/LPCC/LCPC/LMHC/LCMHC) or equivalent. Clinical license shall be independent and unrestricted. Licensed Marriage and Family Therapists (LMFTs) are not acceptable for CDFs without detained families. Staff shall maintain appropriate licensure to conduct mental health evaluation, mental health and substance abuse treatment (i.e. psychotherapy – individual or group; clinical counseling, etc.), mental health diagnosis, segregation monitoring,

DRAFT

serious mental illness (SMI), monitoring, and assessing suicidality/homicidality risk, and suicide watch contacts. Mental Health Providers are onsite positions and must adhere to staffing requirements.

The following key personnel shall not provide direct patient care at, or on behalf of, non-IHSC facilities or their personnel:

Field Medical Coordinators (FMC) Role & Core Functions

Field Medical Coordinators (FMCs) are U.S. Public Health Service officers within ICE ERO field offices who serve as healthcare compliance officers and liaisons between ICE/IHSC and the non-IHSC health care staff at non-IHSC detention facilities that house ICE detainees.

1) Provides oversight and consultation regarding health care compliance and delivery of health care in accordance with ICE medical standards. Collaborates with other IHSC entities as needed;
2) Assists ICE and IHSC with the coordination of services and transfer of detainees as needed or warranted for continuity of care;
3) Performs case monitoring of hospitalized detainees and those with significant chronic health care needs based on daily updates, documents, and/or reports provided electronically by the vendor, or upon request as needed;
4) Gathers information and documents from the vendor for medical reviews, follow-up reports and investigations;
5) Conducts site visits annually, situationally/ad hoc, as needed at non-IHSC staffed detention facilities which house detainees in ICE custody to ensure compliance with ICE standards regarding health care;
6) Collaborates with other appropriate health officials to ensure continuity of care for detainees with significant health conditions upon release/removal; and
7) Oversees the adjudication process of requested medical services referrals entered into the Medical Payment Authorization Request (MedPAR) system.

Referral Coordinators (RC) Role & Core Functions

Referral Coordinators (RCs) are Contractors assigned to non-IHSC facilities who administratively process electronic medical referrals for off-site community specialty health services, in accordance with IHSC policies, protocols, and guidance.

1) Performing recordkeeping functions aligned with IHSC policy;
2) Tracking of appropriate follow up and completion of scheduled appointments;
3) Executing and completing reports to ensure referrals are transmitted to the TPA (third party administrator) correctly;
4) Serving as the liaison between IHSC, the requesting facility provider, and off-site community providers;
5) Scheduling of off-site community specialty consults and follow-up appointments;
6) Handling correspondence requiring authorization for payment of medical services;
7) Prepare, update, and maintain medical referral information and ensure

DRAFT

accuracy of the information in the patient medical record;

8) Provides timely notices or reminders prior to each scheduled appointment where applicable and requests completed off-site community medical records for routing to appropriate clinical staff for review;
9) Assists with billing and claims resolution, including denied claims, as needed for off-site community providers;
10) Supports the off-site community provider enrollment process by initiating recruitment efforts and maintaining a reference of vendorized off-site community providers for appointment scheduling;
11) Contacts the off-site community provider to schedule appointment for specialty care based on IHSC provider referral and coordinates transport for off-site community medical appointments as needed; and
12) Coordinate receipt of needed durable medical equipment for patients in custody.

Behavioral Health Case Manager (BHCM) Role & Core Functions

Behavioral Health Case Managers (BHCMs) are U.S. Public Health Service officers within ICE ERO field offices who serve as behavioral health compliance officers and liaisons between ICE ERO and IHSC, as well as the non-IHSC health care staff at non-IHSC detention facilities that house ICE detainees.

1) Provides oversight and consultation regarding behavioral health care compliance and delivery of behavioral health care in accordance with ICE behavioral health standards. Collaborates with other IHSC entities as needed (i.e., Field Medical Coordinators);
2) Assists ICE and IHSC with the coordination of services and transfer of detainees as needed or warranted for continuity of care;
3) Performs case monitoring of hospitalized detainees and those with significant chronic behavioral health care needs based on daily updates, documents, and/or reports provided electronically by the vendor, or upon request as needed;
4) Gathers information and documents from the vendor for behavioral health reviews, follow-up reports and investigations;
5) Conducts site visits annually, situationally/ad hoc, as needed at non-IHSC staffed detention facilities which house detainees in ICE custody to ensure compliance with ICE standards regarding behavioral health care;
6) Collaborates with other appropriate health officials to ensure continuity of care for detainees with significant behavioral health conditions upon release/removal; and
7) Oversees the adjudication process of requested medical services referrals entered into the Medical Payment Authorization (MedPAR) system.

33.8. Medical Care Expenses and Reimbursement

All costs associated with the medical care provided by the vendor must be included in the pricing for this contract. On-site radiology imaging, routine labs and Clinical Laboratory Improvement Amendments (CLIA) waived testing will be a requirement of

DRAFT

the Contractor. Off-site labs must be approved through the Medical Payment Authorization Request (MedPAR)referral or waiver processes established by IHSC and the off-site lab provider will be reimbursed through IHSC's claim processing third-party administrator (TPA). All routine medical supplies will be provided by the Contractor and must be included in the pricing for this contract. The following are not included in the pricing: off-site specialty care, offsite emergent care, hospitalizations, approved formulary and non-formulary network pharmacy purchases of medications and patient specific durable medical equipment (DME). All non-IHSC formulary medications are approved for purchase via retail network pharmacies. All non-formulary medications require approval by IHSC medical authority or designee. High value medications which cost above $5,000 require approval by the CO, in consultation with the IHSC medical authority or designee. Retail purchases are only allowed by authorized health staff as designated through the position description submitted by the Contractor. DME identified as clinically necessary by a medical provider and approved by an IHSC Regional Clinical Director (RCD) or designee, will be made available through the MedPAR referral system or purchase card process with the assistance of the IHSC FMC, or designee as needed.

33.9. Standards of Medical Care

Evidence-based Standards of Medical Care
The Contractor is responsible for providing resources for evidence-based standards of medical care which can be used as a guide for treatment of most diagnosed health care concerns. The Contractor must follow the IHSC Tuberculosis Clinical Practice Guidelines for the evaluation and treatment of suspected or confirmed tuberculosis patients. All other conditions, the Contractor shall establish and make available to the government the provider's proposed evidence-based standards of medical/mental health care within 90 calendar days from the contract award. See examples of resources below:

IHSC Sample Clinical Practice Guidelines (To Be Provided Upon Request):
a. HIV
b. Asthma
c. Hepatitis C
d. Hypertension
e. Sickle Cell Disease

33.10. Credentialing Requirements:

The Contractor must have a process in place to ensure that all health care providers utilized for the care of ICE detainees are credentialed, to include primary source verification, current licensure, certifications,, and/or registrations within the State and/or City where they treat the detained population, and up-to-date inquiry regarding sanctions or disciplinary actions from prior practices (i.e., National Practitioner Data Bank).

The Contractor will maintain written documentation confirming that everyone providing services under this contract has and maintains requisite credentials. Any change in status regarding any credentialing requirements must be reported in writing by the Contractor to ICE and the IHSC FMC within seven business days. The Contractor shall ensure the following medical personnel maintain valid, active,

DRAFT

permanent, full, independent, and unrestricted credentials in accordance with State law:

a. Licensed Independent Provider (LIP): An LIP is defined as an individual, as permitted by law and regulation, and by the organization, to provide care and services without direction or supervision within the scope of the individual's license and consistent with the privileges granted by the organization.

    1) Physicians: Medical Doctor (MD), Doctor of Osteopathy (DO);
    2) Dentists: Doctor of Dental Surgery (DDS), Doctor of Dental Medicine (DMD);
    3) Psychologists: Doctor of Psychology (PsyD or PhD) in Clinical or Counseling Psychology from a graduate program in Psychology accredited by the American Psychological Association:
        i. At least, two (2) years of supervised experience in Clinical, Counseling, or Health Psychology; and
        ii. Meet requirements for inclusion in the National Registry of Psychologist Providers if graduated after 1 January 1982.
    4) Social Workers: Licensed Clinical Social Worker (LCSW) requirements:
        i. Successful completion of a Master of Social Work (MSW) from a graduate program accredited by Council on Social Work Education (CSWE); and
        ii. The clinical social worker license must be the highest clinically independent licensed clinical social work designated by the licensing board where it was received; and
        iii. A minimum of three years post-independent licensure clinical experience providing independent clinical assessment, diagnosing using the DSM-V-TR (and any future DSM publications) and developing clinical treatment plans without supervision; and
        iv. Provide documentation/transcripts demonstrating clinical work within completed graduate program requested; and
        v. Must complete 20 hours of Continuing Education Units (CEUs) annually approved by the American Psychological Association (APA) or National Association of Social Workers (NASW); Additional CEU hours may be obtained by another sponsoring equivalent; and
        vi. Shall maintain membership with licensing board associated with clinical license and submit required completion of CEUs to the licensing board annually as required; Membership with the state or territory clinical licensing board is required.
    5) Licensed Clinical Professional Counselors (LCPC)/Licensed Clinical Mental Health Counselors (LCMHC)/Licensed Professional Mental Health Counselor requirements:
        i. Education: Hold a master's or doctoral degree in: Clinical Mental Health Counseling; Clinical Rehabilitation Counseling; Clinical Mental Health Counseling and Clinical Rehabilitation Counseling; or a related field, from a program accredited by the Council on Accreditation of Counseling and Related Educational Programs (CACREP). Examples of related mental health counseling fields include but are not limited to Addiction Counseling; Community Counseling; Gerontology Counseling; Marital, Couple, and Family

DRAFT

Counseling. CACREP defines the date when graduates are considered to have graduated from a CACREP accredited program. Additional information may be obtained from http://www.cacrep.org/directory/. NOTE: Traditional Rehabilitation counseling programs that are accredited by CACREP do not meet the LPMHC qualification standards as Traditional Rehabilitation counseling differs from Clinical Rehabilitation counseling; and

ii. Must hold a full, current, and unrestricted license to independently practice as a Licensed Professional Mental Health Counselor (or other acronym from above), which includes diagnosis and treatment; and

iii. A minimum of three years post-independent licensure clinical experience providing independent clinical assessment, diagnosing using the DSM-V-TR, and developing clinical treatment plans without supervision.

6) Mental Health Providers can only be Clinical Psychologist, Licensed Clinical Social Workers (LCSWs), or Licensed Professional Clinical Counselors/Licensed Clinical Professional Counselors/Licensed Clinical Mental Health Counselors, etc. (LPC/LPCC/LCPC/LMHC/LCMHC); No Licensed Marriage and Family Therapists (LMFTs) unless explicitly designated by ICE as a family residential center (FRC). Exceptions can be made for LMFTs in a non-FRC ICE detention facility on a case-by-case basis.

Appropriate licensure ensures ability to conduct mental health evaluation, provide clinically appropriate mental health and substance abuse treatment (i.e. psychotherapy – individual or group; clinical counseling, etc.), mental health diagnosis, segregation monitoring, SMI designations ‘and monitoring, and assessing suicidality/homicidality risk, suicide watch contacts, etc.

b. Licensed Supervised Provider (LSP): An LSP is defined as an individual, as permitted by law and regulation, and by the organization, to provide care and services under a Collaborative Practice and Prescriptive Authority Agreement (CP/PAA).

1) Physician Assistants (PA-C);
2) Nurse Practitioners: Adult Nurse Practitioner (ANP), Advanced Practice Registered Nurse (APRN), Certified Nurse Practitioner (CNP); and
3) Clinical Pharmacist.

c. Licensed Dependent Provider (LDP): All licensed or certified healthcare providers that do not fall under the category of LIP or LSP are considered LDPs.

1) Registered Nurse (RN);
2) Dental Hygienists (DH);
3) Licensed Vocational Nurses (LVN) or Licensed Practical Nurses (LPN);
4) Certified Nursing Assistants (CNA); and
5) Certified Medication Aid (CMA).

DRAFT

33.11. Basic Life Support (BLS) Certification, Medical Emergency Response, and Suicide Prevention

The Contractor shall ensure that all facility personnel, to include medical personnel, administrative staff, and custody officers, complete all training and drills related to fire, man down, mass disaster, emergency evacuation, life safety, and suicide prevention. These activities must be conducted in accordance with applicable ICE standards and, if required, relevant accreditation standards (e.g., ACA). The Contractor should consider the Train-the-Trainer concept for cost savings.

All medical personnel shall achieve and maintain BLS certification through American Heart Association (AHA) approved vendors.

1) All personnel shall complete, at minimum, initial (4 hrs.) and annual (4 hrs.) training on the following:
    a. Response to health-related emergencies within 4-minutes;
    b. Cardiopulmonary resuscitation (CPR);
    c. Automated external defibrillator (AED) use;
    d. Emergency first aid;
    e. Signs of potential health emergencies and required response;
    f. Methods of obtaining emergency medical assistance;
    g. Signs and symptoms of mental illness and suicide risk;
    h. Plan and procedures for providing emergency medical care including, when required, the safe and secure transfer of detainees for appropriate hospital or other medical services;
    i. All other emergency response requirements as outlined in the applicable ICE standard, to include accreditation standards (e.g. ACA), if required;
    j. Any training that occurs more frequently than initial and annual must be adhered to as outlined in the applicable ICE standard, to include accreditation standards (e.g. ACA), if required;
    k. Administer medications; and
    l. Know the universal precautions for protection against blood-borne diseases.

– AND –

2) Complete 8hrs of Suicide Prevention and Intervention training annually, to include:
    a. Training on emergency use of cutdown tools, which should be provided upon hire and 2hrs of this training annually; and
    b. Training on Nonviolent Crisis Intervention through the Crisis Prevention Institute (CPI), https://www.crisisprevention.com/ (or a similar nonviolent crisis intervention modality) and trauma-informed care practice.

33.12. Off-site Medical Care and Reimbursement

IHSC reimburses community providers for health care services of a detainee in ICE custody via IHSC's TPA , who issues payment on behalf of ICE according to U.S. Code Title 18, Part III Chapter 301, section US Code 4006: Subsistence for prisoners. Authorized payments for health care services are reimbursed and shall not exceed Medicare reimbursement rates (reimbursement of services is only authorized for dates

DRAFT

of service wherein detainees are in ICE custody).

The Contractor shall not charge any ICE detainee a fee or co-payment for medical services or treatment provided at the off-site facility.

The Health Authority of the Contractor shall notify ICE and the FMC as soon as possible if emergency off site care was or will be required; and in no case more than 72 hours after the detainee received such care.

The Contractor is responsible for access to hospital and specialty medical care/services for detainees in ICE custody. The Contractor initiates and completes letters of recruitment as outlined by IHSC with potential community hospitals and providers for provision of medically necessary health services and enrollment in IHSC's provider network. The Contractor routes all completed letters of recruitment through the FMC. IHSC is responsible for completion of recruitment and enrollment processes.

The Contractor is responsible for timely entry of all MedPAR/referral requests for provision of community health services for detainees, into the IHSC MedPAR version 2 System (MPv2S) by designated and trained MPv2S end-users. The IHSC MPv2S is a web-based system in which authorized users submit requests for reimbursable health care services to IHSC for authorization.

Any removal of a community provider from the IHSC provider network will be communicated by the FMC via email to the Contractor and related stakeholders. Upon notification of removal, the Contractor is not authorized to refer a detainee in ICE custody for medical services to the removed community provider, nor is the removed community provider authorized to render services to detainees in ICE custody.

Additionally, Contractor requirements are as follows:

a. Provide and maintain a comprehensive, current list of hospitals and community providers that includes the outlined data:
    1) Provider Name
    2) Physical Address (for transport)
    3) Specialty type
    4) Contact information as applicable (person of contact's first & last name, phone, email, fax and mailing address) related to:
        i. making appointments
        ii. medical record requests
        iii. billing/claims communications
    5) Billing NPI#; tax ID/Employer Identification Number (EIN)

b. The Contractor shall ensure any staff who need access to the IHSC MPv2S to electronically enter MedPARs/referrals follow the process outlined in the IHSC MPv2s User Guide https://medpar.ice.gov and adhere to the following MPv2s requirements:
    1) To be completed upon designation as a MPv2S end user and annually thereafter
        i. Watch the MPv2s user guide training video, located on the MPv2s homepage.
        ii. Read the MPv2s User guide located inside MPv2s;

DRAFT

iii. Read the MedPAR guidance Reference Guide for Non-IHSC IGSA Detainees

2) All MPv2s end-users are required to read and utilize (as applicable) the IHSC Provider Information packet (located inside of MPv2s) to assist providers with claim issues and send the IHSC Provider Information packet to the community provider.

c. Provide the FMC with a point of contact who is assigned by the Contractor, primarily responsible for managing community MedPAR/referrals within the IHSC MPv2S and who primarily is responsible for the following:

1) Sends completed recruitment letters to the FMC for potential enrollment in the IHSC provider network.
2) Serves as the services provider's subject matter expert, customer service point of contact for internal/external stakeholders, and trainer related to use of the IHSC MPv2S, IHSCs MedPAR/referral process (should be a day-to-day end user), the provider recruitment process, and the IHSC Provider Information packet (located within the MPv2s).
3) Ensures all detainees who receive offsite medical services has a completed corresponding MedPAR/referral r/t that care as outlined in the MPv2S User Guide https://medpar.ice.gov and adhere to MPv2S end user requirements.
4) Completes timely adjudication of MedPARs/referrals (cancellation, making appointments, sending authorizations, etc.).
5) Ensures MedPAR/referral entries related to emergency department or hospital admissions must be entered into the MPv2S within one business day after the detainee is discharged.
6) Serves as the primary POC that collaborates with the FMC to resolve alien number discrepancies between the MPv2S and Enforce system.
7) Responsible for arranging custody transport for detainee authorized MedPAR/referrals community provider appointments.
8) Responsible for sending authorizations of MedPARs/referrals to community providers or their billing partners.
9) Responsible for providing and maintaining a current comprehensive list of hospitals and community providers with data points as specified and provide a copy to the FMC initially and when updates are made.
10) Serves as the primary contact for FMCs, other IHSC staff, community providers, and other applicable stakeholders related to adjudication of MedPARs/referrals, medical record requests, billing and medical claims adjudication.
11) Responsible for responding to medical referral/billing/claims, or authorization communications received for timely resolution (mail, emails, or phone calls) and collaborating with the FMC as applicable.
12) Responds and assists community providers with complaints related to denied claims by gathering the following information to review with the FMC within three business days.
    i. Provider Name
    ii. Provider phone number
    iii. Provider email address
    iv. Point of contact first/last name
    v. TAX ID# or EIN
    vi. Billing NPI#
    vii. Illegal Alien First Name

DRAFT

viii. Illegal Alien Last Name
ix. Alien ID#
x. Date of Birth
xi. Date(s) of Service
xii. MedPAR Specialty: (ER, In-Pt etc.)
xiii. Denial code from Explanation of Benefit (EOB).
xiv. IHSC issued authorization number if applicable

33.13. Prescription Drug Reimbursement

IHSC only provides prescription drug reimbursement to network pharmacies via a pharmacy benefits manager (PBM) (TPA) for detainees in ICE custody. A network pharmacy is a pharmacy that accepts the PBM copayment.

The IHSC FMC maintains a list of participating network pharmacies which can be accessed through the COR. The PBM creates and provides IHSC the list of participating network pharmacies. The PBM pays for all the medication's cost from a network pharmacy. The IHSC FMC coordinates IHSC regional chief pharmacists to identify and create an identifier (group ID) for submitting claims through the PBM by the network pharmacy for the Contractor using a pharmacy benefit letter. IHSC regional chief pharmacist submits the Contractor's information and specific identifier to the PBM to register the Contractor. The IHSC regional chief pharmacists provide the pharmacy benefits letter to the IHSC FMC. IHSC FMCs share the list of network pharmacies and pharmacy benefit letter with the Contractor. Below is the process for filling prescriptions for ICE detainees at network pharmacies:

a. The Contractor delivers the prescription to the network pharmacy with the Contractor's specific pharmacy benefits letter.
b. The network pharmacy shall run the prescription through the PBM's prescription processing system. After a paid claim is received, the network pharmacy dispenses formulary prescriptions.
c. Non-formulary prescriptions require prior authorization. The Contractor faxes the Drug Prior Authorization Request Form to PBM. The PBM sends the request to IHSC for approval or denial. IHSC approves or denies the request and transmits the final decision to the PBM. If the nonformulary is approved, the network pharmacy receives notification, resubmits a claim, and the network pharmacy dispenses the medication. If not approved, the PBM notifies the network pharmacy and does not approve a claim.

The Contractor must ensure adequate supply of medication(s) for release, transfer, or removal of a detainee in accordance with detention standards or additional medication supply requirements (e.g., court mandate minimum supply, ICE mission requirements). ICE, through the IHSC FMC, may request additional supply of medication(s) to support continuity of care. The Contractor shall be given advance notice by ICE/ERO prior to the release, transfer, or removal of a detainee, so that medical staff may determine and provide for any medical needs associated with the transfer, release, or removal.

In the event ICE/ERO is transferring a detainee to a less than 72-hour facility for ultimate release or removal, the Contractor shall fill the prescription(s) at a network

DRAFT

pharmacy and ensure an adequate supply of medication(s) for both transfer and release is provided to the detainee.

33.14. Serious Medical Conditions

The Contractor must notify ICE (through the COR) and the IHSC FMC of detainees with serious medical conditions immediately upon identification of conditions and no more than 24 hours of identification of the case. Examples of cases include but are not limited to: uncontrolled hypertension; uncontrolled diabetes; unstable respiratory disease or any detainee requiring oxygen treatment; history of congestive heart failure complaining of shortness of breath; pregnancy; multiple unstable chronic conditions; liver failure; renal failure; infectious and communicable diseases (i.e., HIV/AIDS, viral hepatitis, varicella, measles, mumps, COVID-19); and infectious disease outbreaks.

33.15. Notification Requirements for Medical Conditions that Render Continued Detention Unacceptable

If the Contractor determines that an ICE detainee has a medical condition which renders that person unacceptable for detention under this agreement (for example, condition needing life support, uncontrollable violence, or serious mental health condition), the Contractor shall notify their FMC, Behavioral Health Case Manager (BHCM) and ICE. Upon such notification, the Contractor shall allow ICE reasonable time to make the proper arrangements for further disposition of the detainee. The Contractor should expect to be requested and attest to ICE that the detainee is medically cleared for transportation and advise ICE of the necessary precautions and equipment required for such transportation. IHSC FMC, BHCM, and/or Medical Case Management Program Coordinators (MCMPC) consultation regarding these matters is available at any time.

33.16. Serious Mental Disorders or Conditions/Serious Mental Illness (SMI)

The Contractor shall identify, track, record and maintain a list of all detainees identified as having a serious mental disorder or condition and/or who are determined to be incompetent by an immigration judge until removal or release. The Contractor shall complete the IHSC Form 883 and submit it to IHSC FMC/Behavioral Health Case Manager (BHCM) when the detainee has been identified. Notification to the FMC and the COR shall occur as soon as practicable but no later than 72 hours after identification of detained individuals with a serious mental disorder or condition. In addition, a list shall be provided to the COR and IHSC FMC on a weekly basis and include name, A#, date of arrival, diagnosis (es), presence or absence of suicidality, specific symptoms exhibited by detainee that meets criteria of a Serious Mental Disorder or Condition, list of prescribed psychotropic medication with dosage, date when IHSC Form 883 was completed and submitted to IHSC FMC, and details for Safe Release Planning pursuant to ICE Directive 11063.2: Identification, Communication, Recordkeeping, and Safe Release Planning for Detained Individuals with Serious Mental Disorders or Conditions and/or Who Are Determined To Be Incompetent By An Immigration Judge.

A serious mental disorder or condition/SMI is characterized by a qualified mental health provider or physician after:

DRAFT

a. Determining that an individual in custody:

1) Has a mental disorder that is causing serious limitations in communication, memory, or general mental and/or intellectual functioning (e.g., communicating, conducting activities of daily living, social skills), or a severe medical condition(s) (e.g., traumatic brain injury or dementia) that is significantly- impairing mental function; or

2) Is exhibiting one or more of the following active psychiatric symptoms and/or behavior: severe disorganization, active hallucinations or delusions, mania, catatonia, severe depressive symptoms, suicidal ideation and/or behavior, and/or marked anxiety or impulsivity;

– OR –

b. Otherwise diagnosing a detained individual as demonstrating significant symptoms of one or more of the following:

1) Psychosis or Psychotic Disorder;
2) Bipolar Disorder;
3) Schizophrenia or schizoaffective disorder;
4) Major Depressive Disorder with Psychotic Features;
5) Dementia and/or a Neurocognitive Disorder; and/or
6) Intellectual Development Disorder (moderate, severe, or profound).

33.17. Serious Mental Illness (SMI) Training

The Contractor shall provide semi-annual SMI training to clinic staff, in accordance with current ICE policies and procedures in coordination with IHSC, and communicated through the COR.

33.18. Emergency Medical Services

In the event of a medical emergency, the Contractor shall ensure immediate response and provide necessary emergency medical treatment, including initial on-site stabilization and off-site transport to an appropriate emergent care facility, as needed. The Contractor shall notify ICE as soon as practical regarding the nature of the transferred detainee's illness or injury and the type of treatment provided. All emergency medical services provided off-site require an authorized MedPAR/referral to be entered within the MPv2S within one business day upon return from the hospital. IHSC reimburses community providers for health care services of a detainee in ICE custody via a third-party claim processor, who issues payment on behalf of ICE according to U.S. Code Title 18, Part III Chapter 301, section US Code 4006 that specifies reimbursement is not to exceed Medicare rates. At no time shall the Contractor or detainee incur financial liability related to such services. The primary point of contact for obtaining pre-approval for non-emergent care as well as the post-approval for emergent care will be the IHSC FMC assigned to the location.

ICE is committed to ensuring emergency response services including ambulance and fire support do not overwhelm locally available resources. Therefore,

DRAFT

the Contractor shall provide direct, ready access to licensed ambulance services capable of advanced life support (ALS) and basic life support (BLS). Ambulances must be available for transport to local hospitals or medical facilities as needed 24/7. EMS personnel must be licensed and maintain current certifications in CPR, first aid, and relevant EMS protocols. The Contractor shall ensure all EMS equipment and supplies are maintained, inspected, and available for immediate use. Ambulances must be equipped in accordance with applicable federal standards. The Contractor shall establish effective relationships with local community providers.

The Contractor shall ensure comprehensive fire suppression and emergency response services are available 24/7. Services shall include, but are not limited to:

- Deployment of trained and certified personnel capable of responding to fire emergencies, hazardous material incidents, and related emergencies.
- Operation and maintenance of fire suppression equipment, including fire trucks, extinguishers, sprinkler systems, and other necessary apparatus.
- Implementation of rapid response protocols to ensure timely arrival and effective mitigation of fire and emergency incidents.
- Conducting regular fire safety inspections, drills, and training for facility staff.
- Coordination with local emergency services and authorities as required.
- Documentation and reporting of all incidents, responses, and maintenance activities in accordance with applicable regulations and standards.

The Contractor shall provide monthly reports to the COR on emergency response, response times, and incidents.

33.19. Emergency Health Care Contact List

The Contractor shall furnish a 24 hours/seven days per week emergency medical/dental/mental health care contact list which must include local hospitals and other off-site specialty care providers to the COR. The Contractor shall ensure detainees always have access to an off-site emergency medical provider.

33.20. Facility Emergency Evacuation Procedure Guide

The Contractor must maintain a facility emergency evacuation procedure guide that includes evacuation of any patients currently housed in a medical/mental health housing area, including any isolation rooms as well as other special housing areas within the facility. The Contractor must provide training on all emergency plans to the on-site medical staff, both initially and annually after hire.

33.21. Hospitalization of Detainees

Upon order of the COR or designated ICE officer, or in an emergency, the Contractor shall take custody of and safeguard detainee(s) at a hospital or clinic when the detainee(s) is undergoing medical examination. The Contractor employee will remain on duty until relieved by another Contractor employee. 24-hour custody shall be maintained, with constant visual observation when practicable. The detainees shall not use the telephones unless the Contractor receives prior approval from the COR or other designated ICE official. The Contractor employees shall not fraternize with clinic/hospital staff or with casual visitors to the clinic/hospital. The Contractor is

DRAFT

obligated to relay messages as requested by the detainee to the COR or other designated ICE official.

Visitation for detained aliens is not permitted at the hospital. To prevent any situation which could result in a breach of security, requests for visitation while the alien is in detention, including hospital detention, shall be pre-approved by the COR(s) or other designated ICE officials prior to allowing access to the alien.

34. Manage a Detainee Death

The contractor shall comply with NDS 2026, Standard 4.6 Terminal Illness and Death, in the event of a detainee injury or death. In the event of a detainee death, the Contractor shall immediately notify the FMC and COR or ICE designated official and submit a written report within 24 hours. The Contractor shall fingerprint the deceased. Staff members performing the fingerprinting shall date and sign the fingerprint card to ensure that a positive identification has been made and file the card in the detainee's file. Personal property of the deceased shall be inventoried, and release is to be coordinated with ICE to the designated family member, the nearest of kin, or the Consular Officer of the detainee's country of legal residence.

If death is due to violence, accident surrounded by unusual or questionable circumstances or is sudden and the deceased has not been under immediate medical supervision, the Contractor shall notify the coroner of the local jurisdiction to request a review of the case, and if necessary, examination of the body.

The Contractor shall establish, and report to the COR, coroner notification procedures outlining such issues as performance of an autopsy, who will perform the autopsy, obtaining state-approved death certificates, and local transportation of the body.

The Contractor, in coordination with the COR or Designated Service Official, shall ensure the body is turned over to the designated family member, the nearest of kin, or the Consular Officer of the detainee's country of legal residence.

When an autopsy is requested, the Contractor shall communicate the request to the FMC. The Contractor must obtain an invoice from the autopsy provider and, if applicable, provide a complete recruitment letter and submit it to the FMC.

The Contractor shall release all information relevant to the detainee death investigation to ICE (e.g., medical information, incident reports, eyewitness accounts, video footage) upon request.

35. Facility Requirements for Infectious Disease Prevention, Management, and Screening

The Contractor will adhere to all infectious disease prevention and management guidelines, treatment, and reporting as required by local, state, and federal public health authorities. The Contractor should follow infectious disease and standard precautions as well as isolation, cohorting, and quarantine recommendations as outlined in the most current guidance set forth by the IHSC Public Health, Safety, and Preparedness Unit.

DRAFT

In order to prevent the spread of airborne infectious disease or cross contamination of zones within the facility, the HVAC system in the intake screening area shall be designed to exhaust to the exterior and prevent air exchange between the intake screening area and any other area within the facility (see CDC guidelines http://www.cdc.gov/tb/publications/guidelines/Correctional.htm). Airborne Isolation Infection (AII) rooms (e.g., negative pressure rooms) must be inspected annually by a certified technician, or per manufacturer recommendations, to ensure proper functionality and quality control.

The Contractor will ensure that there is adequate space and equipment to provide medical intake screening including tuberculosis (TB) screening within the intake processing area.

a. Tuberculosis Screening:
The Contractor will perform onsite TB screening as part of the routine intake screening, which must be completed within 12 hours of detainee admission. TB screening will include, at a minimum, both TB symptom screening and testing for TB infection and/or disease using any Center for Disease Control and Prevention (CDC) approved method or chest x-ray. Detainees who have symptoms suggestive of TB disease will be immediately placed in an airborne infection isolation room and promptly evaluated for suspected TB disease. Detainees who are initially tested using a test for TB infection [TB skin test (TST) or interferon gamma release assay (IGRA)], and the results are positive according to criteria, but have no symptoms suggestive of TB disease, must be evaluated with a chest radiograph within 5 days of the notification of a positive result.

Detainees who are identified with confirmed or suspected active TB (e.g., symptoms or chest radiograph suggestive of TB) will be placed in a functional airborne infection isolation room and managed in accordance with the applicable standard and all applicable CDC guidelines:
http://www.cdc.gov/tb/publications/guidelines/default.htm. If there is no clinical or radiographic evidence suggestive of TB disease the detainee can be housed with the general population. Only a trained and qualified health care provider can perform chest radiography if the site has this capability, and only a credentialed radiologist can interpret these radiographs. The facility will have an alternative non-punitive process in place for detainees who refuse the TB screening assessment.

The Contractor will notify IHSC and the local health department of all detainees with confirmed or suspected TB disease, including detainees with clinical or radiographic evidence suggestive of TB. Notification shall occur within one working day of identifying a detainee with confirmed or suspected TB disease. Notification to local health departments shall identify the detainee as being in ICE custody and shall include the ICE detainee number and other identifying information. For detainees with confirmed or suspected TB disease, the Contractor will coordinate with IHSC and the local health department to facilitate release planning and referrals for continuity of care prior to release.

The Contractor will evaluate detainees annually for symptoms consistent with TB within one year of the previously documented TB evaluation. For detainees initially screened with a TST or IGRA with a negative result, annual evaluation will include

DRAFT

testing with the same method as previously used. For detainees initially evaluated with a chest radiograph interpreted as not suggestive of TB disease, routine annual chest radiograph is not recommended.

i. Radiology Services:

a. When the Contractor conducts initial TB screening using any CDC-recommended method, including onsite radiology services (e.g., mobile radiology), the cost shall be included in the bed rate. If the Contractor utilizes offsite radiology services for TB screening confirmation, the Contractor must follow IHSC's third-party claim process (MEDPAR entry or waiver) to obtain reimbursement.

b. When the Contractor opts to purchase x-ray equipment (and all other associated costs) to utilize chest radiology for the purpose of TB screening, the Contractor will be financially responsible for purchasing the equipment, associated equipment servicing costs, as well as any federal or state mandated radiology certification costs, to include dosimetry. Additionally, the Contractor is financially responsible for all associated radiology staffing service costs, and diagnostic interpretation costs.

36. Environmental Health

The Contractor shall implement all general housekeeping and environmental cleaning and disinfection requirements consistent with the Environmental Health and Safety sections of the applicable standard in all areas where medical, dental, mental health, and intake medical screening services are rendered, including routine and terminal cleaning of medical housing and medical isolation units based on 24/7/365 needs.

37. Medical Quality Assurance (QA) Program

The Contractor shall implement an internal review and medical quality assurance program for the purpose of maintaining operations in accordance with the applicable ICE detention standards, ACA standards, and any other accreditation standards , which refers to formal certification by authorized organizations confirming compliance with established health care service standards.

The Contractor shall conduct a quality improvement / quality of care review consistent with an established quality improvement (medical quality management) program and interfacing with the IHSC quality improvement program (available upon request) consistent with federal, state, and local laws.

The minimum data inputs for trending, analysis, planning, executing, and assessing the effectiveness of QA- and quality improvement (QI)-related activities and corrective actions will derive from data collected by means of formal incident reports and IHSC encourages facilities to collect additional data unique to the facility and its environment for use in their QA program.

The Contractor shall provide a continuous quality improvement plan/ medical quality assurance plan and annually to the FMC for review. The clinical operations will be audited by IHSC annually, at minimum. This audit will be conducted by a designated IHSC healthcare professional(s). The facility will be assessed by their quality assurance program and compliance to the applicable standard by IHSC utilizing

DRAFT

medical review tools.

The Contractor ensures quality health care delivery and accountability in compliance with detention standards through a continuous quality improvement (CQI) system that includes risk management, patient safety, and health services delivery quality assurance programs. The CQI system will identify, address, and monitor health care delivery for undesired outcomes and trends, including but not limited to those due to near miss occurrences, adverse events, sentinel events, and systemic processes or outcomes. Concerns identified from the CQI system risk assessment will be addressed through corrective action plans.

The Contractor is required to report all incidents, according to IHSC incident reporting criteria, to the FMC immediately. Detainee deaths while housed at the facility are subject to an IHSC directed mortality review, concurrent or subsequent root cause analysis for the purpose of identifying actual, and potential process failures and errors. The IHSC incident reporting criteria is available upon request.

In addition, the CQI program shall include:

a. Participation in a multidisciplinary QI committee;
b. Collection, trending analysis, and evaluation of data, along with planning, interventions, and reassessments;
c. Analysis of the need for ongoing education and training;
d. On-site monitoring of health service outcomes on a regular basis through:
    1) Chart reviews (including investigation of complaints and quality of health);
    2) Review of practices for prescribing and administering medication;
    3) Investigation of complaints and grievances;
    4) Monitoring of corrective action plans;
    5) Reviewing all deaths, suicide attempts and illness outbreaks;
    6) Developing and implementing QI activities or corrective actions plans to address and resolve identified problems and concerns;
    7) Reevaluating problems or concerns to determine whether QI activities or corrective actions implemented achieved and sustained desired results;
    8) Incorporating findings of internal review activities into the organization's educational and training activities;
    9) Ensuring records of internal review activities comply with legal requirements on confidentiality of records; and an
    10) External peer review on an annual basis for all independently licensed medical professionals.

38. Immediate Jeopardy

Immediate Jeopardy is a situation in which the provider's or supplier's non-compliance with one or more requirements, conditions of participation, conditions for coverage, or conditions for certification has caused, or is likely to cause, serious injury, harm, impairment, or death to a resident or patient (Code of Federal Regulation 489.3). For purposes of this agreement, "resident or patient" includes all illegal aliens housed at and in the custody of the facility. The Contractor shall adhere to IHSC's Immediate Jeopardy guidelines and cooperate fully with any investigations conducted pursuant to these guidelines. The Contractor shall promptly identify, report, and address any such situations in accordance with IHSC protocols and directives.

DRAFT

A. IHSC Monitoring and Determination of Immediate Jeopardy

1) **IHSC monitoring role**
   IHSC staff (including the Regional Field Medical Coordinator (RFMC), Regional Program Manager (RPM), Field Medical Coordinator (FMC), Behavioral Health Case Managers (BHCM), and other IHSC personnel) are responsible for monitoring non-IHSC facilities for conditions that may constitute- Immediate Jeopardy to illegal aliens.

2) **Information sources**
   IHSC may identify potential Immediate Jeopardy through, including but not limited to:
   a. Site visits (scheduled or ad hoc); Review of medical, mental health, and detention records;
   b. ICE ERO reports or findings;
   c. Self-report from Contractors or facility staff;
   d. RFMC/FMC remote review or other oversight activities.

3) **IHSC criteria for Immediate Jeopardy**
   In assessing whether Immediate Jeopardy exists, IHSC will consider the current or potential presence of:
   a. Harm;
   b. Immediacy;
   c. Culpability.

   IHSC may consider questions such as:
   - Was harm caused?
   - Is there a likelihood for potential harm?
   - Does the situation need to be immediately addressed?
   - What is the likelihood of the situation reoccurring?
   - Did the facility create a situation or allow a situation to continue which resulted in serious harm, injury, impairment, or death of an illegal alien?
   - Was the facility aware of the situation? If yes, when did they first become aware?
   - Is the situation related to neglect, indifference, or disregard for illegal alien care, comfort, or safety?
   - Did the facility have the opportunity to implement corrective actions or preventive measures? If yes, when?

4) **IHSC decision process (summary)**
   a. Upon identification of potential Immediate Jeopardy, the FMC will contact the RFMC and RPM, collect necessary information, and collaborate with the RFMC to develop recommendations for immediate and short/long-term corrective actions (e.g., population caps, transfers, focused site visits, staffing changes, process changes, ongoing monitoring).
   b. IHSC will communicate findings and recommendations to ICE ERO, the Contracting Officer's Representative (COR), and other IHSC leadership as outlined in IHSC policy.
   c. The FMC will issue a Uniform Corrective Action Plan (UCAP) or similar document once approved by the RPM.
   d. Resolution of Immediate Jeopardy is determined by the RFMC based on investigation and verification that corrective actions appropriately address and resolve Immediate Jeopardy factors.

DRAFT

B. Contractor/Facility Obligations When IHSC Identifies Immediate Jeopardy

When IHSC identifies or reasonably suspects Immediate Jeopardy at a non-IHSC facility, the following obligations apply to the Contractor:

1) **Access, Information, and Cooperation**

The Contractor shall:

i. **Provide access**

a. Provide IHSC and ICE ERO/COR personnel prompt access to the facility, relevant housing units, illegal aliens, staff, and records needed to evaluate and address Immediate Jeopardy.

ii. **Provide information and documents**

a. Furnish, upon IHSC request and within the timeframes specified by IHSC/ICE ERO, all documents and data relevant to the situation, including medical and mental health records, detention logs, incident reports, staffing rosters, policies, and procedures.

iii. **Preserve evidence**

a. Preserve relevant records and information (including, to the extent available, video footage, electronic data, and logs) related to the Immediate Jeopardy situation, and refrain from altering or destroying such records except as directed by the Government.

iv. **Facilitate site activities**

a. Facilitate IHSC/ICE ERO ad hoc site visits, focused reviews, interviews, and monitoring activities related to the Immediate Jeopardy finding.

2) **Immediate Protective and Operational Measures**

Upon receiving notice from IHSC/ICE ERO that Immediate Jeopardy has been identified or is suspected, the Contractor shall, as directed by IHSC/ICE ERO:

i. **Implement immediate protective measures**

a. Take specified actions to protect affected illegal aliens (for example, moving illegal aliens to safer housing, providing immediate medical or mental health evaluation and treatment, or increasing observation/rounding), as directed by IHSC/ICE ERO.

ii. **Modify or cease unsafe practices**

a. Immediately implement any operational changes ordered by IHSC/ICE ERO that are intended to halt or mitigate the unsafe practice or condition, which may include, but not limited to:

1. Suspending specified procedures or activities;
2. Restricting use of particular areas, equipment, or processes;
3. Adjusting staffing patterns or reassigning staff.

iii. **Support transfers and population management**

Cooperate with any IHSC/ICE ERO decisions regarding population caps, temporary stops to new admissions, or transfers of illegal aliens to other facilities when these actions are part of the Immediate Jeopardy response.

DRAFT

3) **Corrective Action Plan (UCAP) Implementation**
   i. **Acceptance and implementation**
      a. Implement the Uniform Corrective Action Plan (UCAP) or other corrective action document issued by IHSC (through the FMC/RFMC/RPM), including all interim and long-term corrective measures specified therein.
   ii. **Designation of responsible staff**
      a. Designate facility staff responsible for carrying out each corrective action item and for coordinating with IHSC/ICE ERO regarding progress and obstacles.
   iii. **Status reporting**
      a. Provide IHSC/ICE ERO with updates, documentation, and data demonstrating implementation of corrective actions in the format and frequency specified by IHSC/ICE ERO (which may include routine written updates and participation in follow-up calls or meetings).

4) **Acknowledgment of IHSC Authority and Resolution**
   a. The Contractor acknowledges that IHSC (through the RFMC) determines whether Immediate Jeopardy exists and when it has been resolved, based on investigation and verification of corrective actions.
   b. The Contractor shall not unilaterally declare Immediate Jeopardy resolved or resume any restricted practices or operations that IHSC/ICE ERO has suspended or modified, unless and until IHSC/ICE ERO provides written authorization.

5) **Documentation and Recordkeeping**
   a. The Contractor shall maintain complete documentation of all actions taken in response to an Immediate Jeopardy determination or directive, including:
      i. Communications with IHSC/ICE ERO;
      ii. Interim safety measures;
      iii. Corrective actions;
      iv. Monitoring/quality-assurance results.
   b. The Contractor shall provide copies of such documentation to IHSC/ICE ERO upon request and in the manner directed by IHSC/ICE ERO, for storage in the Government's designated systems.

39. Detainee Reporting Requirements

The Contractor shall participate and respond in a timely manner or in accordance with any applicable ICE directives or policies to the reporting requirements requested by ICE and/or IHSC. The following is a list of routine reporting requirements. Routinely the FMC will request any of the following as needed or other reporting as may come up.

a. HIV
b. Hunger Strike
c. Pregnancy
d. Serious Mental Illness (SMI)/Significant Detainee Illness (SDI)
e. Suicide Watches (SW)
f. Hospital Clinical/Administrative Updates
g. Incident Reports
h. Chronic Care List

DRAFT

i. Sick Call Log
j. Medical Grievance Logs
k. Cohorting/Infectious Disease Surveillance
l. Durable Medical Equipment (DME)
m. Emergency Room Transfers
n. Miscellaneous/Ad Hoc

40. Health Records Requests and Physical Access

The Contractor shall allow IHSC and ICE personnel access to its facility, electronic health record system (if applicable) and ICE detainees' medical records (hard copies, electronically and virtually) for healthcare review, complaint investigations, and liaison activities with the local contract Health Authority and associated Contractor departments. The Contractor shall provide ICE detainee medical records to ICE whether created by the Contractor or a sub-Contractor upon request from the FMC and/or Contracting Officer's Representative or Contracting Officer in accordance with HIPAA privacy exception at 45 CFR §§ 164.512 (k)(5)(i). This privacy exception allows disclosure without consent to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual if the correctional institution or such law enforcement official represents that such protected health information is necessary for:

a. The provision of health care to such individuals;
b. The health and safety of such individual or other detainees
c. The health and safety of the officers or employees of or others at the correctional institution;
d. The health and safety of such individuals and officers or other persons responsible for the transporting of detainees or their transfer from one institution, facility, or setting to another;
e. Law enforcement on the premises of the correctional institution; and
f. The administration and maintenance of the safety, security, and good order of the correctional institution.

The Contractor shall respond within seven business days to ICE and/or IHSC requests for reporting, documentation, and other data required to respond to pending and current litigation, congressional inquiries, other federal, state, or local entity requests for information. The Contractor shall release all medical information for ICE detainees to IHSC representatives upon request. In addition, the Contractor shall respond and collaborate with stakeholders (IHSC, Custody Programs, CRCL, etc.) in completion of success action plans (SAP), formerly referred to as corrective action plans (CAP) to address potential and confirmed deficient practices identified through inspections, site audits and/or complaint investigations.

41. Detainee Medical Records

A separate medical record, apart from the resident's social record/or alien file, is to be maintained by the authorized Contractor. Medical records will be created and maintained by the responsible authorized Contractor and/or the ICE contracted vendor. The Contractor and/or the ICE contracted vendor will disclose patient's personal information and protected health information to Facility/IHSC staff and comply with medical record requests from IHSC, as permitted by a criminal justice release of

DRAFT

information, signed by the patient and in compliance with state and federal laws, rules, and regulation including, but not limited to, federal regulations Health Insurance Portability and Accountability Act (HIPAA) and Confidentiality of Substance Use Disorder Patient Records (42 CFR, Part 2). OTP accreditation is a federal requirement established by the Substance Abuse and Mental Health Services Administration (SAMHSA) to ensure that programs providing opioid agonist treatment meet rigorous standards for patient care, safety, and medication management. OTP understands an exemption from HIPAA applies for patients in the custody of ICE and the information contained in the 01/26/2021 IHSC memo "Release of Medical Information Regarding ICE Detainees" has been reviewed.

These documents will be maintained and stored per the following:

a. ICE Health Service Corps uses the following retention requirement to maintain detainee health records for 10 years after release from custody for adults; the records for minors will be maintained until the minor reaches the age of 27 years. Records will be maintained in a format that is easily accessed, and, in a location, that is secure, pest and vermin free environment, protected from fire, flood, humidity, dust, mildew, mold, and preferably climate controlled.

b. Upon his/her request, while in detention, a detainee or his/her designated representative shall receive information from their medical records. Copies of health records shall be released by the HSA directly to a detainee or their designee, at no cost to the detainee, within a reasonable timeframe after receipt by the HSA of a written authorization from the detainee. Medical records and/or a book-in packet must accompany the arriving detainee, unless ICE/ERO and facility officials have authorized other arrangements "Detainee Transfers" also requires that a Medical Transfer Summary accompany the detainee. If official health records accompany the detainee, they are to be placed in a sealed envelope or other container labeled with the detainee's name and A-number and marked "Confidential Medical Records." A copy of a detainee's medical records shall be transferred with the detainee upon request of the detainee. Otherwise, a medical transfer summary shall accompany each detainee outlining necessary care during transit and initial period of detention entry into another facility, including current medications, medical precautions, tuberculosis testing and evaluation status, equipment needed, and appropriately authorized methods of travel. It is preferred that the Contractor seek to provide an Office of the National Coordinator (ONC) certified electronic health record for recording all detainee encounters. If a paper record is used, the record format must adhere to the ACA and/or other National Health Record format.

42. Electronic Health Record (EHR) Requirement Interoperability:

External Interfaces –

The Contractor will be responsible for utilizing an EHR system certified under the Office of the National Coordinator for Health Information Technology's (ONC) Health IT (HIT) Certification Program. The Contractor will be responsible for establishing connectivity to a DHS interface and transmitting medical record information in a format that conforms to ONCHIT interoperability standards.

External interfaces will be integrated with the EHR systems as part of agreements

DRAFT

between the Contractor and external medical support organizations. The Contractor will maintain the agreements with these organizations separately. The Contractor, in conjunction with their external medical support organization, is responsible for maintaining the interfaces to the EHR.

Direct Accessibility:
IHSC will also require access to individual detainee medical records or required queries or reports upon request.

Medical record is defined as a record of the patient's medical information to include, but not limited to: medical history, care or treatments received, progress notes, diagnostic test results, diagnoses and medications taken. The Contractor shall provide access to their EHR system through remote login. The Contractor shall provide access accounts for IHSC personnel (as requested; contact information for these IHSC personnel will be provided to the Contractor by the COR). The Contractor will also provide a primary and secondary point of contact for EHR data requests.

Applicable Policies and Standards:
The Contractor's EHR shall support:

- HL7 Version 3 CCD, and
- American Society for Testing and Materials (ASTM) International CCR Standard E2369-05

The Contractor's EHR system shall comply with the latest version of all technology standards and architecture policies, processes, and procedures and Federal mandates applicable to the IHSC IT health care environment, including those defined in ICE OCIO Architecture Division publications. These publications include, but are not limited to, the following:

- DHS 4300A Sensitive Systems Handbook
- DHS 4300A Sensitive Systems Policy Directive
- DHS 4300B National Security Systems Handbook
- DHS Management Directive (MD) 4300, IT Systems Security Publication
- DHS MD 4010.2 (DRAFT), Section 508 Program Management Office & Electronic and Information Technology Accessibility
- ICE Technical Reference Model
- ICE Architecture Test and Evaluation Plan
- ICE Enterprise Systems Assurance Plan
- ICE System Lifecycle Management (SLM) Handbook
- ICE Web Standards and Guidelines
- National Institute of Standards and Technology (NIST) Computer Security Resources Center (CSRC) standards, guidelines, and special publications
- Privacy Act of 1974
- Section 508 1194.2, Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220)

HIPAA Compliance-
The Contractor shall adhere to the provisions of Public Law 104-191, Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 111-5, Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009, and the National Standards to Protect the Privacy and Security of Protected Health

DRAFT

Information (PHI). As required by HIPAA, the Department of Health and Human Services (HHS) has promulgated rules governing the security and use and disclosure of protected health information by covered entities. Additionally, HITECH strengthens HIPAA requirements, especially regarding electronic records and breach notifications. The Contractor shall utilize HIPAA and HITECH compliant systems with web viewing capability tools, encrypted data transmission, and cloud storage. The systems shall provide quality assurance solutions with community radiologist level review. The Contractor shall certify they are and will maintain HIPAA compliance.

All EHR solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the Contractor shall comply with the following Homeland Security Enterprise and ICE Architecture requirements:

- Description information for all EHR data assets, information exchanges, and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.
- In compliance with Office of Management (OMB) mandate, all EHR network hardware shall be IPv6 compatible without modification, upgrade, or replacement.
- All EHR encryption shall be FIPS 197 Advanced Encryption Standard (AES) that has been FIPS 140-2 certified.

FedRAMP Compliance –

Data Storage and Integration: The Contractor must certify they will only utilize a GSA FedRAMP certified environment.

FedRAMP certification must be maintained continuously throughout the life of the contract. If the Contractor (or its FedRAMP provider) loses its FedRAMP certification, the Contractor must report this information to the Government immediately in writing. The Contractor must, within thirty (30) days after losing FedRAMP certification, re-certify or contract with an authorized FedRAMP provider. Failure to comply will result in termination of the contract.

The EHR data shall be stored solely in a GSA FedRAMP compliant environment (see http://cloud.cio.gov/fedramp/cloud-systems). Non-compliant FedRAMP systems shall result in a Factor 1 rating of "unacceptable". The Contractor shall provide certificate or evidence of compliant FedRamp system.

The Contractor shall support Certification and Accreditation (C&A) efforts to ensure Federal Information Security Management Act (FISMA) compliance to ICE.

Section 508 Compliance-
Accessibility Requirements (Section 508):

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public

DRAFT

who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable EIT accessibility standards have been identified:

Section 508 Applicable EIT Accessibility Standards:

- 36 CFR 1194.21 Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to government off-the-shelf (GOTS) and commercial off-the-shelf (COTS) software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.
- 36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous JavaScript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.
- 36 CFR 1194.26 Desktop and Portable Computers, applies to all desktop and portable computers, including but not limited to laptops and personal data assistants (PDA) that are procured or developed under this work statement.
- 36 CFR 1194.31 Functional Performance Criteria applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.
- 36 CFR 1194.41 Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required 1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offers telephone support, such as, but not limited to, a help desk, shall have the ability to transmit and receive messages using TTY.

Section 508 Applicable Exceptions:

Exceptions for this statement of work have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the Contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those Contractors assigned to fulfill the obligations of this work statement and for the

DRAFT

purposes of this requirement, are not considered members of the public.

Section 508 Compliance Requirements:

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency's business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

43. NEW O&M Task

Task Order: Ongoing Maintenance and Facility Operations for ICE Detention Facility

1. Scope
   The Contractor shall provide caretaker operations and maintenance (O&M), including preventive and corrective maintenance, facility operations, post-closing services, and compliance with safety, environmental, medical, and security requirements for the ICE detention facility, in accordance with ICE National Detention Standards (NDS).

2. Preventive Maintenance
   2.1 Plan Development
   Develop and submit a comprehensive Preventive Maintenance (PM) Plan for all facility assets (HVAC, plumbing, electrical, fire protection, structural components, kitchen/laundry equipment, elevators if applicable, building envelope, grounds, medical equipment, and security systems including doors, locking mechanisms, cameras, entry/exit, and movement tracking systems) within 30 days of contract award.
   Update the PM Plan annually or as required.

   2.2 Asset Inventory
   Establish and maintain a complete inventory of all assets requiring preventive maintenance.

   2.3 Scheduling
   Develop a preventive maintenance schedule specifying frequency (daily, weekly, monthly, quarterly, semi-annual, annual) and tasks for each asset.

   Schedule maintenance to minimize disruption to facility operations.

   2.4 Task Execution

DRAFT

Perform preventive maintenance tasks per the approved schedule and documented procedures, including inspection, cleaning, lubrication, adjustment, calibration, testing, replacement of consumables, functional testing of safety devices, and exercising emergency systems.

2.5 Documentation
Maintain records of all preventive maintenance activities in a computerized maintenance management system (CMMS) or equivalent.
Retain records for at least five years and make available upon request.

2.6 Reporting
Submit monthly and annual preventive maintenance summary reports, including completed tasks, outstanding items, and recommendations.

Immediately report critical deficiencies or system failures to facility management.

3. Corrective Maintenance

3.1 Response and Repairs
Respond to service calls and repair requests within specified response times.
Diagnose and repair building systems, equipment, and infrastructure.
Document all corrective actions and repairs.

3.2 Emergency Response
Provide 24/7 on-call emergency maintenance services.
Respond to facility emergencies (power outages, plumbing failures, security breaches) within one hour of notification and restore critical systems ASAP.

4. Facility Operations
4.1 Building Systems
Monitor and operate building automation and control systems.
Manage utilities (water, electricity, gas, steam, compressed air).
Ensure continuous operation of critical systems (HVAC, power, security).

4.2 Grounds and Exterior Maintenance
Mow lawns, trim landscaping, maintain exterior appearance, and remove debris.
Remove snow and ice from walkways, roads, and parking areas as required.
Inspect and maintain exterior lighting and signage.

4.3 Custodial Services
Maintain office, warehouse, and clinical areas in clean, dust-free condition.
Ensure trash and recycling are collected as directed by the Government.

4.4 Facility Accessibility
Maintain ADA-compliant access routes, signage, and equipment (including accessible restrooms, ramps, lifts) in accordance with applicable standards.

5. Medical Areas and Equipment Maintenance
5.1 Medical Equipment

DRAFT

Provide preventive and corrective maintenance for all medical and dental equipment and clinical spaces in accordance with manufacturer recommendations, ICE NDS, and applicable healthcare regulations.
Maintenance activities shall include inspection, calibration, cleaning, repair, and documentation of all medical equipment (including but not limited to exam tables, diagnostic devices, emergency medical equipment, dental equipment, and refrigeration units for medications).

5.2 Clinical Area Maintenance
Ensure clinical areas are maintained in accordance with infection control standards, including regular cleaning and repair, and participate in facility-wide emergency drills, including medical emergencies.
All maintenance records for medical equipment and clinical spaces shall be retained for at least five years and made available to facility management and auditors upon request.

6. Fire Protection and Life Safety
   Inspect, test, and maintain fire alarms, sprinklers, extinguishers, and suppression systems per NFPA and AHJ schedule.
   Conduct regular fire drills and system checks.
   Maintain and test backup power systems for medical and life safety equipment.
   Document all activities in accordance with regulatory and accreditation requirements.

7. Environmental, Health, and Safety
   7.1 Compliance
   Comply with all federal, state, and local regulations (EPA, OSHA, ACA, NDS, NFPA).
   Maintain Safety Data Sheets (SDS) and ensure proper storage and handling of hazardous materials.
   Conduct regular safety inspections and drills.

   7.2 Infection Control and Biohazard Management
   Handle, store, and dispose of medical and biohazardous waste in accordance with CDC, OSHA, and ICE NDS standards.
   Provide training for staff in infection control and biohazard handling.

   7.3 Environmental Protection
   Monitor compliance with environmental protection requirements.
   Document non-compliance in daily reports; report serious or imminent danger immediately.

   - Waste & Recycling Management
     Collect, segregate, and dispose of solid, hazardous, and medical waste per regulations.
     Maintain documentation of waste disposal and recycling activities.
   - IT and Communications Infrastructure
     Maintain and repair IT, communications, and data systems (including

DRAFT

computers, phones, network cabling, Wi-Fi, intercoms), especially those used for security and medical recordkeeping.

- Protection of Government Property
  Protect all government property from damage with due diligence.
- Debris Removal
  Daily cleanup and removal of all debris generated by contract performance from secure areas.
- Temporary Security Measures

8. Installation
   Install temporary fencing, bollards, security cameras, and monitoring systems around designated perimeter areas as identified by the Government.

   Submit installation plan and schedule for approval prior to commencement.

   Ensure fencing height, materials, gates, and signage comply with Government requirements and do not damage infrastructure or landscaping.

9. Removal and Restoration
   Upon completion, remove all temporary security measures and restore affected areas to original condition within 48 hours.

- Post-Closing Services
  Replace all existing exterior locking cylinders on pedestrian doors with new, compatible cylinders meeting UL 437 and ANSI/BHMA A156.5 standards.
  Determine adequacy of site security lighting and report deficiencies with recommendations.

- Performance Standards
  All work shall comply with applicable codes, standards, and regulations.
  Maintain facility structure and envelope (no leaks, breaches, or pest intrusion).
  Maintain HVAC, electrical, plumbing, fire protection, medical, IT, and security systems per PM plan and regulatory requirements.
  Submit caretaker inspection and maintenance reports monthly.
- Pest Control
  Conduct regular pest control inspections and treatments, especially in food service, medical, and residential areas, in accordance with ICE NDS and local health codes.
- Quality Assurance & Control
  Implement a quality control plan to monitor and evaluate service delivery.
  Conduct regular inspections and audits; address deficiencies promptly.
- Personnel Requirements
  All personnel must pass background checks and clearances.
  Maintain sufficient qualified staff, including licensed trades as required.

DRAFT

Provide ongoing training and certification in safety, security, infection control, medical equipment maintenance, emergency response, and technical skills.

- Reporting & Communication
  Designate a single point of contact (Project Manager) for contract administration.
  Attend regular coordination meetings with facility management.
  Provide timely updates on maintenance activities and issues.

- Capital Improvement Identification and Planning

  9.1 Identification and Assessment
  The Contractor shall regularly assess all facility systems, infrastructure, and assets to identify areas requiring significant cost investment for repair, replacement, or upgrade.
  Assessments shall include, but are not limited to, structural components, mechanical systems, electrical systems, security and life safety systems, medical equipment and clinical areas, IT infrastructure, and other critical facility assets.

10. Reporting
    The Contractor shall submit a Capital Improvement Report to the Government on a quarterly basis, or as requested, detailing:

    - Identified deficiencies or areas requiring major investment
    - Estimated costs for repair or upgrade
    - Impact on facility operations and mission
    - Recommended priority and timeline for remediation

11. Review and Approval
    The Government will review submitted Capital Improvement Reports and determine which projects will proceed.
    The Contractor shall provide additional information or clarification as requested by the Government during the review process.

12. Implementation Planning
    Upon Government approval, the Contractor shall develop a detailed Implementation Plan for each approved project, including:

    - Scope of work
    - Schedule and milestones
    - Resource requirements

DRAFT

- Risk assessment and mitigation strategies
- Coordination with facility operations to minimize disruption

13. Execution and Documentation
Execute approved projects in accordance with the Implementation Plan and applicable codes and standards.
Maintain documentation of all activities, expenditures, and outcomes, and submit progress reports as required by the Government.

44. General Cyber Security Contract Requirements

1. **In accordance with ITAR 4.5.3.1 – Compliance with DHS Security Policy Terms and Conditions.**
   i. Compliance with DHS Security Policy Terms and Conditions:
   ii. All hardware, software, and services provided under this task order must be compliant with *DHS 4300A DHS Sensitive System Program 4300A version 13.3 Feb. 13, 2023, and attachments*.
2. **In accordance with ITAR 4.5.3.4 and ITAR 4.5.4.4 – Security Review**

   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.
3. **Supply Chain Risk Management Terms and Conditions--ITAR 4.5.3.7**

   The Contractors supplying the Government hardware and software shall provide the manufacturer's name, address, state and/or domain of registration, and the Data Universal Numbering System (DUNS) number for all components comprising the hardware and software. If subcontractors or subcomponents are used, the name, address, state, and/or domain of registration and DUNs number of those suppliers must also be provided.

   Subcontractors are subject to the same general requirements and standards as prime contractors. Contractors employing subcontractors shall perform due

DRAFT

diligence to ensure that these standards are met.

The Government shall be notified when a new contractor/subcontractor/contractor is introduced to the supply chain, or when suppliers of parts or subcomponents are changed. Contractors shall provide, implement, and maintain a Supply Chain Risk Management Plan that addresses internal and external practices and controls employed to minimize the risk posed by counterfeits and vulnerabilities in systems, components, and software.

The Plan shall describe the processes and procedures that will be followed to ensure appropriate supply chain protection of information system resources developed, processed, or used under this contract.

The Supply Chain Risk Management Plan shall address the following elements:

i. How risks from the supply chain will be identified;

ii. What processes and security measures will be adopted to manage these risks to the system or system components; and

iii. How the risks and associated security measures will be updated and monitored.

The Supply Chain Risk Management Plan shall remain current through the life of the contract or period of performance. The Supply Chain Risk Management Plan shall be provided to the Contracting Officer Representative (COR/CO) 30 days post award.

The Contractor acknowledges the Government's requirement to assess the Contractors Supply Chain Risk posture. The Contractor understands and agrees that the Government retains the right to cancel or terminate the contract, if the Government determines that continuing the contract presents a risk to national security.

The Contractor shall disclose, and the Government will consider, relevant industry standard certifications, recognitions and awards, and acknowledgments.

The Contractor shall provide only new equipment unless otherwise expressly approved, in writing, by the CO. Contractors shall provide only Original Equipment Manufacturer (OEM) parts to the Government. If a shipped OEM part fails, all replacement parts must be OEM parts.

The Contractor shall be excused from using new OEM (i.e. "grey market, "previously used) components only with formal Government approval. Such components shall be procured from their original source and have them shipped only from manufacturers authorized shipment points.

For software products, the contractor shall provide all OEM software updates to correct defects for the life of the product (i.e., until the “end of life"). Software updates and patches must be made available to the government for all products

DRAFT

procured under this contract.

Contractors shall employ formal and accountable transit, storage, and delivery procedures (i.e., the possession of the component is always documented from initial shipping point to destination, and every transfer of the component from one custodian to another is fully documented and accountable) for all shipments to fulfill contract obligations with the Government.

All records pertaining to the transit, storage, and delivery will be maintained and available for inspection for the lessor of the term of the contract, the period of performance, or one calendar year from the date the activity occurred.

These records must be readily available for inspection by any agent designated by the U.S. Government as having the authority to examine them.

This transit process shall minimize the number of times en route components undergo a change of custody and make use of tamper-proof or tamper-evident packaging for all shipments. The supplier, at the Government's request, shall be able to provide shipping status at any time during transit.

The Contractor is fully liable for all damage, deterioration, or losses incurred during shipping and handling, unless the damage, deterioration, or loss is due to the Government. The Contractor shall provide a packing slip which shall accompany each container or package with the information identifying the contract number, the order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact. The contractor shall send a shipping notification to the intended government recipient or contracting officer. This shipping notification shall be sent electronically and will state the contract number, the order number, a description of the hardware/software being ship (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

4. **In accordance with HSAR Class Deviation 15-01, REV 1, SAFEGUARDING OF CONTROLLED UNCLASSIFIED INFORMATION (JULY 2023) and ALTERNATE 1 (JULY 2023)**

***Alternate I of 3052.204-72 SAFEGUARDING OF CONTROLLED UNCLASSIFIED INFORMATION (JULY 2023)**

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.

DRAFT

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 Federal 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

DRAFT

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 federal 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

DRAFT

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

DRAFT

unauthorized access, use, disclosure, disruption, modification, or destruction 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

DRAFT

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) Federal 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);

DRAFT

(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

DRAFT

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 because 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

DRAFT

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

DRAFT

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 2023 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)

Authority to Operate - Compliance

The contractor shall obtain full authority to operate (ATO) in accordance with DHS Policy Directive 4300A, current revision and in *accordance with 3052.204-72 Safeguarding of Controlled Unclassified Information* of this document. If unable to meet the requirements, the contractor shall provide, within thirty (30) days of award, a Cybersecurity Compliance Plan (CCP) to obtain ATO within six (6) months of the contract effective date, which includes incremental delivery of deliverables and supporting artifacts, as requested. The CCP shall include a completed Authorization Readiness Report to provide overview of the system's cybersecurity posture and current readiness of each deliverable. The contractor shall notify the Contracting Officer (CO) immediately, or as soon as reasonably possible, should the contractor encounter any delay that would necessitate the need to revise the compliance plan. Cybersecurity deliverables and the Authorization Readiness Report are provided in Attachment: "Cybersecurity Deliverables Sensitive Information Systems_HIGH_MOD 05.08.24."

(End of clause)

3052.204-73 **NOTIFICATION** AND 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.

(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) *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

DRAFT

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 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:

DRAFT

(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)

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

DRAFT

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 federal 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

DRAFT

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,

DRAFT

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.

(End of clause)

ALTERNATE I (JULY 2023)

(g) Before receiving access to information resources under this contract, the individual must complete a security briefing; additional training for specific categories of CUI, if identified in the contract; and any nondisclosure agreement furnished by DHS. The Contracting Officer's Representative (COR) will arrange the security briefing and any additional training required for specific categories of CUI.

(h) The Contractor shall have access only to those areas of DHS information resources explicitly stated in this contract or approved by the COR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information resources not expressly authorized by the terms and conditions in this contract, or as approved in writing by the COR, are strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions about the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for DHS. It is not a right, a guarantee of access, a condition of the contract, or government-furnished equipment (GFE).

DRAFT

(j) Contractor access will be terminated for unauthorized use. The Contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management, or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. For a waiver to be granted:

(1) There must be a compelling reason for using this individual as opposed to a U.S. citizen; and

(2) The waiver must be in the best interest of the Government.

(3) 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.

(End of clause)

45. DHS FAR Class Deviation 17-03 – Revision 1
52.224-3 Privacy Training – Alternate I (DEVIATION)

(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.

DRAFT

(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.

46. Cloud Services Contract Requirements

ALTERNATE I (JULY 2023)

1. **In accordance with ITAR 4.5.3.2** – Encryption Compliance
   Encryption Compliance Terms and Conditions
   If encryption is required, the following methods are acceptable for encrypting sensitive information:

   a) FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2.

   b) National Security Agency (NSA) Type 2 or Type 1 encryption.

   c) Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the *Department of Homeland Security (DHS) IT Security Program Handbook (DHS Management Directive (MD) 4300A) for Sensitive Systems*).

2. **In accordance with ITAR 4.5.3.5 and ITAR 4.5.4.5 – Interconnection Security Agreement (ISA)**
   ISA Terms and Conditions

   Interconnections between DHS/ICE and non-DHS/ICE IT systems shall be established only through controlled interfaces and via approved contractors. The controlled interfaces shall be authorized at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements; memoranda of understanding, service level agreements or interconnection security agreements.

3. **In accordance with ITAR 4.5.3.6 and ITAR 4.5.4.6 – Required Protections for DHS/ICE Systems Hosted in Non-DHS/ICE Data Centers**

DRAFT

a) Security Authorization Terms and Conditions

A Security Authorization of any infrastructure directly in support of DHS/ICE information system shall be performed as a general support system (GSS) prior to DHS/ICE occupancy to characterize the network, identify threats, identify vulnerabilities, analyze existing and planned security controls, determine likelihood of threat, analyze impact, determine risk, recommend controls, perform remediation on identified deficiencies, and document the results. The Security Authorization (SA) shall be performed in accordance with DHS/ICE Security Policy and the controls provided by the hosting provider shall be equal to or stronger than the FIPS 199 security categorization of DHS/ICE information system.

At the beginning of the contract, and upon request thereafter (generally at the deployment of a new system or renewal of a System Authority to Operate), the contractor/Cloud Contractor (CSP) shall provide the results of an independent assessment and verification of security controls. The independent assessment and verification shall apply the same standards that DHS/ICE applies in the SA process of its information systems. Any deficiencies noted during this assessment shall be provided to the COR for entry into DHS/ICE POA&M Management Process. ICE shall use DHS' POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies shall be corrected within the timeframes dictated by DHS/ICE POA&M Management Process. CSP procedures shall be subject to periodic, unannounced assessments by DHS/ICE officials. The documented physical aspects associated with CSP activities shall also be subject to such assessments. Inspections of CSP physical facilities will be scheduled in advance and coordinated with the provider in accordance with their federal facility procedures. On a periodic basis, DHS and its Components, including DHS Office of Inspector General, may choose to evaluate any or all the security controls implemented by the contractor under these clauses. Evaluation could include, but is not limited to vulnerability scanning. The DHS and its Components reserve the right to conduct audits at their discretion. With ten working days' notice, at the request of the Government, the CSP and reseller shall fully cooperate and facilitate in a Government-sponsored security control assessment at each location wherein DHS/ICE information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of DHS/ICE, including those initiated by the Office of the Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) determined by DHS/ICE in the event of a security incident.

b) Enterprise Security Architecture Terms and Conditions

The CSP shall utilize and adhere to DHS/ICE Enterprise Security Architecture in accordance with applicable laws and DHS/ICE policies to the satisfaction of DHS/ICE COR.

DRAFT

c) Continuous Monitoring Terms and Conditions

The CSP shall participate in the DHS/ICE Continuous Monitoring methodologies and, shall provide a Continuous Monitoring capability over their resources as required by FedRAMP. The DHS Chief Information Security Officer (CISO) issues annual updates to its Continuous Monitoring requirements via the Annual Information Security Performance Plan. At a minimum, the CSP shall adhere to all ITAR and FedRAMP continuous monitoring requirements and ensure that DHS/ICE can implement and integrate the following processes:

a. Asset Management

b. Vulnerability Management

c. Configuration Management

d. Malware Management

e. Log Integration

f. Patch Management

g. Providing near-real-time security status information to DHS/ICE SOC Specific Protections Terms and Conditions

h. Specific protections that shall be provided by the CSP include, but are not limited to the following:

Specific Operations Terms and Conditions

The Contractor shall operate a SOC to provide security for the below mentioned services. The CSP shall support regular reviews with DHS/ICE Information Security Office to coordinate and synchronize the security posture of the CSP hosting federal facility with that of DHS Data Centers. The SOC personnel shall provide 24x7x365 staff to monitor the network and all its devices. The CSP staff shall also analyze the information generated by the devices for security events, respond to real-time events, correlate security device events, and perform continuous monitoring. It is recommended that the CSP staff shall also maintain a trouble ticket system in which incidents and outages are recorded. In the event of an incident, the CSP federal facility SOC shall adhere to the incident response plan.

d) Computer Incident Response Services Terms and Conditions

The CSP shall provide Computer Incident Response Team (CIRT) services. The CSP shall adhere to the standard Incident Reporting process as determined by the Component and is defined by a DHS/ICE-specific incident response plan that adheres to DHS/ICE policy and procedure for reporting incidents. The CSP shall conduct Incident Response Exercises to ensure all personnel are familiar with the plan. The CSP

DRAFT

shall notify DHS/ICE SOC of any incident in accordance with the Incident Response Plan and work with DHS/ICE throughout the incident duration.

e) **Network Intrusion Detection Systems (NIDS) and Monitoring Terms and Conditions**
The Contractor shall provide the design, configuration, implementation, and maintenance of the sensors and hardware that are required to support the NIDS solution. The contractor is responsible for creating and maintaining the NIDS rule sets for their federal facility(s). The NIDS solution should provide real-time alerts. These alerts and other relevant information shall be in a central repository. The NIDS shall operate 24x7x365. A summary of alerts shall be made available to DHS/ICE upon request. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS/ICE point of contact in accordance with the incident response plan.

f) **Physical and Information Security and Monitoring Terms and Conditions**
The CSP shall provide a federal facility using appropriate protective measures to provide for physical security. All facilities will be located within the United States. The CSP shall maintain a process to control physical access to all DHS/ICE IT assets. DHS/ICE IT Assets shall be monitored 24x7x365. A summary of unauthorized access attempts shall be reported to the appropriate DHS/ICE security office upon request.

g) **Vulnerability Assessments Terms and Conditions**
The CSP and reseller shall provide all information from any managed device to DHS/ICE, as requested, and shall assist, as needed, to perform periodic vulnerability assessments of the network, operating systems, and applications to identify vulnerabilities and propose mitigations. Vulnerability assessments shall be included as part of compliance with the continuous monitoring of the system.

h) **Anti-malware (e.g., virus, spam) Terms and Conditions**
The CSP shall design, implement, monitor, and manage to provide comprehensive anti-malware service. The CSP shall provide all maintenance for the system providing the anti-malware capabilities to include configuration, definition updates, when changes are required. A summary of alerts shall be reported to DHS/ICE SOC in weekly status report. If an abnormality or anomaly is identified, the CSP shall notify the appropriate DHS/ICE point of contact in accordance with the incident response plan.

i) **Log Retention Terms and Conditions**
Log files for all infrastructure devices, physical access, and anti-malware should be retained online for 180 days and offline for three years.

4. **In accordance with ITAR 4.5.3.8 – Personal Identification Verification (PIV) Credential**

DRAFT

Compliance
Personal Identification Verification (PIV) Credential Compliance Terms and Conditions

a) Procurements for products, systems, services, hardware, or software involving controlled federal facility or information system shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.

b) Procurements for software products or software developments shall be compliant by accepting PIV credentials as the common means of authentication for access for federal employees and contractors.

c) PIV-enabled information systems must demonstrate that they can correctly work with PIV credentials by responding to the cryptographic challenge in the authentication protocol before granting access.

d) If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan for achieving HSPD-12 compliance shall be required for review, evaluation, and approval by the CISO.

5. In accordance with FedRAMP

Note: *The following requirements/clauses apply to both* ***CUI and CLASSIFIED REQUESTS****.*

1) FedRAMP IT Systems Security Requirements

a) The Federal agency will determine the security category for the cloud system in accordance with Federal Information Processing Standard 199; then, the contractor/Cloud Contractor (CSP) shall apply the appropriate set of impact baseline controls as required in the FedRAMP Cloud Computing Security Requirements Baseline document to ensure compliance to security standards. The FedRAMP baseline controls are based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5.1.1, Security and Privacy Controls for Federal Information Systems and Organizations (as amended) and includes a set of additional controls for use within systems providing cloud services to the federal government.

b) The CSP shall maintain a security management continuous monitoring environment that meets or exceeds the requirements outlined in the latest edition of FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements.

2) FedRAMP Privacy Requirements

Contractor shall be responsible for the following privacy and security safeguards:

a) To the extent required to carry out the FedRAMP assessment and authorization process and FedRAMP continuous monitoring, to safeguard against threats and hazards to the security, integrity, and

DRAFT

confidentiality of any non-public Government data collected and stored by the Contractor, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.

b) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

c) The contractor shall also comply with any additional FedRAMP privacy requirements.

d) The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. In accordance with the Federal Acquisitions Regulations (FAR) clause 52.239-1, contractor shall be responsible for the following privacy and security safeguards:

   i. The Contractor shall not publish or disclose in any manner, without the CO's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception—Disclosure to a Consumer Agency for purposes of C&A verification.

   ii. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours. The program of inspection shall include, but is not limited to: Authenticated and unauthenticated operating system/network vulnerability scans Authenticated and unauthenticated we b application vulnerability scans Authenticated and unauthenticated database application vulnerability scans Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools.

   iii. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

   iv. If the vendor chooses to run its own automated scans or audits,

DRAFT

results from these scans may, at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided, in full, to the Government.

DRAFT

3) **Sensitive Information Storage**

Sensitive But Unclassified (CUI) information, data, and/or equipment will only be disclosed to authorize personnel on a need-to-know basis. The contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following NIST SP 800-88, Guidelines for Media Sanitization.

The disposition of all data will be at the written direction of the COR, this may include documents returned to Government control; destroyed; or held as specified until otherwise directed. Items returned to the Government shall be hand carried or sent by certified mail to the COR.

4) **Protection of Information**

The contractor shall be responsible for properly protecting all information used, gathered, or developed because of work under this contract. The contractor shall also protect all Government data, equipment, etc. by treating the information as sensitive. All information about the systems gathered or created under this contract should be considered as CUI information. It is anticipated that this information will be gathered, created, and stored within the primary work location. If contractor personnel must remove any information from the primary work area they should protect it to the same extent they would their proprietary data and/or company trade secrets. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

The government will retain unrestricted rights to government data. The government retains ownership of any user created/loaded data and applications hosted on vendor's infrastructure, as well as maintains the right to request full copies of these at any time.

The data that is processed and stored by the various applications within the network infrastructure contains financial data as well as personally identifiable information (PII). This data and PII shall be protected against unauthorized access, disclosure or modification, theft, or destruction. The contractor shall ensure that the facilities that house the network infrastructure are physically secure.

The government-owned data must be available to the Government upon request within one business day or within the timeframe specified otherwise and shall not be used for any other purpose other than that specified herein. The contractor shall provide requested data at no additional cost to the government.

No data shall be released by the Contractor without the consent of the Government in writing.

All requests for release must be submitted in writing to the COR/CO.

DRAFT

5) **Security Classification**
The preparation of the deliverables in this contract will be completed at a Sensitive but Unclassified level unless a higher level is specified.

6) **Confidentiality and Nondisclosure**
The preliminary and final deliverables and all associated working papers and other material deemed relevant by the agency that have been generated by the contractor in the performance of this contract, are the property of the U.S. Government, and must be submitted to the COR at the conclusion of the contract. The U.S. Government has unlimited data rights to all deliverables and associated working papers and materials in accordance with FAR 52.227-All documents produced for this project are the property of the U.S. Government and cannot be reproduced or retained by the contractor. All appropriate project documentation will be given to the agency during and at the end of this contract. The contractor shall not release any information without the written consent of the CO.

Personnel working on any of the described tasks may, at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

a. Information made available to the Contractor by the Government shall be used only for carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

7) **FedRAMP Security Requirements Overview:**
   a) The minimum requirements for low and moderate impact cloud systems are contained within the FedRAMP Cloud Computing Security Requirements Baseline. The contractor and Federal Government Agency share responsibility to ensure compliance with security requirements.

   b) The implementation of a new Federal Government cloud system requires a formal process, known as Assessment and Authorization, which provides guidelines for performing the assessment.

DRAFT

c) FedRAMP requires cloud contractors to utilize a Third-Party Assessment Organization (3PAO) to perform an assessment of the cloud contractor's security controls to determine the extent to which security controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting security requirements.

d) The FedRAMP PMO security staff will be available for consultation during the process. Both the FedRAMP PMO staff and JAB will review the results before issuing a Provisional Authorization decision. The Government reserves the right to verify the infrastructure and security test results before issuing an Authorization decision.

e) Federal agencies will be able to leverage the provisional Authorization granted by FedRAMP and any documentation prepared by the contractor to issue their own authority to operate.

f) The vendor is advised to review the FedRAMP guidance documents (see References below) to determine the level of effort that will be necessary to complete the requirements. All FedRAMP documents and templates are available at http://FedRAMP.gov.

8) FedRAMP Security Compliance Requirements

The contractor shall implement the controls contained within the FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements for low and moderate impact system (as defined in FIPS 199). These documents define requirements for compliance to meet minimum Federal information security and privacy requirements for both low and moderate impact systems. While the FedRAMP baseline controls are based on NIST SP 800-53, Revision 4. The contractor shall generally, substantially, and in good faith follow FedRAMP guidelines and Security guidance. In situations where there are no procedural guides, the contractor shall use generally accepted industry best practices for IT security.

9) Required FedRAMP Policies and Regulations

The contractor shall comply with FedRAMP Security Assessment Framework – describing a general security Assessment Framework for the Federal Risk and Authorization Management Program (FedRAMP). This document details the security assessment process which must be used to achieve FedRAMP compliance. Download here:
https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Fra mework.pdf

10) Assessment and Authorization

DHS/ICE may choose to cancel the contract/award and terminate any outstanding orders if the contractor has its provisional authorization revoked and the deficiencies are greater than agency risk tolerance thresholds.

11) Assessment of the System

a) The contractor shall comply with FedRAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's NIST Federal Information Processing Standard (FIPS) Publication 199 categorization. The contractor shall create, maintain and update the following documentation using FedRAMP requirements and templates, which are available at http://FedRAMP.gov :

- Privacy Impact Assessment (PIA)
- FedRAMP Test Procedures and Results
- Security Assessment Report (SAR)
- System Security Plan (SSP)
- IT System Contingency Plan (CP)
- IT System Contingency Plan (CP) Test Results
- POA&M Continuous Monitoring Plan (CMP)
- FedRAMP Control Tailoring Workbook
- Control Implementation Summary Table
- Results of Penetration Testing
- Software Code Review
- Interconnection Agreements/Service Level Agreements/Memorandum of Agreements.

b) Information systems must be assessed by an accredited 3PAO whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.

c) The Government reserves the right to perform Penetration Testing. If the Government exercises this right, the contractor shall allow Government employees (or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with FedRAMP requirements (https://www.fedramp.gov/assets/resources/documents/CSP_Penetration_Test_Guidance.pdf

d) Review activities include but are not limited to scanning operating systems, web applications, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.

e) Identified gaps between required FedRAMP Security Control Baselines and Continuous Monitoring controls and the contractor's implementation as documented in the Security Assessment Report shall be tracked by the contractor for mitigation in

a POA&M document. Depending on the severity of the gaps, the Government may require them to be remediated before a provisional authorization is issued.

f) The contractor is responsible for mitigating all security risks found during A&A and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 30 days from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.

12) Authorization of System

The contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, to verify compliance with the requirements for an Information Technology security program. The Government reserves the right to conduct onsite inspections. The contractor shall make appropriate personnel available for interviews and provide all necessary documentation during this review.

13) Reporting and Continuous Monitoring

Maintenance of the FedRAMP Provisional Authorization will be through continuous monitoring and periodic audit of the operational controls within a contractor's system, environment, and processes to determine if the security controls in the information system continue to be effective over time considering changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated and submitted to the FedRAMP PMO as required by FedRAMP Requirements. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. The deliverables will allow the FedRAMP JAB to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur. Contractors will be required to provide updated deliverables and automated data feeds as defined in the FedRAMP Continuous Monitoring Plan.

All deliverables shall be labeled *"Controlled Unclassified Information" (CUI).* External transmission/dissemination of *Controlled Unclassified Information" (CUI)* to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140 (as amended), "Security requirements for Cryptographic Modules."

CUI is government created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations and government wide parties.

14) Non-Repudiation

The Cloud Contractor vendor shall provide a system that can implement NIST SP 800-53 Control AU-10 approved controls, which provides for origin authentication, data integrity, and signer non-repudiation. This binds the identity of the information producer with the information to and provides the means for authorized individuals to determine the

DRAFT

identity of the producer of the information.

15) Identification and Authentication (Organizational Users)

The vendor shall support a secure, multi-factor method of remote authentication and authorization to identified Government Administrators that will allow Government designated personnel the ability to perform management duties on the system.

The vendor shall support multi-factor authentication including User ID and Password, digital certificate, PIV or smart card, PIN.

16) Identification and Authentication (Non-Organizational Users)

The vendor shall support a secure, dual factor method of remote authentication and authorization to identified Vendor Administrators that will allow vendor-designated personnel the ability to perform management duties on the system.m

17) Incident Reporting Timeframes

Cloud Contractors are required to report all computer security incidents to the United States Computer Emergency Readiness Team (U.S.-CERT) in accordance with U.S.-CERT "Incident Categories and Reporting Timeframes" in , Appendix J, Table J-1 of NIST SP 800-61 (as amended), "Computer Security Incident Handling Guide." Any Category (CAT) 1, CAT 2, or CAT 3 incident, must be reported immediately to their Information Systems Security Officer (ISSO) and the Senior Agency Information Security Officer (SAISO). Any incident that involves compromised Personally Identifiable Information (PII) must be reported to U.S.-CERT within 1 hour of detection regardless of the incident category reporting timeframe.

18) Media Transport

The vendor shall document activities associated with the transport of Federal agency information stored on digital and non-digital media and employ cryptographic mechanisms to protect the confidentiality and integrity of this information during transport outside of controlled areas.

Digital media, containing Federal agency information, that is transported outside of controlled areas must be encrypted using AES 256; non-digital media including but not limited to CD-ROM, floppy disks, etc., must be secured using the same policies and procedures as paper.

Media, containing Federal Agency information that is transported outside of controlled areas must ensure accountability. This can be accomplished through logging and a documented chain of custody form.

Federal Agency data that resides on mobile/portable devices (e.g., USB flash drives, external hard 12 drives, and SD cards) must be encrypted using AES 256. All Federal Agency data residing on laptop computing devices must be protected with approved encryption software.

DRAFT

19) **Boundary Protection**
The CSP/Reseller shall route all external connections through a Trusted Internet Connection (TIC).

20) **Protection of Information at Rest**
The CSP shall provide security mechanisms for handling data at rest and in transit in accordance with FIPS 140-2.

21) **Security Alerts, Advisories, and Directives**
The CSP/Reseller shall provide a list of their personnel, identified by name and role, with system 1 administration, monitoring, and/or security responsibilities that are to receive security alerts, two advisories, and directives. This list shall include ICE SOC.COTS Software Contract Requirements

47. Encryption Compliance

1. **In accordance with ITAR 4.5.3.2 – Encryption Compliance**

Encryption Compliance Terms and Conditions
If encryption is required, the following methods are acceptable for encrypting sensitive information:

a) FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2.

b) National Security Agency (NSA) Type 2 or Type 1 encryption.

c) Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the Department of Homeland Security (DHS) IT Security Program Handbook (DHS Management Directive (MD) 4300A) for Sensitive Systems).

2. **In accordance with ITAR 4.5.3.5 and ITAR 4.5.4.5–**

ISA Terms and Conditions
Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved contractors. The controlled interfaces shall be authorized at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements; memoranda of understanding, service level agreements or interconnection security agreements.

3. **In accordance with ITAR 4.5.3.8 – Personal Identification Verification (PIV) Credential Compliance**

Personal Identification Verification (PIV) Credential Compliance Terms and Conditions

a) Procurements for products, systems, services, hardware, or software involving controlled federal facility or information system shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.

b) Procurements for software products or software developments shall be compliant by accepting PIV credentials as the common means of authentication for access for

DRAFT

federal employees and contractors.

c) PIV-enabled information systems must demonstrate that they can correctly work with PIV credentials by responding to the cryptographic challenge in the authentication protocol before granting access.

d) If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan for achieving HSPD-12 compliance shall be required for review, evaluation, and approval by the CISO.

4. Patch Management Terms and Conditions

The Contractor shall perform patch management services. The Contractor shall push patches that are required by vendors and DHS system owner. This is to ensure that the infrastructure and applications that directly support DHS information system are current in their release and that all security patches are applied. The contractor shall be informed by DHS which patches are required by DHS through the Information Security Vulnerability Management bulletins and advisories. Core applications, the ones DHS utilizes to fulfill their mission, shall be tested by DHS. However, the contractor shall be responsible for deploying patches as directed by DHS. It is recommended that all other applications (host-based intrusion detection system (HIDS), network intrusion detection system (NIDS), Anti-malware, and Firewall) shall be tested by the contractor prior to deployment in a test environment.

48. Detention Services

1. Language Assistance

The contractor is responsible for identifying detainees with limited English proficiency (i.e., who do not speak English as their primary language and who have limited ability to read, speak, write, or understand English) and providing them access to all facility programs and services through language assistance (accurate, timely, and effective communication) at no cost to the detainee. This should be accomplished through professional in-person, telephonic, or video interpretation and translation services or bilingual personnel. The contractor may utilize technological solutions using artificial intelligence (AI), such as machine learning translation or generative AI, to the extent practicable during non-critical communication (i.e., moderate degree of importance, urgency, and significance) or informal interactions with detainees. Machine Translation Technology should be used to communicate the general concept of a request or topic during a discussion or review of a non-vital document. Examples of such communication include collecting or relaying basic and scripted information to or from a detainee during intake; having an informal conversation with a detainee in the housing unit; reviewing and responding to a detainee's non-English grievance or other request related to basic issues/concerns within detention; etc. If the contractor uses Wi-Fi connected technology, then the safety, security, and/or privacy risks will be assessed if any personally identifiable or other sensitive information is stored or shared. Oral interpretation or assistance should be provided for aliens who are illiterate or who speak a language in which written material has not been translated. The contractor shall secure and utilize its own contract for professional language services. If a contractor cannot accommodate a particular language via their own language services contract, ICE will provide support by offering contact information and resources to assist in securing necessary interpretation services at no additional cost. All facility postings and written materials provided to aliens shall generally be translated via professional language services into Spanish and other

DRAFT

languages spoken by significant segments of the detained ICE population with limited English proficiency at the facility. Other than in emergencies, and even then, only until appropriate language services can be procured, other aliens shall not be used for interpretation or translation services. In such situations, the contractor must notify the COR within 24 hours of the emergency.

2. **Disability Accommodations**
   a. **Technical Requirements:** The contractor is required to identify detainees that have open, obvious, and apparent disabilities, including communications and mobility impairments, and provide assistance and reasonable accommodations as requested by the detainee or third-party or needed as identified by facility staff, in accordance with NDS 2026 4.7, Disability Identification, Assessment, and Accommodation, or any modified version of the detention standards published by ICE.

   b. **Operational Requirements:** The contractor must have their own sign language or certified deaf interpretation service. This should be accomplished through professional in-person, telephonic, or video interpretation. The contractor will provide auxiliary aids and services to detainees with communication impairments to ensure there is effective communication between the detainee and facility staff, and detainees and outside stakeholders, such as consulates, attorneys, and religious services providers.

      The contractor must have at minimum the following auxiliary assistive devices at the facility:

      1. Sound Amplifier
      2. Magnifying Glasses or similar
      3. Audio Reader technology
      4. Varying types of batteries for hearing aids
      5. Varying non-prescription strength eyeglasses

3. **Religious Services and Other Programming**
   a. **Space and Technical Requirements:** The detention facility shall provide dedicated space for religious services. The multi-purpose spaces for religious services shall accommodate multiple religious services per week accommodating multiple faith groups sufficient to meet the needs of all aliens who want to participate and considering different classification levels and sexes.

   b. **Operational Requirements:** The contractor shall provide programming for detainees, including religious services and social programs. The contractor shall provide a dedicated Chaplain or religious service coordinator to provide all religious activities consistent with the requirements of NDS 2026.

      The contractor shall provide dedicated space for religious services. The design and operation

DRAFT

of this space shall be consistent with the requirements of NDS or any modified version of the detention standards published by ICE. One multiple purpose space for religious services is not sufficient. The facility will provide one indoor multiple purpose area per 500 beds.

c. **Facilitation of Religious Prayer and Worship Items:** The contractor must maintain a stock of frequently requested religious worship or prayer items, such as religious scriptures/text of various faiths in various languages, rosaries, saint cards, prayer rugs, religious headwear, statues, etc.

   If requested religious items are needed and not available within the facility, the contractor must facilitate the procurement of the items through in-kind donations from family/friends, religious community, or other non-governmental organization, or by purchasing the items. Donated or purchased items to the facility may be retained by the facility upon a detainee's release or removal, if maintaining the items is not a sanitation concern (e.g. headwear worn by detainees should not be maintained). Donated items designated for a specific detainee at the time of the donation, shall become the personal property of the detainee, and may not be retained by the facility.

4. **Legal Access**

a. **Space and Technical Requirements:** The facility shall provide private areas for in-person attorney-client visits equipped with phones, as well as spaces with video teleconferencing capabilities (in-person spaces can include video teleconferencing capabilities or the facility can opt for Virtual Attorney Visitation rooms/booths for video teleconferencing). See 11.0 - Virtual Attorney Visitation Capability and Operation.

   The detention facility shall provide space(s) for a law library that includes connectivity sufficient to allow computers with limited web access to load the ICE provided online law library via the ICE Portal (including websites referenced therein). The number of law library spaces shall be sufficient to accommodate each sex and classification level for a minimum of five (5) hours a week.

b. **Operational Requirements:** The facility shall provide easy access to legal services and meet all requirements of NDS, or any modified version of the detention standards published by ICE.

c. **Staffing Requirements:** The facility shall provide law library coordinator staff with requisite training and/or certification in the following areas to support detained aliens use of the library:

   - Legal research materials and tools, including electronic law library media provided by ICE

   - Notary certification to provide free, notary services as needed language services (including use of language line).

DRAFT

5. **Group Legal Orientation Space**
The Contractor will provide a multi-purpose space that can accommodate group legal orientation presentations. The space shall accommodate no less than 40 aliens and include tables and chairs. The space shall also be equipped with speakers and/or headsets, audio-visual equipment for presentations, and video-conferencing capability for virtual presentations. The multi-purpose space shall be made available for legal presentations for no less than two presentations for three hours in length (including group and individual orientations), three times a week (Monday through Friday).

6. **Manage and Maintain an Alien ICE Telephone System (ITS)**
The ICE designated Alien Communication Services Contractor shall be the exclusive provider of alien communications (phones, tablets) for this federal facility. The Contractor shall be allowed to install vending debit machines and shall receive 100 percent of all revenue collected by sales of prepaid debit services. The Contractor shall be responsible for the costs incurred for installation of the equipment, any monthly telephone charges incurred from the operation of an alien telephone system, and the maintenance and operation of the system. The Contractor shall not be entitled to any commissions, fees, or revenues generated using the alien telephone system or the alien telephones. Telephones should be in an area that provides for a reasonable degree of privacy and a minimal amount of environmental noise during phone calls.

If authorized to do so under applicable law, the Contractor shall monitor and record alien conversations. If alien telephone conversations can be monitored under applicable law, the Contractor shall provide notice to aliens of the potential for monitoring. However, the Contractor shall also provide procedures at the federal facility for aliens to be able to place unmonitored telephone calls to their attorneys.

Telephone rates will not exceed the Federal Communications Commission rates for inmate telephone service, as well as established state rates where applicable, and shall conform to all applicable federal, state, and local telephone regulations.

7. **Recreation**
   a. **Space and Technical Requirements:** The facility shall provide indoor and outdoor space for recreational activities appropriate for the detainee population and consistent with the requirements under NDS or any modified version of the detention standards published by ICE.

   b. **Operational Requirements:** The facility shall provide detainees with access to recreational programs and activities, held outdoors when available, within the constraints of the safety and security of the facility and consistent with the requirements under NDS. No more than 250 aliens shall be in one recreational space at any one time.

   Recreation shall be offered at a reasonable time of day. Weather permitting, each detainee shall have access for at least one hour per day, five days per week; or, six or more hours per week, at least four days per week that allows for vigorous aerobic exercise with extended hours of availability.

8. **Alien Voluntary Work Program**
Facility permitting, detainees may participate in a voluntary work program to earn money.

DRAFT

Participation in a voluntary work program is strictly voluntary and may include assignments in industrial, maintenance, custodial, service, or other tasks. Detainees shall not be required to work, except for personal housekeeping. Detainee volunteers shall not be used as substitutes for facility employees or assigned work in areas where sensitive documents are stored, such as designated ICE workspaces.

The facility shall provide sufficient security staff to supervise detainees participating in the

voluntary work program. Work assignments must remain within the security perimeter unless approved by the Contracting Officer's Representative (COR). High-custody detainees shall not, under any circumstances, work outside the secure outer perimeter.

STANDARDS AND PROCEDURES

1. **Voluntary Work Program**

   If the facility has a voluntary work program, the facility shall develop a voluntary work program plan, subject to approval by the COR.

   Participation in the program is strictly voluntary.

   It will be the sole responsibility of ICE to determine whether a detainee will be allowed to perform on voluntary work details and at what classification level. All detainees shall be searched when they are returned from work details.

   Voluntary Special Details

   Detainees may volunteer for temporary special work details, typically lasting several hours to several days, involving tasks such as digging trenches, removing topsoil, and other labor-intensive activities.

   a. Detainee Selection
      The federal facility shall develop site-specific rules for selecting work detail volunteers
      Detainees shall not be denied voluntary work opportunities based solely on race, religion, national origin, color, sex, sexual orientation, age, or disability.

   b. Detainees with Disabilities
      Where possible, the federal facility shall allow detainees with disabilities to participate in the voluntary work program through appropriate work assignments.

   c. Work Hours and Restrictions
      Detainees participating in the voluntary work program shall adhere to a fixed schedule, working no more than 8 hours per day and 40 hours per week.
      The federal facility may limit the number of work details assigned to a detainee in a single day.

   d. Reimbursement
      Detainee volunteers participating in the voluntary work program are not considered

federal facility and/or government employees and are not entitled to wages or benefits under applicable federal wage laws, state minimum wage laws, or labor regulations.

Detainees shall not receive a stipend exceeding the amount Congressionally allocated to ICE for reimbursing contract facilities in support of the Voluntary Work Program. The federal facility is responsible for ensuring detainees receive their owed reimbursement in cash (USD) before transfer or release.

e. Removal of Detainee from Work Detail
A detainee may be removed from a work detail for cause. The federal facility shall document the justification for removal in the detainee's detention file or a retrievable electronic record.

f. Detainee Responsibilities
The federal facility shall establish procedures to inform detainee volunteers of their job responsibilities and reporting procedures. Detainees must use safety equipment and follow other precautions as instructed by the work supervisor.

g. Detainee Training and Safety
Detention facilities shall comply with all applicable federal health and safety regulations and standards. Detainees shall be provided basic OSHA protections and appropriate safety/protective clothing and equipment during work assignments.

Medical staff shall ensure detainees are medically screened and certified before undertaking food service assignments. The federal facility shall ensure all department heads develop appropriate training for detainee workers.

Before beginning any job or work detail, the supervisor shall provide the detainee with thorough instructions on safe work methods and, if applicable, hazardous materials. The detainee must sign a voluntary work program agreement, confirming they have received and understood the training provided by the supervisor. The agreement shall be placed in the detainee's detention file or retrievable electronic record.

h. Detainee Injury and Reporting Procedures
The federal facility shall establish procedures to immediately and appropriately respond to on-the-job injuries, including immediate notification to ICE/ERO.

49. Detention Facility ERO Case Processing Specialists Position Description

Case Processing Specialists

The Case Processing Specialist shall hold an accredited associate or bachelor's degree in an appropriate discipline or have a minimum of one year of directly related industry experience. The Case Processing Specialist will have knowledge of program objectives, policies, procedures, and requirements related to immigration case processing. The Case Processing Specialist must have prior experience and/or training related to reviewing law enforcement documentation such detention files, custodial records, or immigration case files including A-files and DHS databases, or previous experience conducting interviews for immigration or detention related purposes.

DRAFT

Case Processing Specialists shall assist ICE Personnel with the following duties under the general direction of ICE field office personnel:

1. **Case Processing, Docket Management, Data Entry and Records Management duties:**
   a. Process cases and perform all peripheral activities, immigration records management, and document preparation.

   b. Prepare, review, and manage case files, ensuring accuracy and completeness in all documentation.

   c. Ensure Alien Files (A-files) and ICE systems reflect a case status that is updated, accurate, and complete.

   d. Accurately enter data into ICE systems, ensuring compliance with agency protocols and data integrity requirements.

   e. Maintain and update electronic and paper-based case files, ensuring compliance with federal privacy laws, DHS policies, and federal data security requirements.

   f. Retrieve, compile, and organize county, state, and federal court records, conviction documents, and supporting case materials from multiple databases, and other government sources.

   g. Maintain up-to-date case status records, court scheduling details, and case tracking logs.

   h. Generate case status reports and monitoring dashboards.

   i. Assist with docket coordination with EOIR and USCIS. Coordinate with ICE officers to facilitate interviews, hearings, removals, and case updates.

   j. Review appropriate paperwork for completeness and accuracy.

   k. Ensure all administrative applications are reviewed, A-files are updated, and docket officers timely notified for appropriate law enforcement action.

   l. Track compliance with release conditions and report violations, as applicable.

   m. Assist ICE Office of Principal Legal Advisor (OPLA) in obtaining criminal history checks and other supporting documentation as needed prior to court.

   n. Assist ICE personnel with scheduling and coordinating interviews between detainees and ICE officers, consulates, and legal representatives, as assigned.

2. **Removal and Post Removal Management duties:**
   a. Organize and prepare removal documents and coordinate with ICE personnel for scheduling removal and staging flights. Ensure all documentation is prepared and accurate.

   b. Ensure aliens scheduled for removal have the necessary documentation in A-files per ICE

instructions.

c. Ensure travel information, ICE Air scheduling and manifest(s) are completed, detention center release forms are prepared, and property inventories/receipts are ready on the scheduled time and day of departure.

d. Ensure detainees have the necessary legal paperwork, seven-day supply of medications, property, and valuables before transfer or removal.

e. Collect, review for completeness and accuracy, and file signed Form I-205 Warrant of Removal/Deportation departure verifications in A-file

f. Ensure case is closed in ICE data systems and file is transferred to the National Record Center for storage.

3. Other duties:

a. Schedule interviews between detainees and ICE officers, consulates, and legal representatives as applicable.

b. Communicate with all aliens in the alien's primary language.

c. Provide other logistical and administrative support for ICE personnel as assigned.

d. Provide surge support after hours, including expanded breadth and depth of tasks, as required.

50. Robotics Process Automation (RPA) Contract Requirement

The Detention Facility Robotics Process Automation (RPA) process requires that data supporting detention bed space, ground transportation, and any other additional costs covered by the current contract will be recorded utilizing the Detention Transportation Template (DTT) (Attachment 16). This data template should be completed in its entirety in the established format once all data supporting the monthly operations is available. Once completed, the DTT must be submitted via e-mail to both the ERO Field Office COR and the ERO RPA Team Mailbox. Please note that the requirement for submission of the DTT is prior to and in addition to the invoice submission requirement already included in this contract. Please note that DTT updates may be requested by the COR and will require timely resubmission to the COR and the ERO RPA Team Mailbox.
The government reserves the right to update the federal detention facility invoice process, templates or other related documents, to fix issues, expand capabilities, and improve performance of the reconciliation process.

51. Notification and Public Disclosures

There shall be no public disclosure regarding this contract made by the Contractor (or any subcontractors) without review and approval of such disclosure by ICE Public Affairs. The government considers such information privileged or confidential.

DRAFT

52. Records, Visits, and Disclaimers

All records related to contract performance shall be retained in a retrievable format for the duration of the contract. The Contractor shall, upon completion or termination of the contract, transmit to the government any records related to the performance of the contract, in a format acceptable to the CO.

The Contractor shall comply with all statutes, regulations, and guidelines from the National Archives and Records Administration (NARA). Records and information management functions are required and mandated by the following laws and regulations: Chapters 21, 29, 31, and 33 of Title 44, U.S. Code; 36 CFR 12; 41 CFR 201 subchapters A and B; Office of Management and Budget (OMB) Circular A-130; and Department of Justice (DOJ) Order 2710.8A, *Removal and Maintenance of Documents*. Criminal penalties for unlawfully destroying, damaging, removing, or improperly handling or releasing federal records are addressed in Chapters 37 and 101 of Title 18, U.S. Code.

All alien files are to be prepared, maintained, retired, and disposed of in accordance with ICE policy. Policies and procedures shall be developed to ensure the confidentiality and security of all alien files. The Contractor shall be responsible for alien record keeping services and personal property. See Attachment 15 – Personal Property Operations Handbook.

The Contractor shall safeguard all records related to the operation of the federal facility.

Except as provided in the below paragraph, all records acquired or generated by the Contractor in the contracting process, or its performance of this contract, or as a result of this contract, including records classified as Privacy Act systems of records, are federal records under the control of ICE and all determinations regarding the disclosure of this information will be made by ICE in accordance with applicable federal laws, regulations, policies, and executive orders or as ordered by a court.

ICE will comply with the provisions set forth in 6 C.F.R §5.7 "Confidential Commercial Information," as applicable, in the event ICE intends to release the contract documents or

any information relating to this contract, including clause (e) "Opportunity to Object to Disclosure" thereof. Insofar as any documents created by the Contractor contain any information related to one or more ICE aliens, these records shall be the property of ICE and all determinations regarding the disclosure of this information will be made by ICE in accordance with applicable federal laws, regulations, policies, and executive orders or as ordered by a court. To the extent the Contractor intends to release the contract or any information relating to the contract, the Contractor agrees to coordinate with the CO and obtain an ICE concurrence prior to any such release

Contractor-owned records are considered the property of the Contractor and are not within the scope of the paragraph above. Contractor-owned records include the following:

a. Contractor's employment related records,

b. Contractor's patents, copyright, and trademark applications, where the Contractor has elected rights or has permission to assert rights and has not relinquished such rights or turned such rights over to the government,

c. Contractor's non-public financial records which are not related to the performance of this contract, and

d. Contractor's records which are not related to the performance of this contract.

All records acquired or generated by the Contractor related to this contract and in possession of the Contractor, including those described in the two paragraphs above, shall be subject to inspection, copying, and audit by the government or its designees at all reasonable times, and the Contractor shall afford the government or its designees reasonable facilities for such inspection, copying, and audit; provided; however, that upon request by the CO, the Contractor shall deliver such records to a location specified by the CO for inspection, copying, and audit. The government or its officials shall use such records in accordance with applicable federal law, regulation, and policy (including, but not limited to, the Privacy Act), as appropriate.

This clause applies to all records created, received and maintained by the Contractor without regard to the date of origination of such records, including all records acquired from a predecessor Contractor or predecessor contract or intergovernmental service agreement. The requirements of this clause shall flow down to all sub-Contractors of the Contractor in the performance of this contract.

The Contractor shall notify the COR when a member of the U.S. Congress or any media outlet requests information or makes a request to visit the federal facility. The Contractor shall coordinate all public information related issues with the CO. All press statements and releases shall be cleared, in advance, with the ICE Office of Public Affairs, which can be reached through the Internet website: ICEMedia@ice.dhs.gov.

The Contractor shall ensure employees agree to use appropriate disclaimers clearly stating the employees' opinions do not necessarily reflect the position of the U.S. government in any public presentations they make or articles they write that relate to any aspect of contract performance or the federal facility operations.

53. ICE/ERO Control Over Facility Access

Pre-clearance approval from ICE/ERO is required for any person or entity to have access to ICE field staff, facilities and information, including any proposed law enforcement officer visits. All requests must be submitted in accordance with the requirements found at www.ice.gov/leadership/ocr. At facilities that house detainees for both ICE and the U.S. Marshals Service, inquiries regarding each agency's detainees will be directed to agency responsible for the detainee.

All requests by NGOs and other stakeholders (which include, but are not limited to, intergovernmental entities, state and local governmental agencies, and members of academia, for tours or visits (including combined tour-and-visits events) must be submitted in writing to the local ICE/ERO Field Office. Tour requests should not be directed to the facility.

Any such requests received by the facility shall be forwarded to the Field Office for review. When

deciding whether to approve or deny the request, the Field Office Director, or his or her designee, will take into consideration safety and security, and the availability of personnel to staff the tour or visit. All tour or visit participants will be expected to submit personal information required by applicable ICE policies, so the Field Office can perform background checks as necessary.

54. Federal Judiciary

The contractor shall ensure all judicial inquiries and program recommendations are responded to in a timely and accurate manner. All judicial inquiries and contractor responses, specifically related to an alien, shall be made part of the alien's A-file.

55. Quality Control Plan (QCP)

The Contractor is responsible for management and actions necessary to meet the standards set forth in the contract. The Contractor shall provide an overall QCP that addresses critical operational performance standards for the services required under this contract. The Contractor shall provide a QCP to the CO and the COR for concurrence not later than the post award conference (or as directed by the CO). The CO will notify the Contractor of concurrence or required modifications to the plan before the contract's start date. The QCP shall ensure that services will be maintained at an acceptable level. At a minimum, the Contractor shall review and update the QCP on an annual basis or as required. The QCP shall identify deficiencies, appropriate corrective action(s), and timely implementation plan(s) to the COR.

56. Quality Assurance Surveillance Plan (QASP)

ICE has developed a Quality Assurance Surveillance Plan (QASP), incorporated in Section J *(See PWS Attachment – Quality Assurance Surveillance Plan)*, pursuant to the requirements of the PWS. It will present the financial values and mechanisms for applying adjustments to the contractor's invoices as dictated by work performance measured to the desired level of accomplishment.

The purpose of the QASP is to:

a) Define the roles and responsibilities of participating Government officials.

b) Define the types of work to be performed.

c) Describe the evaluation methods that will be employed by the Government in assessing the contractor's performance.

d) Describe the process of performance documentation.

e) Roles and Responsibilities of Participating Government Officials a) The COR(s) will be responsible for monitoring, assessing, recording, and reporting on the technical performance of the contractor on a day-to-day basis. The COR(s) will have primary responsibility for completing "Quality Assurance Surveillance Forms" to document their inspection and evaluation of the contractor's work performance.

f) The CO or designee has overall responsibility for evaluating the contractor's performance in areas of contract compliance, contract administration, cost, and property control. The CO shall review the COR's evaluation of the contractor's performance and invoices. If applicable,

DRAFT

deductions or withholdings will be assessed in accordance with the evaluation of the contractor's performance, e.g., monetary adjustments for inadequate performance.

57. Contractor's Failure to Perform Required Services

The rights of the government and remedies described in this section are in addition to all other rights and remedies set forth in the contract. Specifically, the government reserves its rights under the inspection of services and termination clauses. Any reductions on the Contractor's invoice shall reflect the contract's reduced value resulting from the Contractor's failure to perform the required services. The Contractor shall not be relieved of the full performance of the services hereunder and may be terminated for default based upon the inadequate performance of services, even if a reduction was previously taken for any inadequate performance.

58. Performance Evaluation Meetings

The Contractor's representatives shall meet with the COR monthly or as deemed necessary by performance, and a discussion and resolution of problems.

59. Organizational Chart

The Contractor shall provide an organizational chart that describes the structure of authority, responsibility, and accountability within the facilities. The Contractor shall update this chart as necessary. The Contractor shall make the chart available for review by the CO or COR upon request.

60. Personnel and Staffing

1. Federal Facility Staffing Plan and Key Personnel

   The Contractor shall have a staffing plan to effectively staff the federal facility in a safe and secure manner. The number, type and distribution of staff as described in the staffing plan shall be maintained throughout the term of the contract. Candidates that have been cleared by the contractor's screening process, and who are fully enrolled into the U.S. Government's suitability determination processing system, will be counted toward the minimum monthly staffing levels. Written requests to change the number, type and/or distribution of staff described in the staffing plan must be submitted to the CO and the COR, for approval prior to implementation and incorporation into this contract. Staffing levels should not fall below a monthly average of 85% for custody staff, 85% for health services staff, and 85% for all other departments of the approved staffing plan. The approved staffing levels for detention officers (custody) shall not fall below a monthly average of 85%. Staffing levels for all departments other than custody and health services will be calculated in the aggregate. If the Contractor does not provide health services, the health services staffing level does not apply.

   Each month, the Contractor shall submit to the COR the current average monthly vacancy rate and indicate any individual positions that have been vacant more than 120 calendar days. Failure to fill any individual position within 120 calendar days of the vacancy may result in a deduction from the monthly invoice. In assessing deductions, ICE may also consider costs associated with overtime used to cover vacant positions.

   Each month, the Contractor shall submit to the COR any key personnel that will be absent from the federal facility for over five working days. If the key personnel will be absent for over five working days and the Contractor will not provide an "acting" position to backfill that key

DRAFT

personnel position during the absence, the CO has the right to make a deduction based on the salary and benefits of the absent key personnel position.

2. **Federal Facility Floor Plan and Guard Post Map**
   The Contractor shall provide a federal facility floor plan which clearly identifies all recommended detention guard posts and corresponding guard shift requirements (e.g., 24/7, 8 hours M – F, weekend-only, etc.). The floor plan shall be submitted with the federal facility staffing plan and shall be approved by the CO/COR prior to commencement of services under this contract.

   Changes to the guard posts or shift requirements shall be approved by the CO/COR.

3. **Employment Eligibility**
   The Contractor shall employ personnel whose qualifications are commensurate with job responsibilities and authority levels. The Contractor shall assure that employees meet the standards of competency, training, appearance, behavior, and integrity. The Contractor will affect disciplinary or adverse action against employees who disregard those standards.

   Screening criteria under DHS Instruction 121-01-007-001 (Personnel Security, Suitability and Fitness Program), or successor thereto, that may exclude Contractor employees from consideration to perform under this contract includes:

   i. Misconduct or negligence in employment.

   ii. Criminal or dishonest conduct.

   iii. Material, intentional false statement, or deception of fraud in examination or appointment.

   iv. Refusal to furnish testimony as required by 5 CFR § 5.4 (i.e., a refusal to provide testimony to the Merit Systems Protection Board or the Office of Special Counsel).

   v. Illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation.

   vi. Alcohol abuse, without evidence of substantial rehabilitation, of a nature and duration that suggests that the applicant or appointee would be prevented from performing the duties of the position in question or would constitute a direct threat to the property or safety of the applicant, appointee, or others.

   vii. Knowing and willful engagement in acts or activities designed to overthrow the U.S. government by force.

   viii. Any statutory or regulatory bar which prevents the lawful employment of the person involved in the position in question.

DRAFT

ix. Any other nondiscriminatory reason that an individual's employment (or work on a contract) would not protect the integrity or promote the efficiency of the service.

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

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

4. Key Personnel

The COR shall provide written approval before any employee is assigned as key personnel to perform duties under this contract. Rejection of any key personnel shall come in writing from the contracting officer. The Contractor shall have key personnel employed and available for duty before the Contractor can begin contract performance. Any subsequent changes to key personnel must meet these criteria and be approved in writing by the CO. The following are considered key personnel for the contract. The Contractor may use other titles.

a) Facility Administrator. The facility administrator shall hold an accredited bachelor's degree in an appropriate discipline, or significant military, or corrections experience at a minimum of 15 years, and have at least five years of related administrative experience, and have knowledge of program objectives, policies, procedures, and requirements for managing a secure detention/correctional federal facility. The degree requirement may be satisfied by completion of a career development program that includes work related experience, training, or college credits at a level of achievement equivalent to the bachelor's degree, as practiced in the federal hiring process. The official holding this position, even in an acting capacity, shall meet ACA requirements.

b) Assistant Facility Administrator. The assistant facility administrator shall hold an accredited bachelor's degree in an appropriate discipline or have a minimum of three years of related industry experience, and have knowledge of program objectives, policies, procedures, and requirements for managing a secure detention/correctional federal facility. The official holding this position, even in an acting capacity, shall meet ACA requirements.

c) Supervisory Detention Officers. Supervisors must have a minimum of one year of experience as a detention officer and two years of successful experience in field supervision (e.g., civilian community law enforcement, commercial or industrial guard service, or supervisory security service positions). The two-year requirement may be satisfied by completion of a career development program that includes work-related experience, training, or college credits at a level of achievement equivalent to the basic requirement,

DRAFT

as practiced in the federal hiring process.

d) Training Officers. Certified instructors shall conduct all instruction and testing of Contractor personnel. A state or nationally recognized institution certification of instructors is mandatory unless otherwise approved in writing by the COR. Certification of instructors may be established by documentation of experience in teaching positions or by successful completion of a course of training for qualifying personnel as instructors. The COR must approve the instructor prior to any training.

e) Quality Assurance Manager. The quality assurance manager shall hold an accredited bachelor's degree in an appropriate discipline or have a minimum of three years of related industry experience, and have knowledge of program objectives, policies, procedures, and requirements for managing a secure detention/correctional federal facility.

f) Corporate Security Officer: The corporate security officer will interface with the ICE Office of Professional Responsibility (OPR) Personnel Security Division (PSD) through the COR on all security matters, to include physical, personnel, and protection of all government information and data accessed by the Contractor.

5. Health Requirements for all Detention Officers

The Contractor is solely responsible for ensuring employees can perform essential functions described within this contract, with reasonable accommodation, if applicable. All officers who work under this contract shall pass a medical examination conducted by a licensed medical professional within 30 days prior to initial assignment.

6. Employee Health and Health Records

OSHA Publications By Search | Occupational Safety and Health Administration

Employee health files for all Contractor employees must be maintained on-site, in a locked cabinet. Health files are to be maintained in accordance with DHS and ICE Privacy Policies and the Privacy Act of 1974 and contain the following documents:

a. Initial and annual tuberculosis (TB) infection screening results.

b. Vaccination records including results, titers, and Immunization Declination Form(s).

c. OSHA 301 Incident forms.

d. Blood borne pathogen exposure documentation.

e. Respirator medical clearance.

f. Respirator fit test results.

g. Other employee health documents.

The Contractor may initiate employment of an individual who has initiated the required

vaccines schedule, and the individual hired may begin work on the contract if they meet all subsequent vaccine schedule requirements until fully vaccinated.

7. **Minimum Staffing Requirements**
Exclusive of the agreed upon ramp periods, the Contractor shall fully staff the federal facility to secure, control, feed, and supervise aliens in custody regardless of the population. The Contractor shall ensure daily detention officer assignment rosters, by shift, are maintained. The assignment rosters shall indicate the number of staff, job titles, names, hours, and days of work for each post. The daily roster shall be posted 24 hours in advance. Shift rosters must be provided to the COR daily.

8. **Recommended Immunizations**
Individuals employed by the Contractor in a custody or detention environment are at significant risk for acquiring or transmitting Hepatitis B, measles, mumps, rubella, varicella, seasonal influenza, and COVID-19. These diseases are vaccine preventable. Therefore, the following vaccinations are highly recommended for the Contractor's personnel. If staff decline or refuse any of these recommended vaccines, an Immunization Declination Form is required, and the COR must be notified of the refusal. ICE reserves the right to refuse Contractor employees that refuse vaccines.

a) Hepatitis A.

b) Hepatitis B; (Note: The U.S. OSHA Blood-borne Pathogens (BBP) Standard requires employers to provide employees at risk of occupational exposure to blood and other potentially infectious material (OPIM) with the Hepatitis B vaccination series. Refer to OSHA regulations Occupational Safety and Health Administration

c) Varicella.

d) Measles, Mumps, Rubella (MMR).

e) Diphtheria, tetanus, a-cellular pertussis (DTAP); and

f) Annual seasonal influenza.

g) COVID-19

The Contractor's personnel will provide immunization documentation or titer results to the health services administrator or the employer's representative for placement in the employee health file. It is recommended that the CDCs Immunization of Healthcare Workers: Recommendations of the Advisory Committee on Immunization Practices and the Hospital Infection Control Practices Advisory Committee be used as a reference for employee health immunization issues.

https://www.osha.gov/law-regs.html

OSHA Publications By Search | Occupational Safety and Health Administration

DRAFT

If requested by the COR, the Contractor shall make medical records of contract employees available for review. Prior to the officer's initial assignment or reassignment to the federal facility, the Contractor shall certify in writing to the COR that each detention officer is in full compliance with the following:

a. Staff shall not have diseases that may be transmitted to and result in the disablement of other individuals and shall be physically and mentally able to perform the essential functions of their position, either with or without reasonable accommodation, and without creating a significant risk of substantial harm to the health or safety of that officer or others, which risk cannot be eliminated or reduced by a reasonable accommodation.

b. Detention officers are required to have the following:

c. Correctable distant vision must be equal to or better than 20/20 in each eye.

d. Binocular distant vision must be correctable to 20/20.

e. Monocular vision is generally disqualifying; depth perception must be equal to or better than 70 seconds
of arc.

f. Peripheral vision must be normal.

g. Color vision must be normal.

    i. Acceptable measure of color discrimination is the Ishihara color (14 plates). X chrome lenses are not acceptable to ICE as a means of correcting color deficiencies. Any disease or condition which interferes with a person's vision may be considered disqualifying. Cases will be reviewed on a case-by-case basis by the COR.

h. Detention officers are required to be able to hear in the frequency range from 500-2000 hertz (Hz), the deficit should not exceed 30 decibels in either ear. At 3000 Hz, the deficit should not exceed 40 decibels in either ear. Any disease or condition, which interferes with the ability to hear, may be considered disqualifying. Cases will be reviewed on a case-by-case basis by the COR.

i. Detention officers shall not have heart, lung, skeletal, or other physical defects that would impair their ability to perform effectively in either normal or emergency situations.

j. Detention officers shall possess unimpaired use of hands, arms, legs, and feet.

k. detention officers shall be able to run when necessary and be capable of handling portable fire extinguishers, building fire hoses, and related equipment.

l. Detention officers shall be able to wear all necessary equipment, or other protective

DRAFT

items.

m. Officers shall be mentally alert and emotionally stable with an absence of detectable neurotic or psychoneurotic conditions that would affect their ability to act during a stressful situation involving mental stress.

n. As required by the OSHA, 29 CFR, Part 1910.1035 (Occupational Exposure to Tuberculosis), all employees in occupations with high-risk exposure are required to have a TB Skin Test completed annually. The Contractor shall complete a baseline test on all newly hired employees. Each employee must have a TB Skin Test Certificate prior to entering on his/her first day of duty. The Contractor shall be responsible for re-testing employees annually.

   The Contractor shall report immediately any changes to (1) through (8) above, in a detention officer's health status to the COR. If the COR determines that Contractor employees do not meet minimum health standards, the Contractor's employee must undergo a "Fitness for Duty" examination at no cost to the government.

o. Officers must have no hearing defects or no hearing defects with the use of a correctable device.

9. Contractor Staffing and Employee Requirements

The Contractor shall provide employee requirements or policies, which, at a minimum, address the following:

a. Organization.

b. Recruiting procedures.

c. Opportunities for equal employment.

d. Qualifying for jobs, job descriptions, responsibilities, salaries, and fringe benefits.

e. Screening employees for illegal drug use.

f. Holidays, leave, and work hours.

g. Personnel records, employee evaluations, promotion, and retirement.

h. Training.

i. Standards of conduct, disciplinary procedures, and grievance procedures.

j. Resignation and termination.

k. Employee-management relations.

DRAFT

l. Security, safety, health, welfare, and injury incidents.

The Contractor shall provide a copy of the rules or policies to federal facility employees. Upon request by the COR, the Contractor shall document that all employees have reviewed a copy of the requirements or policies.

10. Minimum Standards of Employee Conduct

The Contractor shall develop standards of employee conduct and corresponding disciplinary actions that are consistent with the following standards of conduct. All employees shall certify in writing that they have read and understand the standards. A record of this certificate must be provided to the COR prior to each employee beginning work under this contract. The Contractor will hold employees accountable for their conduct based on these standards, which are not restricted to, but should include:

a. Employees shall not display favoritism or preferential treatment to one alien, or group of aliens, over another.

b. Employees shall not discuss or disclose information from alien files or immigration cases, except, when necessary, in the performance of duties under this contract.

c. The employee may not interact with any alien except in a relationship that supports the approved goals of the federal facility. Specifically, employees shall not receive nor accept any personal (tangible or intangible) gift, favor, or service, from any alien, any alien's family, or associate no matter how trivial the gift, favor, or service may seem, for themselves or any members of their family. In addition, the employee shall not give any gift, favor, or service to aliens, alien's family, or associates.

d. The employee shall not enter any business relationship with aliens or their families (e.g., selling, buying, or trading personal property).

e. The employee shall not have any outside or social contact with any alien, his or her family, or associates, except for those activities which are part of the federal facility program and a part of the employee's job description.

f. All employees are required to immediately report to the warden/federal facility director or ICE supervisor any criminal or non-criminal violation or attempted violation of these standards.

g. The Contractor or ICE supervisor shall report all violations or attempted violations of the standards of conduct or any criminal activity immediately to the COR. Violations may result in employee removal from the federal facility. Failure on the part of the Contractor either to report a known violation or to take appropriate disciplinary action against an offending employee(s) shall subject the Contractor to appropriate action including possible termination of the contract for default.

The Contractor should not employ any person whose employment would present an actual or apparent conflict of interest. The Contractor is specifically prohibited from hiring

DRAFT

active-duty military personnel and civilians employed by the government to perform work under this contract.

11. Minimum Personnel Qualification Standards

The Contractor shall ensure that each person employed by the firm, or any subcontractor(s) has a social security card issued and approved by the Social Security Administration, and shall be a U.S. citizen or a person lawfully admitted into the U.S. for permanent residence, have resided in the U.S. for the last five years (unless abroad on official U.S. government duty), possess a high school diploma or equivalent, and obtain a favorable suitability for employment determination. Each employee of the Contractor and any subcontractor(s) must complete and sign a Form I-9, "Employment Eligibility Verification," before commencing work. The Contractor shall retain the original Form I-9 and shall furnish the COR with a copy of Form I-9 before the employee commences work. The Contractor shall be responsible for the acts and omissions of its employees and of any subcontractor(s) and their employees.

In addition, each contract employee shall meet the following requirements in accordance with the contract requirements:

a. All employees shall be at a minimum of 21 years of age.

b. Employees shall have at least one year of general experience that demonstrates the following:

c. The ability to greet and deal tactfully with the public.

d. Capability of understanding and applying written and verbal orders, rules, and regulations. All personnel shall be literate and be able to interpret printed rules and regulations, detailed written orders, training instructions and materials, and must be able to compose reports.

e. Good judgment, courage, alertness, even temperament, and render satisfactory performance through knowledge of his/her position responsibilities.

f. Ability to maintain poise and self-control during situations that involve mental stress, such as fires, explosions, civil disturbances, and building evacuations.

g. All employees on this contract must maintain current/physical residency in the continental U.S.

h. All qualified, armed employees working as transportation officers shall have a minimum of one year of experience as a law enforcement officer, military policeman, or as a security officer engaged in functions related to detaining civil or administrative aliens. A degree in a related or appropriate field/discipline may substitute for experience (i.e., detention, corrections, criminal justice, etc.).

12. Random Drug Testing

DRAFT

The Contractor will have a random drug-screening program. ICE may require drug screening for cause at any time. The Contractor shall order and accomplish drug screening at the Contractor's expense. A laboratory approved by the National Institute of Drug Abuse shall perform the screening. The Contractor shall provide the results of all such drug screenings to the COR within 24 hours of receipt.

13. Contraband Program and Inspection

A contraband control program shall be established in accordance with NDS 2026 on contraband and ACA standards.

The Contractor's employees will be subject to random contraband inspection in accordance with federal facility standards and policies. ICE may require contraband screening and inspection for cause at any time. Upon notification of a violation by the COR, the

Contractor shall immediately remove the employee from performing duties under this contract. The Contractor shall revoke employees' credentials, complete the required disposition, and immediately notify the COR when the employee is removed from duty.

14. Required Documentation

All Contractor personnel must provide documentation regarding the following: History of testing for TB within the last 12 months:

a. Chest x-ray if employee has a history of latent TB infection (LTBI), treatment history for LTBI or TB disease, if applicable.

b. Additionally, on an annual basis and at Contractor's expense, the Contractor shall provide a current, tuberculin skin test or interferon-gamma release assays test result. If the employee previously tested negative for LTBI, evaluate for TB symptoms. If the employee previously tested positive for LTBI and followed up as appropriate in accordance with Centers for Disease Control and Prevention (CDC) guidelines.

15. Removal from Duty

If the COR or the Contractor receives and confirms disqualifying information concerning a Contractor employee, the Contractor shall, upon notification by the COR, immediately remove the employee from performing duties under this contract. The Contractor shall revoke the employee's identification credentials and complete any required dispositions. The Contractor shall immediately notify the COR when the employee is removed from duty. Disqualifying information includes but is not limited to the following:

a. Conviction of a felony, a crime of violence, domestic violence, or a serious misdemeanor.

b. Possessing a record of arrests for continuing offenses.

c. Falsification of information entered on suitability forms.

d. Non-payment of court ordered payments (child support, liens, etc.) or excessive

DRAFT

delinquent debt as determined by credit check.

e. Misconduct or negligence in prior employment, which would have a bearing on efficient service in the position in question or would interfere with or prevent effective accomplishment by the employing agency of its duties and responsibilities.

f. Alcohol abuse of nature and duration which suggests that the applicant or appointee would be prevented from performing the duties of the position in question or would constitute a direct threat to the property or safety of others.

g. Illegal use of narcotics, drugs, or other controlled substances, without evidence of substantial rehabilitation.

h. Introduction of contraband into or unto the federal facility.

i. ICE may direct the Contractor to remove any employee who has been disqualified either for security reasons or for being unfit to perform his/her duties as determined by the COR or the CO. The Contractor shall act immediately and notify the COR when the employee is removed from duty. A determination to be unfit for duty may be made from, but is not limited to, incidents of delinquency set forth below:

i. Violation of the Rules and Regulations Governing Detention facilities set forth in ICE Publications entitled "Detention Officer Handbook."

j. Violation of the Rules and Regulations Governing Public Buildings and Grounds, 41 CFR 101-20.3.

k. Neglect of duty, including sleeping while on duty, loafing, unreasonable delays or failures to carry out assigned tasks, conducting personal affairs during official time, leaving post without relief, and refusing to render assistance or cooperation in upholding the integrity of the security program at the work sites.

l. Falsification or unlawful concealment, removal, mutilation, or destruction of any official documents or records, or concealment of material facts by willful omissions from official documents or records.

m. Theft, vandalism, immoral conduct, or any other criminal actions.

n. Possessing, selling, consuming, or being under the influence of intoxicants, drugs, contraband, or substances which produce similar effects.

o. Unethical or improper use of official authority or credentials.

p. Unauthorized use of communication equipment or government property.

q. Misuse of equipment or weapons.

DRAFT

r. Violations of security procedures or regulations.

s. Recurring tardiness.

t. Undue fraternization with aliens as determined by the COR.

u. Repeated failure to comply with visitor procedures as determined by the COR.

v. Performance, as determined by investigation by the CO, involving acquiescence, negligence, misconduct, lack of diligence, good judgment, and/or good common sense resulting in, or contributing to, an alien escape.

w. Failure to maintain acceptable levels of proficiency or to fulfill training requirements.

x. Changes in an employee's ability to meet the physical and/or mental health requirements of this contract.

y. Contractor employees who are under investigation by any law enforcement agency will be removed from duties pending outcome of the disposition.

    i. At the direction of the COR, the Contractor shall reassign contract employees who have been arrested or who have alleged misconduct, to duties that do not permit direct contact with aliens pending the disposition of the charges. Any alleged misconduct shall be reported immediately to the COR. If such reassignments are not available, the Contractor shall remove the employee from work under this contract and other ICE contracts.

16. Tour of Duty Restrictions

The Contractor shall not utilize any uniformed Contractor employee to perform duties under this contract for more than 12 hours in any 24-hour period and shall ensure that such employees have a minimum of eight hours off between shifts. Authorization is required from the COR prior to an employee performing services that exceed 12 hours; provided, however, the Contractor may utilize uniformed employees to perform duties under this contract for up to 16 hours in any 24-hour period in the event of an emergency or other non-routine circumstances. If an employee is performing other duties for either the Contractor or another employer, those hours shall count against the 12-hour or 16-hour limitation. Employees performing transportation duties can work up to 15 hrs. in a 24-hour period as needed in accordance with U.S. Department of Transportation regulations.

17. Dual Positions

If a supervisory detention officer is not available for duty the Contractor shall provide a full-time supervisor as a replacement. A contract employee shall not hold the position of detention officer and supervisory detention officer simultaneously. The COR will document and refer to the CO the failure of the Contractor to provide necessary personnel to cover positions.

DRAFT

18. Post Relief

As indicated in the post orders, the detention officer shall not leave his or her post until relieved by another detention officer. The Contractor or Contractor's supervisor authorizes rest or relief periods; the Contractor shall assign undesignated officers to perform the duties of the detention officers on break.

19. General Training Requirements

All officers must have the training described in the ACA Standards and in this sub-section. The Contractor shall provide the required refresher courses or have an institution acceptable to the COR to provide the training. Failure of any employee to complete training successfully is enough reason to disqualify him or her from duty.

All new detention officers will receive 60 hours of basic training, not including firearms, prior to EOD and 40 hours of on-the-job training. The Contractor's training officer will be responsible for administering an on-the-job training (OJT) program for new employees. A senior detention officer, during the 40-hour OJT period, must always accompany the detention officers. The Contractor shall provide a copy of the documentation to the COR upon successful completion of the employees' on-the-job training.

In addition, after completion of the first 100 hours of training, the Contractor has 60 days to complete an additional 40 hours of training for each employee. During the remainder of the first year on duty, the Contractor shall provide the employee with an additional 40 hours of training for a total of 180 hours within the first year of employment. The training program must directly relate to the employee's assigned position and afford application of necessary job skills.

Detention officers shall not perform duties under this contract until they have successfully completed all initial training, and the COR receives a written certification from the Contractor. Alternative or e-training techniques, unless approved in writing by the CO via the COR, shall not be used.

20. Basic Training Subjects

Officers must complete the training required in accordance with the ACA and NDS 2026. The required training may include but is not limited to the following:

In-service Orientation	2 HRS
Counseling Techniques/Suicide Prevention and Intervention*	2 HRS
Conduct/Duties/Ethics and Courtroom Demeanor	2 HRS
Bomb Defense and Threats	1 HR
Telephone Communications/Radio Procedures	1 HR
Annual IT Security Training	1 HR
Fire and other Emergency Procedures	2 HRS

DRAFT

Treatment and Supervision of Aliens	2 HRS
ICE, Use of Force Policy	2 HRS
Security Methods/Key Control/Count	1 HR
Procedures/Observational Techniques	4 HRS
Sexual Harassment	2 HRS
Alien Escort Techniques	1 HR
ICE Paperwork/Report Writing	2 HRS
Alien Searches/Alien Personal Property	4 HRS
Property/Contraband	2 HRS
Alien Rules and Regulations	2 HRS
First Aid*	4 HRS
Cardiopulmonary Resuscitation (CPR)*	4 HRS
Blood-borne Pathogens*	2 HRS
Self Defense	8 HRS
Use of Restraints	5 HRS
Firearms Training**	
Sexual Abuse/Assault Prevention and Intervention*	2 HRS
ICE 2026 National Detention Standards	2 HRS
Disability Accommodations	1 HR
Language Access and Effective Communications	1HR
Cultural Competency	1HR

All training shall be conducted in a classroom or on-the-job training environment and shall be in accordance with the ACA Standards and NDS 2026. Online training is specifically prohibited to meet these requirements, unless approved in writing by the COR.

** Critical training subjects*

*** Firearm training for detention officers who are required to provide Armed Transportation shall be in accordance with state licensing requirements. The Contractor shall certify proficiency in accordance with state requirements.*

21. Refresher Training

DRAFT

Annually the Contractor shall conduct 40 hours of refresher training for all detention officers including supervisory detention officers. Refresher training shall consist of the critical subjects listed above and a review of basic training subjects and others as approved by ICE.

The Contractor shall coordinate recertification in CPR and first aid as required. Annually, upon completion, the Contractor shall provide documentation of refresher training to the COR.

In addition to the refresher training requirements for all detention officers, supervisors must receive refresher training relating to supervisory duties.

22. On-the-job Training

After completion of the minimum of 60 hours basic training, all detention officers will receive an additional 40 hours of on-the-job training at specific post positions.

This training includes:

- Authority of supervisors and organizational code of conduct.
- General information and special orders.
- Security systems operational procedures.
- Federal facility self-protection plan or emergency operational procedures.
- Disturbance Control Team training.

23. Training during Initial 60 Day Period

The Contractor shall provide an additional 40 hours of training for detention officers within 60 days after completion of the first 100 hours of training. The Contractor shall provide the training format and subjects, for approval by the COR and/or CO, prior to the commencement of training.

24. Basic First Aid and CPR Training

All Contractor employees shall be trained in basic first aid and CPR. They must be able to:

a. Respond to emergency situations within four minutes.

b. Perform CPR.

c. Recognize warning signs of impending medical emergencies.

d. Know how to obtain medical assistance.

e. Recognize signs and symptoms of mental illness.

f. Administer medication.

DRAFT

g. Know the universal precautions for protection against blood-borne diseases.

25. Supervisory Training

All new supervisory detention officers assigned to perform the work under this contract must successfully complete a minimum of 40 hours of formal supervisory training provided by the Contractor prior to assuming duties. This training is in addition to mandatory training requirements for detention officers. Supervisory training shall include the following management areas:

Techniques for issuing written and verbal orders	2 HRS Uniform
Clothing and grooming standards	1 HR Security
Post inspection procedures	2 HRS
Employee motivation	1 HR
Scheduling and overtime controls	2 HRS
Managerial public relations	4 HRS
Supervision of aliens	4 HRS
Other company policies	4 HRS
Non-violent Crisis Intervention	8 HRS
ICE 2026 National Detention Standards	12 HRS

26. Proficiency Testing

The Contractor shall give a written examination following each training class to display proficiency. To pass any examination, employees must achieve a minimum of 80 percent. Should an employee fail the written test on the initial attempt, the employee shall be given additional training and be given one additional opportunity to retake the test. If the employee fails the second attempt, the Contractor shall remove the employee from the contract.

27. Certified Instructors

Certified instructors shall conduct all instruction and testing. A state or nationally recognized institution shall certify instructors unless otherwise approved in writing by

the COR. Certifications of instructors may be established by documentation of experience in teaching positions or by successful completion of a course of training for qualifying personnel as instructors. The COR must approve the instructor prior to the training course.

28. Training Documentation

The Contractor shall submit a training forecast and lesson plans to the COR and ICE official at least 30 days prior to all training. The training forecast shall provide date, time, and location of scheduled training and afford the COR observation/evaluation opportunity.

DRAFT

The Contractor shall certify and submit the training hours, type of training, date and location of training, and name of the instructor monthly for each employee to the COR and ICE official.

29. Uniforms

The contractor shall provide uniforms to its employees, such as khaki pants and polo shirts. The design and color of the contractor's uniforms shall not be like those worn by ICE officers. All officers performing under this contract shall wear uniforms of the same style and color while on duty. Supervisory personnel should wear different color shirts to distinguish them from line staff. Each officer shall wear an identification nametag over the right breast shirt pocket. Uniforms and equipment do not have to be new but shall be in good condition and meet the standards at the start of duty. Officers who are not in proper uniform shall be considered "not ready for duty/not on duty" until properly uniformed. All uniforms shall be clean, neat, and in good order.

The complete uniform consists of seasonal attire that includes appropriate shirts, pants, belt (mandatory), cap (mandatory), jacket, shoes or boots (mandatory), duty belt, mini-mag flashlight and holder, handheld radio, and key-holder. The contractor shall ensure that each officer has a complete uniform.

Prior to the agreement's performance date, the contractor shall document to the COR, the uniform and equipment items that have been issued to each employee. The COR shall have the right to approve or disapprove any uniform apparel.

30. Identification Credentials

The Contractor shall ensure that all employees, both uniformed and non-uniformed (if applicable), have the required identification credentials in their possession while on the premises. The Contractor identification credential document shall contain the following:

a. A photograph that is at least one-inch square that shows the full face and shoulders of the employee and is no more than 30 days old when the credential is issued.

b. A printed document that contains personal data and description consisting of the employee's name, sex, birth date, height, and eye color, as well as the date of issuance, the signature of the employee, and the signature of project manager or designated Contractor personnel.

c. To avoid the appearance of having government issued badges, the Contractor shall not possess wallet type badges or credentials. All credentials shall be approved by the COR or other ICE officials.

31. Permits and Licenses

The Contractor shall ensure each employee has registrations, commissions, permits, and licenses as required by the district, municipality, county, and state in which ICE work site is performed prior to Entry on Duty (EOD). The Contractor shall verify all licenses and certifications. If applicable, all Contractor staff shall possess a current license/registration, in

DRAFT

the state in which they are practicing.

32. Jurisdiction

The Contractor's authority under this contract is limited to space or posts that are under the charge and control of ICE. The Contractor shall not extend its services into any other areas.

33. Encroachment

Contractor employees shall not have access to government equipment, documents, materials, or telephones for any purpose other than as authorized by ICE. Contractor employees shall not enter any restricted areas of the detention centers unless necessary for the performance of their duties.

34. Work Schedules

The Contractor shall follow the criteria described below when establishing work schedules, contract relief, rest periods, and starting and stopping work.

35. Post Work Schedules

One week in advance, the Contractor shall prepare supervisory and detention officer work schedules, for a two-week period, and shall post them in work areas or locker rooms. A manpower report shall be submitted to the COR monthly. Schedules shall be prepared on a form designated by ICE. Changes in duty hours shall also be posted on this form in enough time to ensure 24-hour advance notice. At the completion of each shift, the Contractor shall, upon request of the COR, also provide an employment report listing (copies of the sign-in sheets [GSA Form 139, Record of Arrival and Departure from Buildings during Security Hours, or approved equivalent Record of Arrival and Departure from Buildings during Security Hours] for each shift) for each employee who actually worked, work classification, post assignments, and hours worked, as well as total hours worked by supervisory and non-supervisory employees. A supervisor shall conduct regular post checks to ensure personnel are on duty. When a contract employee is not being utilized at a given post, the Contractor at the direction of the COR and ICE supervisor on duty may reassign him/her to another post.

36. Starting and Stopping Work

The Contractor is responsible for all employees to be in complete uniform and ready to begin work promptly at the beginning of each shift. Each employee shall remain at the duty locations until the shift is completed.

i. Recording Presence

1. The Contractor shall direct its employees to sign in when reporting for work and to sign out when leaving at the end of their period of duty. The Contractor's supervisory and regular personnel are required to register at the applicable work site(s) and shall use a timekeeping system. The government shall specify the registration points, which will be at the protected premises, and the Contractor shall utilize those points for this purpose.

ii. Rest Periods

1. When the Contractor or a Contractor supervisor authorizes rest and relief periods for the contract employees, a substitute officer shall be assigned to the duty location.

iii. Work Relief

1. When the work assignments require that the Contractor's employees do not leave the assigned duty locations until a substitute officer has provided relief, this condition shall be explicitly stated on GSA Form 2580 (Attachment 17), Guard Post Assignment Record, or other forms designated by the COR. The Contractor shall enforce the procedure without exceptions.

61. Health and Medical Care Policies

The Contractor shall comply with written policies and procedures for appropriately addressing the health needs of aliens in ICE custody. Written policies and procedures shall include, but not be limited to, the following:

- Policies and procedures for prompt summoning of emergency medical personnel.
- Policies and procedures for evacuation of aliens, if deemed necessary by qualified medical personnel.
- Policies, procedures, and post procedures for duty officers to ensure that medical emergencies are recognized and promptly attended to.

62. Federal Facility Requirements for Infectious Disease Screening

The Contractor will ensure that there is adequate space and equipment to provide medical intake screening, including TB screening within the intake processing area.

63. Airborne Precautions

In order to prevent the spread of airborne infectious disease or cross contamination of zones within the federal facility, the HVAC system in the intake screening area shall be designed to exhaust to the exterior and prevent air exchange between the intake screening area and any other area within the federal facility (see CDC guidelines: Tuberculosis (TB) | Tuberculosis (TB) | CDC

64. Required Administration and Management Services

1. **Manage** the Receiving and Discharge of Aliens

During the admissions process, aliens must undergo screening for medical purposes, have their files reviewed for classification purposes, submit to a standard body search, and are personally observed and certified regarding the examination, categorization, inventorying, and safeguarding of all personal belongings. This includes fingerprinting of aliens.

The Contractor shall ensure aliens are classified appropriately using objective criteria. Aliens will be classified upon arrival, before being admitted to the general population. The Contractor will periodically re-classify aliens, in accordance with the NDS 2026.

The Contractor may be required to access and utilize the ICE detention booking system to

properly book aliens in and out of ICE custody.

The Contractor shall effectuate departures. Effectuating departures require Contractor employees to perform alien-related activities including but not limited to positive identification, documentation preparation and review, provision of any sack lunches required, transportation, escorting and returning all DHS documentation to the appropriate ICE supervisor upon completing the escort assignment. In addition, Contractor employees shall, when required by proper authority, affirm, swear, and witness to all actions of effectuating departure that were accomplished, performed, carried out, and done, and in transactions involving the alien(s), when required in a legal setting, deposition, or court of law.

Aliens that are released should, prior to release, be given the opportunity to make a free phone call to arrange for pick up from the federal facility.

Aliens that are released shall be transported to a local airport, bus terminal, train station, or subway station prior to the time of the last departure at their destination, so the released individual would depart the same day, and not be required to spend time overnight in a transportation terminal. The time, point, and manner of release from a federal facility shall be consistent with safety considerations and consider special vulnerabilities.

If public transportation is within walking distance of the federal facility, aliens shall be provided with an information sheet that gives directions to and describes the types of transportation services available. However, the federal facility must provide transportation for any alien who is not reasonably able to walk due to age, disability, illness, mental health, or other vulnerability. In addition, the federal facility must provide transportation for any alien because of weather or other environmental conditions at the time of release that may endanger the safety of the alien.

If an alien resided in the local area near the federal facility prior to arrest and is released to the same local area upon release, they shall be provided with a list of shelter services available, along with directions to each shelter. ICE may provide the Contractor with national resource information to be distributed by the Contractor to aliens upon release. These include lists of resources such as national hotline information.

As practicable, aliens shall be provided with a laundered set of their own clothing, or one set of non-institutional clothing and footwear that is weather-appropriate for their destination.

2. Manage and Maintain a Commissary

A commissary shall be operated by the Contractor as a privilege to aliens who will have the opportunity to purchase from the commissary at least once per week. All items available at the commissary must be approved by the COR and ICE officials. The commissary inventory shall be provided to the COR upon request. Notice of any price increases must be provided to the COR. The Contractor may assess sales tax on the price of items if state sales tax is applicable.

Revenues shall be maintained in the federal facility commissary account and not commingled with any other funds. If funds are placed in an interest-bearing account, the interest earned shall be credited to the aliens. Any expenditure of funds from the account shall only be made

DRAFT

with the approval of the CO. Any revenues earned more than what is required for commissary operations shall be used solely to benefit aliens at the federal facility. Using these funds for any expense for which the Contractor is required to pay is prohibited. The Contractor shall provide independent auditor certification of the funds to the COR every 90 days.

At the end of the contract period, or as directed by the CO, a check for any profits remaining in this account associated with alien commissary purchases shall be made payable to the Treasury general trust fund. The Contractor shall coordinate with the COR to return funds as required.

Aliens are permitted to receive funds from outside sources (i.e., from family, friends, bank accounts). Outside funds or those generated from work may be used to pay for products and services from the commissary.

3. **Manage and Account for Alien Assets (Funds, Property)**
The Contractor is responsible for all alien personal property (i.e., stolen/misplaced goods due to Contractor negligence and/or mishandling of alien personal property). The Contractor shall have written policies and procedures in managing personal property. The safeguarding of personal property will include: the secure storage and return of funds, valuables, baggage, and other personal property; a procedure for documentation and receipting of surrendered property; and the initial and regularly scheduled inventories of all funds, valuables, and other property.

Written procedures shall be established for returning funds, valuables, and personal property to an alien being transferred or released that adheres to the requirements of ICE policy. The Contractor shall ensure that all aliens who are scheduled for either transfer or release are given all funds (in cash or check, whichever is deemed appropriate by the COR or designated ICE official) immediately prior to leaving the federal facility. Confiscated foreign currency funds are to be returned to the alien. This includes the out-processing of aliens on all removal flights. For such removal flights, the Contractor will provide all necessary items for removal processing.

The Contractor shall return or discard any unclaimed, undesired, or abandoned property to the last known address of the alien or his designated contact. The Contractor shall log all property returned or discarded, the address where the property was sent, and the date the property was shipped or destroyed. Property shall be checked at least once per month to ensure that there is not an excess of property left in the federal facility.

4. **Securely Operate the Federal Facility**
Staff responsible for lock maintenance shall receive training and be certified from a government approved training program specializing in the operation of locks and locking mechanisms.

The Contractor shall provide constant less than lethal armed perimeter surveillance of the federal facility. The federal facility shall have sufficient auxiliary power through generator or battery back-up to maintain secure operations.

DRAFT

5. **Establish and Maintain a Program for the Prevention of Sexual Abuse/Assault**
   The Contractor shall develop and implement a comprehensive sexual abuse/assault prevention and intervention program in accordance with NDS 2026, Standard 2.11, Sexual Abuse and Assault Prevention and Intervention, and all federal facility requirements of the DHS PREA (Standards to Prevent, Detect, and Respond to Sexual Abuse and Assault in Confinement Facilities, 79 Fed. Reg. 13100 (Mar. 7, 2014), as outlined in Attachment 11 – Prison Rape Elimination Act Regulations. This program shall include training and/or information that is given separately to both staff and aliens.

6. **Visitation**
   The federal facility's perimeter will ensure that aliens remain within, and that public access is denied without proper authorization. Visitation and/or tours of the federal facility shall be conducted in accordance with the relevant provisions of NDS 2026 or as directed by ICE. For the safety and privacy of the aliens, no videotaping or audio recording devices are permitted by visitors or others (including Contractor employees) within the secure perimeter without prior approval from ICE. This prohibition does not include approved closed-circuit television cameras operated by the Contractor or the government for security purposes.

7. **Manage Computer Equipment and Services in Accordance with all Operational Security Requirements**
   The Contractor shall comply with all federal security and privacy laws and regulations established to protect federal systems and data. The Contractor shall inform all personnel of the confidential nature of ICE alien information.

   The Contractor shall restrict access to data information pertaining to ICE aliens to authorized employees with the appropriate clearance who require this information in the course of their official duties. In accordance with the Freedom of Information/Privacy Act, the contractor shall not disclose information obtained pertaining to ICE detainees to a third party without written permission from the COR.

   The Contractor may not disclose information pertaining to ICE aliens to a third party without written permission from the COR.

   The Contractor shall develop a procedural system to identify and record unauthorized access or attempts to access ICE alien information. The Contractor shall notify the COR and ICE officials within four hours of a security incident.

8. **Non-Segregated Protective Custody Housing**
   The federal facility shall include at least one non-segregated (i.e., not a segregation housing unit) protective custody housing option for placing aliens who may benefit from a more supportive or specialized general population setting together by biological sex. This unit would be used as an alternative to prolonged placement in administrative segregation. The intended population for this housing option may include individuals who have been identified as having a vulnerability, at increased risk in detention, and/or who feel safer in a protective-custody-like setting (i.e., an alternative for those who request administrative segregation for protective custody reasons). The number of non-segregated protective custody housing

DRAFT

options should appropriately reflect the federal facility population, and at a minimum, include both male and female housing options (if the federal facility houses female population).

The federal facility will determine an alien's risk and appropriateness for non-segregated protective custody housing during intake or any time while the alien is in custody. Non-segregated protective custody housing unit(s) are in addition to segregation or medical housing.

Placement in non-segregated protective custody housing may be based on a range of factors, including but not limited to, request by an alien (in lieu of protective custody administrative segregation), behavioral health needs, cognitive impairments, age, disability, or other identified vulnerability. Non-segregated protective custody housing criteria should not be prescriptive but rather based on an individualized assessment of risk and vulnerability. Non-segregated protective custody housing will operate like a general population unit in terms of freedom of movement, and ICE detention standards for general housing will apply. Aliens in non-segregated protective custody housing will have equal access to all federal facility services and programming available to aliens in general population housing and shall not include any limitations not applied to the general population. Non-segregated protective custody housing units shall be staffed by federal facility personnel who should be trained in working with vulnerable populations and trauma-informed care. Staff-to-alien ratios are expected to be higher than in general population housing units to provide for heightened security and care. The housing unit personnel will provide additional assistance (as needed) to aliens, including an enhanced federal facility orientation in the alien's language on federal facility programs and services and how to use various communication mechanisms (i.e., paper forms/requests, telephones, and tablets, where available) to communicate with federal facility staff, ERO, and external parties such as family and legal representatives.

Additional programming applicable to the population in non-segregated protective custody housing units shall be offered. Non-segregated protective custody housing units shall include self-help materials and pro-social organized activities, including those which will assist with promoting a calm environment. The Contractor is expected to be knowledgeable in and implement effective programming for non-segregated protective custody housing units which are also responsive to the population's needs.

The federal facility shall maintain a multi-disciplinary team to oversee and manage placement in non-segregated protective custody housing units. The multi-disciplinary team may be the same group that conducts the weekly review of segregation placements but shall at least include behavioral health staff, custody staff, and a federal facility supervisor. Intake staff will identify and refer prospective candidates for the non-segregated protective custody housing unit to the multi-disciplinary team. Aliens may also request placement in non-segregated protective custody housing at any time while in the federal facility for consideration by the multi-disciplinary team. Monthly individualized assessments by the multi-disciplinary team will consider behavioral health and/or other factors which were the basis for placement in the non-segregated protective custody housing unit. The federal facility will document/track admissions to and departures from the non-segregated protective custody housing unit(s) and the reason for placement in and removal from the unit. A

DRAFT

minimum of two Contractor employees shall be assigned each shift to verify that the segregation paperwork has been completed properly and entered in the alien's segregation file. The employees shall also be responsible for gaining and maintaining access to eSRMS. All required documentation for the segregation population will be entered daily into eSRMS by Contractor employees.

Note: the Contractor must comply with the needs and requirements stated in U.S. ICE Policy 11065.1: Review of the Use of Segregation for ICE Detainees.

9. Collect and Disseminate Intelligence Information

Policies and procedures for collecting, analyzing, and disseminating intelligence information regarding issues affecting safety, security, and the orderly running of the federal facility shall be developed. This information shall include but not be limited to gang affiliations; domestic terrorist groups; tracking of aliens having advanced skills in areas of concern (locksmiths, gunsmiths, explosives, and computers, etc.); narcotics trafficking; mail and correspondences; alien financial information; alien telephone calls; visiting room activity; and actions of high-profile aliens. The Contractor shall share all intelligence information with the COR and ICE officials.

10. ICE Notifications

The Contractor shall immediately report all serious incidents as outlined in the detention standards to the field office director or designee and the COR. Serious incidents include, but are not limited to the following: activation of disturbance control team(s); civil disturbances/protests); staff uses of force including use of lethal and less-lethal force (includes aliens in restraints more than eight hours); assaults on staff/aliens resulting in injuries that require medical attention (does not include routine medical evaluation after the incident); fires; fights resulting in injuries requiring medical attention; full or partial lockdown of the federal facility; escape; weapons discharge; suicide attempts; publicity; adverse weather; fence damage; power outages; bomb threats; high profile alien cases admitted to a hospital; significant environmental problems that impact the federal facility operations; transportation accidents (e.g., airlift, bus) resulting in injuries, death or property damage; and sexual assaults.

Pursuant to ICE instructions, the Contractor shall counteract civil disturbances, attempts to commit espionage or sabotage, and other acts that adversely affect the normal site conditions, the security and safety of personnel, property, aliens, and the public.

65. Property Accountability

1. General

ICE IT Equipment: ICE shall provide and install IT equipment in office spaces for ICE personnel only, to include computer workstations and screens, printers, and fax machines. All infrastructure and cabling shall be provided by the contractor in accordance with the Attachment 12 – CDF Design Standards – ICE – OPLA - Structured Cable Plant Standard.

NOTE: ICE IT system must be a complete, independent, and physically separate system from the Contractor's IT system. The system shall serve all operational components including ICE and EOIR

DRAFT

The Contractor personnel shall not permit any government property to be taken away or removed from the premises. The Contractor shall enact practices to safeguard and protect government property against abuse, loss, or any other such incidents. Government property shall be used only for official business.

All government property furnished under this contract shall remain property of the government throughout the contract term. ICE shall maintain a written inventory of all government property issued to the Contractor for performance hereunder. Upon expiration or termination of this contract, the Contractor shall render a written account to the COR of all such property. The Contractor shall assume all risks and shall be responsible for any damage to, or loss of government furnished property used by Contractor employees. Normal wear and tear will be allowed.

The Contractor, upon expiration or termination of services, shall immediately transfer to the COR, all government property in its possession or in the possession of any individual or organization under its control, except as otherwise provided for in this contract. The Contractor shall cooperate fully in transferring property to the successor Contractor. The government shall withhold final payment until adjustments are made for any lost property.

2. **Use of Government Wireless Communication Devices**
All personnel that have been issued a federal government owned wireless communication device, including but not limited to, cellular telephones, pagers, or wireless Internet devices, are authorized to possess and use those items in all areas of the federal facility. Cellular, telephone, and wireless boosters shall be provided, installed, and maintained by the Contractor to ensure optimal service throughout the federal facility and ICE and/or DOJ administrative areas.

66. Firearms/Body Armor

1. Firearms Requirements
The Contractor shall provide well maintained and serviceable or new firearms and maintain enough licensed firearms and ammunition to equip each armed detention officer and armed supervisor(s) with a licensed weapon while on duty. Firearms may be re-issued to new employees throughout the life of the contract if the firearm is in a serviceable condition. See Attachment 14 – ICE Firearms and Use of Force Handbook.

Personal firearms shall not be used. A licensed gunsmith, in writing, shall certify all firearms safe and accurate.

Firearms shall be standard police service-type, semi-automatic capable of firing hollow-point ammunition that meets the recommendations of the firearms manufacturer.

Ammunition will be factory load only – no reloads. The Contractor shall adhere to the manufacturer's specifications regarding ammunition retention, e.g., ammunition shall be properly rotated, and older ammunition utilized prior to utilization of newer ammunition. All firearms shall be licensed by the State. Armed officers are required to obtain a class G license or equivalent, if required by the state.

The Contractor shall provide enough ammunition for each armed detention officer, including

uniformed contract supervisor(s) to be issued three full magazines.

The Contractor shall account for all firearms and ammunition daily. If any weapons or ammunition are missing from the inventory, the COR shall be notified immediately.

The Contractor shall provide a complete listing of licensed firearms by serial numbers and by each safe location to the COR prior to beginning performance under this contract.

Firearms shall be inspected. This shall be documented by the warden/federal facility director. Loading, unloading, and cleaning of the firearms shall only take place in designated areas. Firearms shall be carried with the safety on, if applicable, with a round in the chamber.

The Contractor shall maintain appropriate and ample supplies of firearms upkeep and maintenance equipment (cleaning solvents, lubricating oil, rods, brushes, patches, and other normal maintenance tools). The firearms shall be cleaned and oiled as appropriate to ensure optimum operating condition.

The Contractor shall obtain and maintain on file appropriate state and municipality permits and weapons permits for each officer.

A copy of this permit shall be provided to the COR at least three working days prior to the anticipated assignment date of any individual. The Contractor shall ensure that its employees always have all permits and licenses in their possession while in the performance of this contract.

The Contractor shall provide safes/vaults for storage of firearms and ammunition, for each location where firearms are issued or exchanged, which meet ICE requirements and are approved for the storage of firearms and ammunition. The COR is responsible for approving the proposed safes/vaults prior to usage. Contract supervisors and guards shall make accurate receipts and return entries on a Firearms and Equipment Control Register. Except when issuing or returning ammunition or firearms, each safe/vault shall always remain locked. The Contractor shall change the combination of each safe/vault at least once every six months, or more often if circumstances warrant.

The Contractor shall certify firearms training to the COR. The Contractor shall certify staff proficiency every quarter.

The Contractor shall provide an ICE approved intermediate weapon(s). The Contractor shall assign one or more Contractor staff to the positions of Ammunition Control Officer and Firearms Control Officer.

2. Body Armor Requirements

The Contractor shall provide body armor to all armed detention officers and armed supervisors. Body armor shall be worn while on armed duty. The body armor will meet all requirements set forth in the ICE Body Armor Policy. See Attachment 13 – ICE Body Armor Policy.

The Contractor shall procure replacement body armor if the body armor becomes unserviceable, ill-fitting, worn/damaged, or at the expiration of service life.

DRAFT

All armed detention officers and armed supervisors need to be made aware of the health risks associated with the wearing of body armor in high heat/high humidity conditions and/or during strenuous exertion. When detention officers and supervisors are required to wear body armor, they shall be provided with opportunities to rehydrate and remove the body armor as necessary.

The use of personally owned body armor is not authorized.

Additional Equipment: The Contractor shall provide the following equipment for each officer performing services under this contract: Metal handcuffs and a handcuff carrying case.

Handcuffs should be equal to or better than the basic Smith & Wesson brand. One mini-mag or comparable size, operational flashlight with batteries and a belt holder.

Inclement weather apparel appropriate to local conditions. Fully operational protection equipment that meets universal protection requirements. This includes but is not limited to gloves, face masks, ear, and eye protection. Hand restraints, leg restraints and belly chains. All operational protection equipment shall be replaced by the Contractor as items begin to show wear and tear.

3. Records Management

The Contractor will 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 hard copy 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.

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 CO or COR. 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 CO or COR to ensure any such destruction follows the governing NARA records control schedule. The agency owns the rights to all information and records produced as part of this contract.

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.

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.

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.

No disposition of documents will be allowed without the prior written consent of the CO. 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.

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.

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 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)

- 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.

- 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). 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.

- A point of contact for addressing recordkeeping issues and rectifying any discrepancies noted during a records assessment and/or inspection

DRAFT

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

67. Personnel Background Security Requirements

1. General

ICE has determined that the performance of the tasks as described in this contract requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor) have access to sensitive DHS information, and that the Contractor will adhere to the following.

2. Contractor Employee Fitness Screening

Screening criteria under DHS Instruction 121-01-007, Revision 2, dated August 10, 2024, Personnel Security, Suitability and Fitness Program, dated June 14, 2017, or successor thereto, and Title 5, CFR part 731, dated December 18, 2024, that may exclude Contractor employees from consideration to perform under this agreement includes:

a. Misconduct or negligence in employment.

b. Criminal conduct.

c. Material, intentional false statement or deception of fraud in examination or appointment.

d. Dishonest conduct.

e. Excessive alcohol use, without evidence of rehabilitation, of a nature and duration that suggests that the applicant or appointee would be prevented from performing the duties of the position in question or would constitute a direct threat to the property or safety of the applicant or appointee or others.

f. Illegal use of narcotics, drugs, or other controlled substances, without evidence of substantial rehabilitation.

g. Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force.

h. Any statutory or regulatory bar which prevents the lawful employment of the person involved in the position in question (for Excepted Service employees).

i. Violent conduct; and

j. Any other nondiscriminatory reason that an individual's employment (or work on a contract) would not protect the integrity or promote the efficiency of the service.

Screening criteria under 6 CFR § 115.117 (Sexual Abuse and Assault Prevention Standards) implemented pursuant to Public Law 108-79 (DHS PREA Standards) or successor thereto, that WILL exclude Contractor employees from consideration to perform under this agreement includes:

DRAFT

a. Engaged in Sexual Abuse in a Prison, Jail, Holding facility, Community Confinement facility, Juvenile facility, or other Institution as defined under 42 USC 1997.

b. Convicted of engaging or attempting to engage in sexual activity facilitated by force, overt or implied threats of force, or coercion, or if the victim did not consent or was unable to consent or refuse.

c. Civilly or administratively adjudicated to having engaged in such activity.

Subject to existing law, regulations and/or other provisions of this Agreement, undocumented aliens shall not be employed by the Contractor.

3. Position Designation

In accordance with Title 5, CFR part 731, dated December 18, 2024, and 5 CFR 1400. Agencies are required to designate position risk and sensitivity level for all Contractor employees to determine the commensurate level of background investigation. The public trust risk in a position is the assessment of the degree of potential damage to the efficiency or integrity of the service that could arise from misconduct by the incumbent in the position. Therefore, once the contract is awarded and before the vendor starts submitting personnel for security vetting, the Contractor will provide, through the CORs, a list of all positions, to include titles and specific description of the duties for each of positions assigned to support the contract.

4. Preliminary Fitness Determination

ICE will exercise full control over granting, denying, withholding or terminating unescorted government federal facility and/or sensitive Government information access for Contractor applicants/employees, based upon the results of a Fitness screening process. ICE may, as it deems appropriate, authorize and make a favorable expedited preliminary Fitness determination based on preliminary security checks. The preliminary Fitness determination will allow the Contractor employee to commence work temporarily prior to the completion of a Full Field Background Investigation. The granting of a favorable preliminary Fitness shall not be considered as assurance that a favorable final Fitness determination will follow as a result thereof. The granting of preliminary Fitness or final Fitness shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by ICE, at any time during the term of the contract. No employee of the Contractor shall be allowed to enter on duty and/or access sensitive information or systems without a favorable preliminary Fitness determination by OPR PSD. No employee of the Contractor shall be allowed unescorted access to a federal Government facility without a favorable preliminary Fitness determination by OPR PSD. Contract employees are processed under 5 CFR 731 dated December 18, 2024, and DHS Instruction 121-01-007, Revision 2, dated August 10, 2024, or successors thereto; those having direct contact with Detainees will also have 6 CFR § 115.117 considerations made as part of the Fitness screening process. Sexual Abuse and Assault Prevention Standards implemented pursuant to Public Law 108-79 (DHS PREA Standards).

5. Background Investigation

Contractor employees (to include applicants, temporary, part-time and replacement

DRAFT

employees) under the contract, needing access to sensitive information and/or ICE Detainees, shall undergo a position sensitivity analysis based on the duties everyone will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. Background investigations will be processed through OPR PSD. Contractor applicants/employees are nominated by a Contracting Officer Representative (COR)

for consideration to support this contract via submission of the DHS Form 11000-25 and ICE Supplement to the DHS Form 11000-25 to OPR PSD. This contract shall submit the following security vetting documentation to OPR PSD, through the COR, within 10 days of notification of initiation of an Electronic Application for Background Investigations (eAPP), or successor thereto, in the Office of Personnel Management (OPM) automated on-line system:

- Standard Form 85P (Standard Form 85PS (with supplement to 85P required for those with direct contact with detainees or armed positions)), "Questionnaire for Public Trust Positions" form completed online and archived by the Contractor applicant/employee in their NBIS eAPP account.

- Signature Release Forms (Three total) generated by NBIS eAPP upon completion of Questionnaire (e-signature recommended/acceptable). Completed online and archived by the Contractor applicant/employee in their NBIS eAPP account.

- Electronic fingerprints taken at an approved federal facility **OR** two (2) SF 87 Fingerprint Cards (current revision) sent to OPR PSD. Additional information regarding fingerprints will be sent to the Contractor applicant/employee from OPR PSD.

- Optional Form 306 Declaration for Federal Employment. This document is sent as an attachment in an e-mail to the Contractor applicant/employee from OPR PSD.

- Social Security Administration 89 form (SSA-89): Authorization for the Social Security Administration (SSA) to Release Social Security Number (SSN) Verification. This document is sent as an attachment in an e-mail to the Contractor applicant/employee from OPR PSD.

- If occupying PREA designated position: Questionnaire regarding conduct defined under 6 CFR § 115.117 (Sexual Abuse and Assault Prevention Standards). This document is sent as an attachment in an e-mail to the Contractor applicant/employee from OPR PSD.

- One additional document may be applicable if the Contractor applicant/employee was born abroad. If applicable, the document will be sent as an attachment in an e-mail to OPR PSD from the Contractor applicant/employee.

Contractor employees who have an adequate, current investigation by another Federal Agency may not be required to submit complete security packages; the investigation may be accepted under transfer of trust. The questionnaire related to 6 CFR § 115.117 listed above in item 5 will be required for positions designated under PREA. OPR PSD will determine if personnel

DRAFT

meet transfer of trust requirements at the initial stage of processing and prior to requesting a new security questionnaire.

With respect to break-in-service requirements for transfer of trust, OPM removed the 24-month break-in-service provision. This requirement is replaced with a new process, established in the Federal Personnel Vetting Investigative Standards issued by the Suitability, Credentialing, and Security Executive Agents, which expands this window of time up to sixty months using a tiered, risk-based approach of graduated levels of investigation.

IAW 5 CFR 731 and E.O. 13764, the fixed five-year periodic reinvestigation for public trust positions and national security positions will soon be eliminated and only once personnel are enrolled in a continuous vetting program. Therefore, PSD will continue the reinvestigation process until this process is completed.

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

To ensure adequate background investigative coverage, Contractor applicants/employees must currently reside in the United States or its Territories. Additionally, Contractor applicants/employees are required to have resided within the United States or its Territories for three or more years out of the last five (ICE retains the right to deem a Contractor applicant/employee ineligible due to insufficient background coverage). This timeline is assessed based on the signature date of the standard form questionnaire submitted for the applied position. Contractor employees falling under the following situations may be exempt from the residency requirement: 1) work or worked for the U.S. Government in foreign countries in federal civilian or military capacities; 2) were or are dependents accompanying a federal civilian or a military employee serving in foreign countries so long as they were or are authorized by the U.S. Government to accompany their federal civilian or military sponsor in the foreign location; 3) worked as a Contractor employee, volunteer, consultant or intern on behalf of the federal government overseas, where stateside coverage can be obtained to complete the background investigation; 4) studied abroad at a U.S. affiliated college or university; or 5) have a current and adequate background investigation (commensurate with the position risk/sensitivity levels) completed for a federal or Contractor employee position, barring any break in federal employment or federal sponsorship.

Only U.S. citizens and Legal Permanent Residents are eligible for employment on contracts requiring access to DHS sensitive information unless an exception is granted as outlined under DHS Instruction 121-01-007, Revision 2, dated August 10, 2024. Per DHS Sensitive Systems Policy Directive 4300A, only U.S. citizens are eligible for positions requiring access to DHS Information Technology (IT) systems or positions that are involved in the development, operation, management, or maintenance of DHS IT systems, unless an exception is granted as outlined under DHS Instruction 121-01-007, Revision 2, dated August 10, 2024.

6. **Continued Eligibility**

ICE will exercise full control over granting, denying, and/or restricting federal facility and

DRAFT

information access of any Contractor employee whose actions conflict with Fitness standards contained in 5 CFR 731 and DHS Instruction 121-01-007, Revision 2, dated August 10, 2024, or who violate standards of conduct under 6 CFR § 115.117. The Contracting Officer or their representative can determine if a risk of compromising sensitive Government information exists or if the efficiency of service is at risk and may direct immediate removal of a Contractor employee from contract support.

The Federal Government is transitioning to Trusted Workforce (TW) 2.0. TW 2.0 is a whole-of-government background investigation reform effort overhauling the personnel vetting process by creating a government-wide system that allows transfer of trust across organizations. All Contractor employees will be subjected to the transition and will be enrolled into a continuous vetting system. Enrollment will include multiple requirements from all personnel and potential changes to processes, procedures, and systems. This contract will comply with all requirements that facilitate the mandated transition to TW 2.0.

OPR PSD will evaluate concerns received via multiple sources under the continuous vetting process, to evaluate continued Fitness of Contractor employees. If concerns cannot be mitigated, the Contractor will be removed from the ICE contract upon notification from OPR PSD.

7. Required Reports

The Contractor will notify OPR PSD, via the COR providing an ICE Form 50-005, Contractor Employee Separation Clearance Checklist, of all terminations/resignations of Contractor employees under the contract within five days of occurrence to the ICEDepartureNotification@ice.dhs.gov group box.

The Contractor will return any expired ICE issued identification cards and building passes of terminated/resigned employees to the COR. If an identification card or building pass is not available to be returned, a report must be submitted to the COR referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card. The COR will return the identification cards and building passes to the responsible ID Unit. IAW DHS Instruction 121-01-007, Revision 2, dated August 10, 2024, the Contracting Officer's Representatives (CORs) notify the servicing personnel and industrial security offices when a Contractor employee is no longer working for DHS on any contract and report any derogatory information concerning the individual immediately, in accordance with the contract requirements. Report this information to PSD-CEP-REPORTING@ice.dhs.gov. The report should include
the Contractor employees' name and social security number, along with the adverse information being reported. The Contractor will provide, through the COR, a Quarterly Report (on a Microsoft Excel Spreadsheet) containing the names of Contractor employees who are actively serving on their contract. The list shall include the Name, Position and SSN (Last Four) and should be derived from system(s) used for Contractor payroll/voucher processing to ensure accuracy. This list is what ICE Industrial Security uses to reconcile the contract quarterly. CORs will submit reports to PSD-Industrial-Security@ice.dhs.gov no later than the 10th day of each January, April, July and October.

Contractors, who are involved with management and/or use of information/data deemed "sensitive" to include 'law enforcement sensitive" are required to complete the DHS Form 11000-6-Sensitive but Unclassified Information Non-Disclosure Agreement (NDA) for Contractor employee access to sensitive information. The NDA will be administered by the COR to all contract personnel within 10 calendar days of the entry on duty date. The completed form shall remain on file with the COR for the purpose of administration and inspection.

Sensitive information as defined under the Computer Security Act of 1987, Public Law 100-235 is information not otherwise categorized by statute or regulation that if disclosed could have an adverse impact on the welfare or privacy of individuals or on the welfare or conduct of Federal programs or other programs or operations essential to the national interest. Examples of sensitive information include personal data such as Social Security numbers; trade secrets; system vulnerability information; pre-solicitation procurement documents, such as statements of work; and information pertaining to law enforcement investigative methods; similarly, detailed reports related to computer security deficiencies in internal controls are also sensitive information because of the potential damage that could be caused by the misuse of this information. All sensitive information must be protected from loss, misuse, modification, and unauthorized access in accordance with DHS Management Directive 11042.1, *DHS Policy for Sensitive Information* and ICE Policy 4003, *Safeguarding Law Enforcement Sensitive Information*."

Any unauthorized disclosure of information should be reported to ICE.ADSEC@ice.dhs.gov.

68. Security Management

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

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

1. **Information Technology Security**

When sensitive government information is processed on Department telecommunications and automated information systems, the contract company agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data as outlined in DHS MD 4300.1*, Information Technology Systems Security* (or its replacement). Contractor employees must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractor employees who fail to comply with Department security policy are subject to having access to Department IT systems and facilities terminated, regardless of if the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy

Act).

2. **Information Technology Security Training and Oversight**
In accordance with the Office of the Chief Information Officer (OCIO) requirements and provisions, all Contractor employees accessing Department IT systems or processing DHS sensitive data via an IT system will require an ICE issued/provisioned Personal Identity Verification (PIV) card. Additionally, Cybersecurity Awareness Training (CSAT) will be required upon initial access and annually thereafter. CSAT training will be provided by the appropriate component agency of DHS.

Contractor employees, who are involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of the Department, shall receive periodic training at least annually in security awareness and accepted security practices, systems rules of behavior, to include Unauthorized Disclosure Training, available on the ICE Training System (ITS) or by contacting ICE.ADSEC@ice.dhs.gov. Contractor employees with significant security responsibilities shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

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

69. Data Ownership Contract Requirements

1. Accessibility of Government-owned Data
All stored program data associated with this acquisition shall be owned by the Government. As such, it will 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 resources, 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:

DRAFT

a. Program data is stored by Contractor personnel

b. Program data is stored by software that is managed, developed, or used by the Contractor

c. Program data is stored in a repository that is managed, developed, or used by the Contractor

2. Minimum Data Access Capability

a. 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.

b. Data access can occur by various means, if 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.

c. 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.

d. The Contractor shall provide the means for the Government to interpret accessible Program Data as follows:

e. 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.

f. 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.

g. 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.

h. Program data delivered to the Government shall conform to the Government approved definition for each data element and grouping of data elements.

i. All data accessible by the Government shall be both machine readable and human-readable in plain text.

j. 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

DRAFT

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 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.

70. Transition

1. **Transition-**In
The Contractor shall be responsible for the transition of all activities identified in this Performance Work Statement (PWS). The Contractor's transition-in shall be accomplished as expeditiously as possible, with a maximum transition-in period of 60 days after the contract award. The transition-in process shall not adversely impact the work being done by the outgoing Contractor. It shall be conducted in a manner consistent with safe operation requirements. The Contractor shall submit a final transition-in plan for approval by the COR within two (2) weeks after the award reflecting input from the COR as well as all necessary activities to facilitate the transition of services to the Contractor and expected completion dates of those activities. All activities must be completed during transition periods. The transition-in plan shall address, at a minimum, the following areas:

- Inventory and orderly transfer of all government equipment and property, if applicable.
- Transfer of documentation.
- Transfer of current project activities.
- Workplace logistics and staffing plan: Identification of the key personnel transition team members by name, position, EOD, clearance, start date, and responsibilities.
- Coordination of knowledge transfer sessions with the incumbent Contractor.
- Favorable EOD for all Contractor staff from the ICE PSD.
- Coordination of transition with COR and local field office.
- Any additional information required by other clauses contained in this contract.

DRAFT

The transition-in plan shall be approved by the COR and describe the Contractor's process for transitioning from the incumbent with no disruption in operational services.

2. **Transition-Out**

The Contractor shall be responsible for the transition-out of all technical activities identified in this PWS during the final, awarded period of performance. The Contractor shall submit the transition-out plan two (2) months prior to the completion of the period of performance of this contract. The Contractor's transition-out plan shall be approved by the COR. The Contractor shall complete the transition by the end of the period of performance of this contract. The transition-out plan shall address, at a minimum, the following areas:

a. Inventory and orderly transfer of all government equipment and property, if applicable. Briefing on all in-progress and committed items.

b. Any additional information required by other clauses contained in this contract.

The Contractor shall fully support the transition of all requirements to any successor to ensure no disruption in operational services.

71. Glossary

ADMINISTRATIVE SEGREGATION: A non-punitive form of separation from the general population for administrative reasons. Authorized only as necessary to ensure the safety of the detainee, federal facility staff, and other detainees; the protection of property; or the security or good order of the federal facility, and therefore should be for the briefest term and under the least restrictive conditions practicable, consistent with the rationale for placement. Generally, detainees in administrative segregation shall receive the same privileges as detainees housed in the general population, consistent with safety and security concerns. Administrative segregation may be necessary for, among other reasons, detainees requiring or requesting protective custody from others who may be likely to harm them; detainees awaiting an investigation or hearing for a violation of federal facility rules; detainees scheduled for release, removal, or transfer within 24 hours; or detainees presenting a clear threat to the security of the federal facility.

ADULT LOCAL DETENTION FACILITY (ALDF): A federal facility which detains people over the age of 18.

AMERICAN CORRECTIONAL ASSOCIATION (ACA): The American Correctional Association is the oldest and largest international correctional association in the world. ACA serves all disciplines within the corrections profession and is dedicated to excellence in every aspect of the field.

BED-DAY: The total billable cost to the government to maintain and house one alien for one day. Bed- day means an alien that is referred to a Contractor for detention. The bed days are calculated by subtracting the date booked into custody from the date released from custody. The Contractor may charge for the day of arrival, but not the day of departure.

BED-DAY RATE: The rate charged for each individual alien per day. Bed-day rate is an all-inclusive burdened rate including direct costs, indirect costs, overhead, and profit necessary to provide the detention, and food service requirements as described in the PWS. BOOKING: A procedure for the

admission of an Immigration and Customs Enforcement (ICE) alien, which includes searching, fingerprinting, photographing, medical screening, and collecting personal history data. Booking also includes the inventory and storage of the individual's accompanying personal property. The Contractor may be responsible for booking the alien into ICE systems upon receiving the alien.

BUREAU OF PRISONS (BOP): The U.S. Federal Bureau of Prisons protects society by confining offenders in the controlled environments of prisons and community-based facilities that are safe, humane, cost-efficient, and appropriately secure, and that provide work and other self-improvement opportunities to assist offenders in becoming law-abiding citizens.

CATEGORICAL EXCLUSION (CATEX): Activities that do not need to undergo detailed environmental analysis in an Environmental Assessment (EA) or Environmental Impact Statement (EIS) because the activities have been determined to normally not have the potential, individually or cumulatively, to have a significant effect on the human environment.

CLASSIFICATION: A process for determining the needs and requirements of aliens for whom detention has been ordered and for assigning them to housing units and programs according to their needs, security risk level, and existing resources of the federal facility.

CONTRABAND: Items that pose a threat to the security of people or property. A contraband item fits into either the category of hard or soft contraband as defined below:

- Hard Contraband: Any item that is inherently dangerous as a weapon or tool of violence, e.g., knife, explosives, "zipgun," brass knuckles. Because hard contraband presents an immediate physical threat in or to the federal facility, an alien found in possession of hard contraband could face disciplinary action or criminal prosecution.
- Soft Contraband: Any item that presents a nuisance, which does not pose a direct and immediate threat to an individual's safety. None-the-less, soft contraband has the potential to create dangerous or unsanitary conditions in the federal facility, such as excess papers that create a fire hazard, food items that are spoiled or retained beyond the point of safe consumption, etc.

CONTRACTING OFFICER (CO): An employee of the government responsible for the complete conduct and integrity of the contracting process, including administration after award. The only individual authorized to issue changes to this contract.

CONTRACTING OFFICER'S REPRESENTATIVE (COR): Employees of the government responsible for monitoring all technical aspects and assisting in administering the contract.

CONTRACTOR: The entity which provides the services described in this PWS.

CONTRACTOR EMPLOYEE: An employee of a private Contractor hired to perform a variety of detailed services under this contract.

CONTROL ROOM: Integrates all internal and external security communications networks within a secure room. Activities conducted within the control room have a critical impact on the institution's orderly and secure operation.

DRAFT

CREDENTIALS: Document providing primary source verification including education, training, licensure, experience, board certification, and expertise of an employee.

DEPARTMENT OF HOMELAND SECURITY (DHS): A department of the U.S. government, which includes ICE.

DEPARTMENT OF JUSTICE (DOJ): A department of the U.S government, which includes the Executive Office of Immigration Review (EOIR), the Federal Bureau of Investigation (FBI), the federal BOP, and the U.S. Marshals Service (USMS).

DESIGNATED SERVICE OFFICIAL: An employee of ICE designated in writing by ERO FOD to represent ICE on matters pertaining to the operation of the federal facility.

DETAINEE: Any person confined under the auspices and the authority of any Federal agency. Many of those being detained may have substantial and varied criminal histories.

DETAINEE RECORDS: Information concerning the individual's personal, criminal, and medical history, behavior, and activities while in custody, including, but not limited to:

- Alien, Personal Property
- Receipts, Visitors List, Photographs
- Fingerprints, Disciplinary Infractions
- Actions Taken, Grievance Reports, Medical
- Records, Work Assignments, Program Participation
- Miscellaneous Correspondence, etc.

DETENTION OFFICERS: Contractor's uniformed staff members responsible for the security, care, transportation, and supervision of aliens during all phases of activity in a detention federal facility. The officer is also responsible for the safety and security of the federal facility.

DETENTION OVERSIGHT UNIT (DOU): The purpose of the DOU is to develop and prescribe policies, standards, and procedures for ICE detention operations and to ensure detention facilities are operated in safe, secure, and humane condition for both aliens and staff.

DIRECT SUPERVISION: A method of alien management that ensures continuing direct contact between aliens and staff by posting an officer(s) inside each housing unit. Officers in general housing units are not separated from aliens by a physical barrier. Officers provide frequent, non-scheduled observation of and personal interaction with aliens.

DIRECTIVE: A document issued by the U.S. government and signed by the President, Departmental Secretary, or an Assistant Secretary that establishes policy, delegates' authority, and/or assigns responsibilities.

DISCIPLINARY SEGREGATION: A punitive form of separation from the general population for

DRAFT

disciplinary reasons. Authorized only pursuant to the order of a federal facility disciplinary panel, following a hearing in which the detainee is determined to have committed serious misconduct in violation of a federal facility rule, consistent with the Disciplinary Severity Scale, and only when alternative dispositions would inadequately regulate detainee behavior.

EMERGENCY: Any significant disruption of normal federal facility procedure, policy, or activity caused by riot, strike, escape, fire, medical exigency, natural disaster, or other serious incident.

EMERGENCY CARE: Care for an acute illness or unexpected serious health care need that cannot be deferred until the next scheduled sick call.

ENFORCEMENT AND REMOVAL OPERATIONS (ERO): A division within ICE, whose mission is the planning, management, and direction of broad programs relating to the supervision, detention, and removal of aliens who are in the U.S illegally.

ENTRY ON DUTY (EOD): The first day the employee begins performance at a designated duty station on this contract.

ENVIRONMENTAL ASSESSMENT (EA): A concise public document for which a Federal agency is responsible that serves to briefly provide sufficient evidence and analysis for determining whether to prepare an EIS or a Finding of No Significant Impact (FONSI), aid an agency's compliance with the National Environmental Policy Act (NEPA) when no EIS is necessary, and facilitate preparation of an EIS when one is necessary.

ENVIRONMENTAL IMPACT EVALUATION: The process of determining the level of significance of a potential impact on the human environment. It includes all necessary studies, consultation, and public involvement needed to analyze the potential for environmental impact of a proposed action, assign a value to the level of impact (e.g., minor, moderate, or major), consider mitigation, and determine the level of significance; whether significant or not. An environmental impact evaluation results in either the application of a CATEX, documentation in the form of an EA and FONSI or a final EIS and record of decision (ROD).

ENVIRONMENTAL IMPACT STATEMENT (EIS): A detailed written statement as required by section 102(2)(C) of the NEPA. It is a comprehensive document that provides full and fair discussion of significant environmental impacts caused by the proposed action(s). It also states the reasonable alternatives, and which of those would avoid or minimize the adverse impact(s) or enhance the quality of the human environment.

EXECUTIVE OFFICE OF IMMIGRATION REVIEW (EOIR): An agency of DOJ. The primary mission of EOIR is to adjudicate immigration cases by fairly, expeditiously, and uniformly interpreting and administering the Nation's immigration laws. Under delegated authority from the Attorney General, EOIR conducts immigration court proceedings, appellate reviews, and administrative hearings.

FEDERAL FACILITY: A structure(s) like a detention center, comprised of buildings and residential care services, where a contractor delivers secure residential support services under the

DRAFT

oversight of the U.S. Government to house its detainees on a 24-hour per day, 7-day per week, 365 day per year basis.

FEDERAL FACILITY ADMINISTRATOR: The contractor's official, regardless of local title (e.g., jail administrator, warden, federal facility director, superintendent), who has the ultimate responsibility for managing the operations of the contracted detention federal facility. The qualifications for the holder of this office shall be consistent with ACA standards.

FEDERAL FACILITY MAINTENANCE: The upkeep of a facility through cleaning, repairs, and similar work to keep the facility in good working order in accordance with all applicable federal laws, regulations, codes, guidelines, and policies.

FEDERAL FACILITY OPERATIONS CHARGE: A fixed fee designated for the maintenance and management of a U.S. Government-operated federal detention center.

FEDERAL DETENTION FACILITY: A federal detention facility, comprised of buildings and residential care services provided by the non-governmental support contractor, to enable the United States Government to house its detainees on a 24-hour per-day, 7-day per-week, 365-day per-year basis.

FINDING OF NO SIGNIFICANT IMPACT (FONSI): A document by a federal agency briefly presenting the reasons why an action, not otherwise excluded, will not have a significant effect on the human environment, and for which an EIS therefore will not be prepared.

FIRST AID: Health care for a condition that requires immediate assistance from an individual trained in first aid care and the use of the federal facility's first aid kits.

FLIGHT OPERATIONS UNIT (FOU): The FOU is the principal mass air transportation and manages government and contract flights.

GRIEVANCE: A written complaint filed by an alien with the federal facility administrator concerning personal health/welfare or the operations and services of the federal facility.

HEALTH AUTHORITY: The physician, health administrator, or agency on-site that is responsible for health care services pursuant to a written agreement, contract, or job description.

HEALTH CARE: The action taken, preventive and therapeutic. To provide for the physical and mental well-being of the alien population. Health care may include medical services, dental services, behavioral health services, nursing, personal hygiene, dietary services, and environmental conditions at the federal facility.

HEALTH CARE PERSONNEL: Duly licensed individuals whose primary duties are to provide health services to aliens in keeping with their respective levels of health care training or experience.

HEALTH UNIT (HU): The physical area in the federal facility and organizational unit set aside for routine health care and sick call. The HU is the designated part of the federal facility for the delivery

DRAFT

of care to aliens on an ambulatory or observation basis.

ICE HEALTH SERVICE CORPS (IHSC): The ICE Health Service Corps serves as the medical authority for ICE on a wide range of medical issues, including the agency's comprehensive alien health care program.

ICE HEALTH SERVICE CORPS (IHSC) FACILITY CARE LEVELS:

> **Facility Care Level 4** medically manage complex, chronic medical conditions that require frequent clinical interactions to maintain control or stability of the condition to include assistance with activities of daily living (feeding, toileting, bathing and hygiene). The facilities help prevent hospitalization or further medical complications. Care Level 4 facilities for behavioral health are inpatient facilities.
>
> **Facility Care level 3** medically manage stable patients suitable for outpatient care requiring regular clinical interventions and clinician evaluations monthly to every 3 months. These facilities have access to enhanced medical resources, through consultations with specialty services by medical specialists in the local community.
>
> **Facility Care Level 2** medically manage stable chronic conditions, all ages (i.e. diabetes, hypertension. Asthma, etc.).
>
> **Facility Care Level 1** medically manage detainees less than 60 years of age who are healthy.

IMMIGRATION PROCESSING CENTER (IPC): To fulfill ICE's critical mission, ERO operates federal, civil immigration detention facilities nationwide that house detainees to secure their presence for immigration proceedings or removal from the U.S.

IMMEDIATE RELATIVES: Spouses, children (including stepchildren and adopted children) and their spouses, parents (including stepparents), brothers and sisters (including stepbrothers and sisters and half- brothers and sisters) and their spouses.

INCIDENT REPORT: A written document reporting an event, such as minor disturbances, officer misconduct, any alien rule infraction, etc.

JUVENILE DETAINEE: Any alien under the age of 18 years.

LIFE SAFETY CODE: A manual published by The National Fire Protection Association specifying minimum standards for fire safety necessary in public interest.

LIMITED ENGLISH PROFICIENT/PROFICIENCY (LEP): A person who does not speak English as his or her primary language and who has a limited ability to read, speak, write, or understand English. LEP individuals may be competent in English for certain types of communication (e.g., speaking or understanding), but still be LEP for other purposes (e.g., reading or writing). LEP designations are also context-specific; an individual may possess sufficient English language skills

DRAFT

to function in one setting, but these skills may be insufficient in other settings.

LOGBOOK: The official record of post operations and inspections.

MAN-HOUR: Man-hour means productive hours when the required services are performed. Only productive hours can be billed and invoiced.

MEDICAL SCREENING: A system of structured observation and/or initial health assessment to identify newly arrived aliens who could pose a health or safety threat to themselves or others.

MILEAGE RATE: A fully burdened rate inclusive of the mileage rate in accordance with General Service Administration Federal Travel Regulation, vehicle equipment, maintenance, and fuel costs.

NON-CONTACT VISITATION: Visitation that restricts aliens from having physical contact with visitors using physical barriers such as screens and/or glass. Voice communications between the parties are typically accomplished by telephones or speakers. NON-DEADLY FORCE: The force a person uses with the purpose of not causing or which would not create a substantial risk of causing death or serious bodily harm.

OFFICE OF PROFESSIONAL RESPONSIBILITY, PERSONNEL SECURITY DIVISION (OPR-PSD): The ICE office which implements a component-wide personnel security program.

ON-CALL/REMOTE CUSTODY OFFICER POST: Posts operated as requested by the COR, or other ICE officials designated by COR, and including, but not limited to, escorting and custody of aliens for hearings, ICE interviews, medical watches, and any other location requested by the COR.

PAT DOWN SEARCH: A quick patting of the alien's outer clothing to determine the presence of contraband.

POLICY: A definite written course or method of action, which guides and determines present and future decisions and actions.

POST ORDERS: Written orders that specify the duties of each position, hour by hour, and the procedures the post officer will follow in carrying out those duties.

PREVENTIVE MAINTENANCE: A system designed to enhance the longevity and/or usefulness of buildings and equipment in accordance with a planned schedule.

PROCEDURE: The detailed and sequential actions that must be carried out to ensure that a policy is implemented. It is the method of performing an operation or a manner of proceeding on a course of action. It differs from a policy in that it directs action required to perform a specific task within the guidelines of that policy.

PRODUCTIVE HOURS: These are the hours when the required services are performed and can be

DRAFT

billed.

PROJECT MANAGER: Contractor employee responsible for on-site supervision of all Contractor employees, with the authority to act on behalf of the Contractor. The Project Manager cannot simultaneously serve in the role of manager and detention officer or supervisory detention officer.

PROPERTY: Refers to personal belongings of an alien.

PROPOSAL: The written plan submitted by the Contractor for consideration by ICE in response to the solicitation.

QUALIFIED HEALTH PROFESSIONAL: Physicians, dentists, and other professional and technical workers who by state law engage in activities that support, complement, or supplement the functions of physicians and/or dentists who are licensed, registered, or certified, as appropriate to their qualifications, to practice.

QUALITY ASSURANCE: The actions taken by the government to assure requirements of the PWS are met.

QUALITY ASSURANCE SURVEILLANCE PLAN (QASP): A government-produced document that is based on the premise that the Contractor, and not the government, is responsible for the day-to-day operation of the federal facility and all the management and quality control (QC) actions required to meet the terms of the contract. The role of the government in quality assurance is to ensure performance standards are achieved and maintained. The QASP validates that the Contractor is complying with ERO-mandated quality standards in operating, maintaining, and repairing detention facilities.

QUALITY CONTROL (QC): The Contractor's inspection system which covers all the services to be performed under the contract. The actions that a Contractor takes to control the production of services so that they meet the requirements stated in the contract.

QUALITY CONTROL PLAN (QCP): A Contractor-produced document that addresses critical operational performance standards for services provided.

RECORD OF DECISION (ROD): A document that explains an agency's decision describes the alternative the agency considered, and discusses the agency's plans for mitigation and monitoring, if necessary.

RELIEF FACTOR: Indicates how many individuals it takes to fill a single job position for a single shift, considering vacation, sick leave, training days, and other types of leave.

RESPONSIBLE PHYSICIAN: A person licensed to practice medicine with whom the federal facility enters into a contractual agreement to plan for and provide health care services to the alien population of the federal facility.

RESTRAINT EQUIPMENT: This includes but is not limited to handcuffs, belly chains, leg irons,

straitjackets, flexi cuffs, soft (leather) cuffs, and leg weights.

SAFETY EQUIPMENT: This includes but is not limited to firefighting equipment, i.e., chemical extinguisher, hoses, nozzles, water supplies, alarm systems, portable breathing devices, gas masks, fans, first aid kits, stretchers, and emergency alarms.

SALLYPORT: An enclosure situated either in the perimeter wall or fence to the federal facility or within the interior of the federal facility, containing gates or doors at both ends, only one of which opens at a time. This method of entry and exit helps to ensure that there shall be no breach in the perimeter or interior security of the federal facility.

SECURITY DEVICES: Locks, gates, doors, bars, fences, screens, hardened ceilings, floors, walls, and barriers used to confine and control aliens. In addition, electronic monitoring equipment, security alarm systems, security light units, auxiliary power supply, and other equipment used to maintain federal facility security.

SECURITY PERIMETER: The outer portions of a federal facility, which provides secure confinement of aliens.

SECURITY RISK – HIGH, MEDIUM, LOW:

- High-Risk– (Level 3) Aliens exhibit behavioral problems, or manifest a pattern of such behavior, or have a history of violent and/or criminal activity. These aliens may not be co-mingled with low custody aliens.

- Medium High-Risk– (Level 2) Aliens exhibit minor behavioral problems or have a history of nonviolent criminal behavior. These aliens have a history of violent or assaultive charges, convictions, institutional misconduct, or those with gang affiliation.

- Medium Low-Risk– (Level 1.5) Aliens with no history of violent or assaultive charges or convictions, no institutional misconduct, and no gang affiliation.

- Low-Risk– (Level 1) Aliens exhibit no behavioral problems and have no history of violent criminal behavior. This level may not include any alien with a felony conviction that included an act of physical violence. Low-risk level aliens may not be co-mingled with high custody aliens.

SEXUAL PRESENTATION OR EXPRESSION: refers to how an individual outwardly communicates or displays aspects of their sex, such as through behavior, clothing, mannerisms, speech, or personal interactions

Perception thereof: refers to how others interpret or assume an individual's sexual orientation, or sexual presentation or expression based on outward characteristics, behavior, appearance, or other cues, regardless of the individual's self-identification

SIGNIFICANT EVENT NOTIFICATION REPORT: A written document reporting a special event (e.g., the use of force, use of chemical agents, discharge of firearms).

DRAFT

SPECIAL MANAGEMENT UNIT: A designated area or unit used to house detainees who require separation from the general population for specific reasons (e.g., administrative segregation, disciplinary segregation, medical observation). These areas are designed to ensure the safety, security, and orderly operation of the federal facility while addressing the unique needs or circumstances of certain detainees.

STRIP SEARCH: An examination of an alien's naked body for weapons, contraband, and physical abnormalities. This also includes a thorough search of the individual's clothing while not being worn.

TRAINING: An organized, planned, and evaluated activity designed to achieve specific learning objectives. Training may occur on site, at an academy of training center, at an institution of higher learning, through contract service, at professional meetings or through closely supervised on-the-job training. Meetings of professional associations are considered training when there is clear evidence of the above elements. All trainers must be certified, and certification shall be approved by the COR or ICE-designee.

TRANSPORTATION COSTS: The cost of all materials, equipment, and labor necessary to respond to requests by designated officials for secure movement of aliens from place to place necessary for processing, hearings, interviews, etc.

TRAVEL COST: Cost inclusive of lodging and meals and incidental expenses for Transportation Officers exceeding the standard working hours. Contractor tours of duty will comply with all current federal laws. This includes but is not limited to the Federal Motor Carrier Safety Administration, CFR 395.5 - Maximum driving time for passenger-carrying vehicles. Cost is based on actual charges per occurrence, not to exceed the allowable Federal Travel Regulation rates/costs in effect on the dates of travel.

WEAPONS: This includes but is not limited to firearms, ammunition, knives, slappers, Billy clubs, electronic defense modules, chemical weapons (mace), and nightsticks.

DRAFT