U.S. Immigration and Customs Enforcement

U.S. Immigration and Customs Enforcement (ICE)

Training Management System (TMS)

Statement of Work (SOW)

For ICE Office of the Chief Information Officer (OCIO) and
Office of Leadership and Career Development (OLCD)

August 1, 2018

Version 1.0

TABLE OF CONTENTS

APPENDICES

1.0 GENERAL

1.1 Background

The U.S. Immigration and Customs Enforcement (ICE) is the single largest investigative branch of the Department of Homeland Security (DHS). ICE's mission is to protect America and uphold public safety by identifying criminal activities and eliminating vulnerabilities that pose a threat to our nation's borders, as well as enforcing economic, transportation, and infrastructure security. ICE works closely with every level of law enforcement and the development of a well-trained workforce is essential to the agency's success as a federal law enforcement agency. ICE's Office of Leadership and Career Development (OLCD) directs and manages the design, administration, and evaluation of all ICE training and professional development curricula and programs. OLCD is responsible for distributed learning, instructional management, accreditation, and policy. OLCD supports the full range of training activities at ICE, including the ICE Academies, a learning management system, a repository and recordation system, learning technology initiatives, training support, and the development and implementation of career development programs. OLCD and the Office of the Chief Information Officer (OCIO) work together to identify appropriate information technology systems that provide administration, management, and records repository of in-person, online, and blended training for 25,000+ ICE employees and contractors, increasing the effectiveness of the ICE workforce while minimizing risks inherent to law enforcement operations.

ICE currently utilizes the Training Management Support System (TMSS), which is a Commercial off the Shelf (COTS) application used to administer and manage instructor-led in-residence law enforcement and career development training activities. TMSS automates law enforcement and career development training operations, including managing classes, registration, scheduling, training, testing, certifications, performance and conduct evaluations, Federal Law Enforcement Training Accreditation, and documentation. TMSS provides lifelong training and certifications records that are accurate, comprehensive, and legally defensible. TMSS feeds into ICE's data warehouse, the Training Reporting Repository (TRR).

OLCD and OCIO require an enterprise training management system (TMS) solution that meets the requirements of TMSS. The solution must also interface directly with ICE's TRR. The TMS solution will provide a standardized method for managing various types of training formats, multiple training locations, accreditation requirements, course curriculums, registration, scheduling, evaluation, student transcripts and records, reporting, and analytical tools. The solution must ensure that training and certification records are legally defensible in civil and legal suits. Federal law enforcement training and accreditation are core functionalities and essential for ICE to meet its mission; they are considered a must-have for the IT system required for this requisition.

ICE has included in this acquisition, an optional CLIN to acquire Learning Management System (LMS) functionalities to deliver and manage on-line course delivery, registrations, SF182 Forms processing in accordance with DHS guidance, tracking assigned training and completions, and reporting.

1.2 Scope of Work

This Statement of Work (SOW) is to procure a training management system including technical and administrative support to service ICE's 25,000+ employees and contractors. The solution shall be web-based, Software-as-a-Service (SaaS), and hosted in a FedRAMP certified cloud environment. The selected solution must provide, at a minimum, the current functionality already in place with ICE's existing system, as well as migrate and incorporate all historical data.

There is an optional task to implement the LMS into the selected system.

All tasks and deliverables of this SOW are Firm Fixed-Price (FFP), unless explicitly excluded.

2.0 SPECIFIC REQUIREMENTS/TASKS

2.1 TMS Requirements/Tasks

2.1.1 TMS Program Services

The Contractor shall provide the following TMS program services:

- The Contractor shall provide points of contact (POC) – primary and alternate – for the management of all aspects of this contract to the Contracting Officer's Representative (COR). The POC shall be responsible for ensuring that the services and deliverables required by ICE are provided in accordance with the contract;
- The Contractor shall meet with the COR and other ICE representatives for a kickoff meeting at 500 12th Street, NW, Washington, DC, within five (5) business days of the effective date of the contract. Two days prior to the kickoff meeting, the Contractor shall provide an agenda for the meeting.

  The objectives of the kickoff meeting are to: initiate the communication process between ICE and the Contractor by introducing key project participants and identifying their roles; ensure the Contractor understands the expectations of key stakeholders regarding the scope of work and the effort described herein, including task requirements and objectives; discuss a Project Schedule; discuss critical aspects of the Project Management Plan (PMP) and deliverables; review communication ground rules; and, define a roadmap to a successful project.
- The Contractor shall meet bi-weekly, via telephone and/or video conferencing, with the COR and other stakeholders to discuss project updates and any critical issues to be resolved. The Contractor shall develop and distribute meeting minutes and action

items for all meetings, and notify the COR within one (1) business day if issues arise that prevent the Contractor from attending a meeting;

- The Contractor shall notify the COR, the IT Project Manager (IT PM_) and the OLCD Program Manager (OLCD PM) within three (3) business days of any event which will create a delay in the schedule and/or result in additional cost to ICE. All notifications shall be submitted electronically to the COR in writing and shall document the reason for the delay, the impact on the project, and the action the Contractor is taking to bring the project back on schedule;
- The Contractor shall submit written monthly status reports electronically to the COR, IT PM and the OLDC PM by the tenth (10th) calendar day of each month. The monthly status report shall address the functional accomplishments, issues, unresolved problems, and a plan of action for resolving any problems identified by ICE. This report shall contain the following:
    - The Contractor's name and address, the contract number, the date of the report, and the period covered by the report;
    - Significant changes to the Contractor's organization or method of operation;
    - Description of significant events occurring during the reporting period;
    - Status of pending deliverables with expected delivery dates;
    - Problem areas affecting technical, schedule, or cost elements of the contract;
    - Status of previously identified problem areas with results, conclusions, and recommendations;
    - Trip reports and significant results;
    - Planned accomplishments for the next reporting period; and,
    - For each task area, the statuses and expected timeframes for completing the associated tasks.
- The Contractor shall participate in, or facilitate, technical meetings, conference calls, and/or workgroups with OLCD and OCIO staff and other stakeholders. Within three (3) business days of a meeting, the Contractor shall develop minutes that identify the attendees, summarize the meeting, and document all action items. The Contractor shall provide the minutes electronically via email to the COR and attendees;
- The Contractor shall develop, maintain, and update a Risk Management Plan and Risk Register by identifying, documenting, analyzing, and prioritizing risks associated with this project. The Contractor shall support the development of management strategies to handle those risks, and monitor the health of the TMS throughout its lifecycle;
- The Contractor shall provide functional program support to ICE with a full-time senior system analyst/application expert located on-site at the ICE Academy in Glynco, GA. The senior system analyst shall support ICE personnel in the implementation, functional integration, and operation of the TMS including, but not limited to:
    - Providing expert guidance on system usage
    - Serving as a System Administrator;
    - Creating specific training documents when requested;
    - Conducting ad-hoc training when requested;
    - Developing solutions to functional issues that may arise;
    - Collaborating on identification of new functional requirements;
    - Providing Tier II support;
    - Reporting the status of service tickets using the ICE approved tracking tool;

  - Referring to the Software Maintenance Tier III Support provided by the Contractor, service tickets not resolved by Software Maintenance Tier II Support or performance of the required tasks; and,
  - Providing program support during normal Eastern Standard Time (EST) business hours
- The Contractor shall be available to support ICE staff in the identification and resolution of all problem reports and help desk tickets;
- The Contractor shall maintain all current and future manual data feeds to supply or consume information from other ICE systems including:
  - Manual extraction of Firearms Certification Training from the TMS and sent to FACTS via Excel; and,
  - Manual bi-weekly import of National Finance Center (NFC) information into TMS. The Contractor shall maintain an NFC/ICE data import tracking log that records the data received, record counts for the number of records received and number of records imported, and the date that the data was successfully imported. The Contractor shall submit the NFC/ICE data import tracking log electronically to the COR, the OLCD PM, and the IT PM within one (1) business day after each successful import;
- The Contractor may be required to travel to other sites to provide program or training support when requested by the OLCD PM and approved by the COR; and,
- The Contractor shall provide the following TMS training activities and materials:
  - Monthly hands-on system training and materials for instructors during the first four (4) months after the system is available to all users. The training shall be no more than four (4) hours in length. At the end of the four months, additional training shall be provided when requested;
  - Monthly hands-on system training and materials for registrars and schedulers during the first four (4) months after the system is available to all users. The training shall be no more than four (4) hours in length. At the end of the four months, additional training shall be provided when requested; and,
  - A student orientation training class, with materials that can be downloaded, for ICE employees to utilize at any time. The orientation training class and materials shall be customized and regularly updated to reflect ICE's instance of the system.

The contractor shall provide the following deliverables:

- Training documentation
- NFC/ICE data import tracking log

2.1.2 Software Subscription and Maintenance

The Contractor shall provide enterprise software licenses and operations and maintenance for the TMS for the life of the contract. The SaaS solution must fulfill all requirements included in Appendix A – TMS Functional Requirements

The Contractor is responsible for the following:

- The Contractor shall provide three separate environments: Production, Testing, and Training;
- The Contractor shall provide and maintain a training environment that mirrors the release level of the production environment and is accessible to all ICE employees for training purposes;
- The Contractor shall provide vendor documentation pertaining to software product releases and updates;
- The Contractor shall ensure the quality of the software and associated documentation that it delivers. The Contractor shall adhere to the DHS/ICE processes for event, incident, problem, and change management, as well as to the DHS/ICE processes, policies, and procedures for security management, including DHS 4300 rules as applicable;
- The TMS environments shall be available 24/7, including weekends and government holidays;
- The TMS shall be available 99.9% of the time, excluding scheduled maintenance;
- All records within the TMS, including legacy, shall be available to users 24/7, including weekends and government holidays;
- The Contractor shall coordinate with the TMS Control Change Board (CCB) to deploy changes after the feature/functionality is complete and has been approved by both the CCB and the product owner;
- The Contractor shall resolve software defects discovered within the code;
- The Contractor shall provide Tier II/ III support to include resolving functional, technical, and policy-related issues that ICE's Tier I helpdesk cannot support. In addition, the Contractor shall utilize ICE's issue-tracking portal to manage and distribute Tier II/III help requests (tickets). The ICE issue-tracking portal shall provide an immediate response to the users, and all email thread/actions will be tracked in a reportable manner. The Contractor shall provide a service level agreement for working/closing Tier II/III issue tickets and provide monthly reporting metrics on Tier II/III tickets. The OLCD PM serves as the designee for policy-based questions/concerns and will have access to the ICE issue-tracking portal. Based on ticket volume, resources allocated to the Tier II/III helpdesk may also be positioned to support other functional areas of the project.

2.1.3 FedRAMP Hosting

The contractor shall host the application in a FedRAMP-certified environment and collaborate with the ICE OCIO Information Assurance Division (IAD) to obtain an Authority-To-Operate. This includes providing information, preparing

completing/maintaining documentation, and participating with ICE Computer Security Scans. The FedRAMP Hosting capability shall provide a disaster recovery capability. See Appendix C: General Cybersecurity Contract Requirements.

The contractor shall provide the following deliverable:

- Security documentation, as required to obtain an ATO

2.1.4 Initial SaaS Configuration

- The contractor shall setup and configure the SaaS environments specific to the needs of ICE and including system interfaces;
- The Contractor shall emulate the configurations that exist in the ICE production environment to include current customizations;
- The Contractor shall develop and maintain in the SaaS environment, existing application interfaces, as well as any application interfaces established in the future;
- The Contractor shall support other contractors supporting an interfacing application with activities to include, but not be limited to, troubleshooting interface issues, developing related scripts, providing data, etc.
    - TMSS currently connects to the Training Reporting Repository (TRR) via a nightly ETL feed from TMSS to TRR;
- The Contractor shall support the disposition/shut-down of the legacy system in DHS DC.

The contractor shall provide the following deliverables:

- A cloud migration project plan detailing high level activities and timelines to complete activities under this task
- A cloud architecture document detailing system/application design, system interconnection requirements, Contractor Cloud capabilities, and software inventory
- Configured, accessible SaaS environments

2.1.5 Data Migration of Legacy System Records into the TMS

- The Contractor shall migrate the legacy system data into the new TMS environments;
- The contractor shall support the migration of data from DHS Data Center 1 (DC1) to the SaaS environment; and,
- The contractor shall develop a data migration plan that describes the data that will be migrated to the new system, how it will be stored in the new system, the process and timeline for how and when data will be transferred, and the process to confirm that all data was accurately and successfully transferred.

The Contractor shall provide the following deliverables:

- Data Migration Plan
- Data Migration Test Plan and Results

- SaaS environment with loaded data

2.1.6 Product Customization

ICE-specific Product Customization includes software changes to the application that are not included in the base product. If ICE requires software customization, it will be funded as required and based on the complexity of the requested change(s). Development will follow the ICE Agile methodology; see Appendix E – Lean-Agile/DevOpsSec Requirements. The Contractor will be required to provide pricing when requirements are identified by ICE.

Note: All ICE-specific changes to the TMS must be approved by the CCB and the product owner prior to implementation.

The Contractor is responsible for the following:

- The Contractor shall provide a test environment to demonstrate new iterations of changes and features;
- The Contractor shall work with OLCD to identify and document requested changes;
- For each release that includes ICE-specific customization, the Contractor shall develop a plan and schedule that itemize all backlog requirements to be included, as well as the number of sprints required to complete each backlog item;
- The Contractor shall ensure the quality of the software and associated documentation that it delivers, including;
    - Sufficient unit, system, and regression testing of new and modified software;
    - Demonstration of the new features/functionality to the product owner upon completion of each sprint;
    - Documented changes to configuration settings as required to ensure the successful operation of the TMS prior to UAT and/or deployment into production;
- The Contractor shall provide secure and accurate configuration management of all application and project artifacts/deliverables within its area of responsibility;
- The Contractor shall create and maintain the System Engineering Lifecycle (SELC)/SLM documentation required for each release based on the project tailoring plan; and,
- The Contractor shall leverage automation tools to reduce the number of manual tasks performed during operations. This includes recurring tasks, scheduled jobs, monitoring, updates, patching, user maintenance, and other operational tasks.

The Contractor shall provide the following deliverables:

- SLM Project documentation for Commercial-Off-The-Shelf (COTS) customization and maintenance activities
- Completed ICE Agile Maturity Model Self-Assessment each fiscal quarter

2.2 LMS Requirements/Tasks (Optional)

2.2.1 Online LMS Data Migration Plan

The Contractor shall provide a data migration of data into the Training Management System (TMS). The data migration plan shall include a description of the methodology for migrating data into the new LMS system, the timeline for how and when LMS data will be transferred, and the process to confirm that all data was accurately and successfully transferred.

The contractor shall provide the following deliverables:

- Data Migration Plan

2.2.2 LMS Program Services

The Contractor shall provide the following LMS program services:

- The Contractor shall meet with the COR and other ICE representatives for a LMS kickoff meeting at 500 12th Street, NW, Washington, DC, within five (5) business days after the LMS CLIN has been exercised. Two days prior to the kickoff meeting, the Contractor shall provide an agenda for the meeting.

  The objectives of the LMS kickoff meeting are to: ensure the Contractor understands the expectations of key stakeholders regarding the scope of work and the effort described herein, including task requirements and objectives; discuss a Project Schedule; discuss critical aspects of the Transition-In Plan and deliverables; and review communication ground rules.

- The Contractor shall incorporate into the TMS Risk Management Plan and Risk Register risks associated with the LMS. The Contractor shall identify, document, and analyze the LMS risks before prioritizing all risks associated with this project;
- The Contractor shall participate in, or facilitate, weekly LMS technical meetings, conference calls, and/or workgroups with OLCD and OCIO staff and other stakeholders throughout the implementation period. Within one (1) business day of a meeting, the Contractor shall develop minutes that identify the attendees, summarize the meeting, and document all action items. The Contractor shall submit the minutes electronically via email to the COR and attendees;
- The Contractor shall notify the COR, OLCD PM and IT PM within one (1) business day of any event which will create a delay in the LMS implementation schedule and/or result in additional cost to ICE. All notifications shall be submitted electronically to the COR, OLCD PM and IT PM in writing and shall document the reason for the delay, the impact on the project, and the action the Contractor is taking to bring the project back on schedule;
- The Contractor shall submit written bi-weekly LMS status reports to the COR, OLCD PM and IT PM electronically via email by 5:00pm EST every other Friday throughout

the implementation period. The status report shall address the LMS functional accomplishments, issues, unresolved problems, and a plan of action for resolving any problems identified by ICE. This report shall contain the following:

- The Contractor's name and address, the contract number, the date of the report, and the period covered by the report;
- Description of significant LMS events occurring during the reporting period;
- Status of pending LMS deliverables with expected delivery dates;
- Problem areas affecting technical, schedule, or cost elements of the LMS implementation;
- Status of previously identified LMS problem areas with results, conclusions, and recommendations;
- Trip reports and significant results related to the LMS implementation; and,
- Planned LMS accomplishments for the next reporting period.

- The Contractor shall provide the following LMS training activities and materials:
  - Monthly hands-on system training and materials for LMS administrators during the first six (6) months after the system is available to all users. The training shall be no more than four (4) hours in length. At the end of the six months, additional training shall be provided when requested;
  - Monthly hands-on system training and materials for LMS course managers during the first six (6) months after the system is available to all users. The training shall be no more than four (4) hours in length. At the end of the six months, additional training shall be provided when requested; and,
  - A LMS student orientation training class, with materials that can be downloaded, for ICE employees to utilize at any time. The orientation training class and materials shall be customized and regularly updated to reflect ICE's LMS instance of the system.
- The Contractor shall provide two (2) full-time Systems analysts/application experts, located at the Contractor's facilities, to provide functional program support to ICE. The analysts shall support ICE personnel in the implementation and functional integration of the LMS into the system, as well as the operation of the system including, but not limited to:
  - Providing expert guidance on system usage;
  - Serving as System Administrators;
  - Creating specific training documents when requested;
  - Conducting ad-hoc training when requested;
  - Developing solutions to functional issues that may arise;
  - Collaborating on identification of new functional requirements;
  - Providing Tier II support;
  - Reporting the status of service tickets using the ICE approved tracking tool;
  - Referring to the Software Maintenance Tier III Support provided by the Contractor, service tickets not resolved by Software Maintenance Tier II Support or performance of the required tasks; and,
  - Providing program support during normal Eastern Standard Time (EST) business hours.
- The Contractor may be required to travel to other sites to provide program or training support when requested by the OLDC PM and approved by the COR.

The contractor shall provide the following deliverables:

- Training documentation

2.2.3 Software Subscription and Maintenance

The contractor shall provide enterprise software licenses and operations and maintenance for the Learning Management System (LMS) for the life of the contract. The system must fulfill all requirements, included in Appendix B: LMS Requirements.

The Contractor is responsible for the following:

- The Contractor shall add incremental capacity to the existing TMS production, training and test environments to accommodate LMS requirements;
- The Contractor shall provide vendor documentation pertaining to software product releases and updates;
- The Contractor shall ensure the quality of the software and associated documentation that it delivers;
- The Contractor shall adhere to the DHS/ICE processes for event, incident, problem, and change management, as well as to the DHS/ICE processes, policies, and procedures for security management, including DHS 4300 rules as applicable;
- The system shall be available 24/7, including weekends, and government holidays;
- The system shall be available 99.9% of the time, excluding scheduled maintenance;
- All records within the system, including legacy, shall be available to users 24/7, including weekends and government holidays;
- The Contractor shall coordinate with the TMS CCB to deploy changes after the feature/functionality is complete and has been approved by both the CCB and the product owner;
- The Contractor shall resolve software defects of discovered within the code; and,
- The Contractor shall add the LMS to its incremental Tier II/III support, to include resolving functional, technical, and policy-related issues that ICE's helpdesk cannot support. The Contractor shall continue to utilize ICE's issue-tracking portal to manage and distribute all Tier II/III help requests (tickets). The Contractor shall update the TMS service level for working/closing Tier II/III issue tickets and provide monthly reporting metrics on Tier II/III tickets to include all LMS issues. Based on ticket volume, resources allocated to the Tier II/III desk may also be positioned to support other functional areas of the project.

2.2.4 FedRAMP Hosting

The contractor shall host the application in a FedRAMP Certified environment and collaborate with the ICE OCIO Information Assurance Division (IAD) to obtain an Authority-To-Operate. This includes providing information, preparing completing/maintaining documentation, and participating with ICE Computer Security

Scans. The FedRAMP Hosting capability shall provide a disaster recovery capability. See Appendix C: General Cybersecurity Contract Requirements.

The contractor shall provide the following deliverable:

- Security documentation, as required to obtain an ATO.

2.2.5 Initial SaaS Configuration

- The contractor shall setup and configure the SaaS environments specific to the needs of ICE and including system interfaces;
- The Contractor shall emulate the configurations that exist in the ICE production environment to include current customizations;
- The Contractor shall develop and maintain in the SaaS environment, existing application interfaces, as well as any application interfaces established in the future;
- The Contractor shall support other contractors supporting an interfacing application with activities to include, but not be limited to troubleshooting interface issues, developing related scripts, providing data, etc.
- The Contractor shall support the disposition/shut-down of the legacy LMS in use in DHS DC.

The contractor shall provide the following deliverables:

- A cloud migration project plan detailing high level activities and timelines to complete activities under this task
- A cloud architecture document detailing system/application design, system interconnection requirements, ICE Cloud capabilities, and software inventory
- Configured, accessible SaaS environments.

2.2.6 Data Migration of Legacy LMS Records into the TMS

- The Contractor shall migrate the legacy LMS data into the TMS environments following the data migration plan detailed in Section 2.2.1 and approved by the COR, ITPM, and OLCD PM; and,
- The Contractor shall support the migration of data from DHS Data Center to the SaaS environment.

The Contractor shall provide the following deliverables:

- Data Migration Test Plan and Results
- SaaS environment with loaded data.

2.2.7 Product Customization

ICE-specific Product Customization includes software changes to the application that are not included in the base product. If ICE requires software customization, it will be funded as required and based on the complexity of the requested change(s). Development will follow the ICE Agile methodology. See Appendix E – Lean-Agile/DevOpsSec Requirements. The contractor will be required to provide pricing when requirements are identified by ICE.

Note: All ICE-specific changes to the Training Management System must be approved by the Configuration Change Board (CCB) and the product owner prior to implementation.

The Contractor is responsible for the following:

- The Contractor shall provide a test environment to demonstrate new iterations of changes and features;
- The Contractor shall work with OLCD to identify and document requested changes;
- For each release that includes ICE specific customization, the Contractor shall develop a plan and schedule that itemize all backlog requirements to be included, as well as the number of sprints required to complete each backlog item;
- The Contractor shall ensure the quality of the software and associated documentation that it delivers, including;
    - Sufficient unit, system, and regression testing of new and modified software;
    - Demonstration of the new features/functionality to the product owner upon completion of each sprint;
    - Documented changes to configuration settings as required to ensure the successful operation of the Training Management System prior to UAT and/or deployment into production;
- The Contractor shall provide secure and accurate configuration management (CM) of all applications and project artifacts/deliverables within its area of responsibility;
- The Contractor shall create and maintain the System Engineering Lifecycle (SELC)/SLM documentation required for each release based on the project tailoring plan; and,
- The Contractor shall leverage automation tools to reduce the number of manual tasks performed during operations. This includes recurring tasks, scheduled jobs, monitoring, updates, patching, user maintenance, and other operational tasks.

The Contractor shall provide the following deliverables:

- SLM Project documentation for Commercial-Off-The-Shelf customization and maintenance activities
- Completed ICE Agile Maturity Model Self-Assessment each fiscal quarter.

2.2.8 LMS Deliverables Table (Optional)

Deliverable	Frequency	Submission Date	ICE Distribution	Format
Kick-off Agenda	Once	3 business days after CLIN exercised	Attendees (TBD)	Word
Project Schedule	Once	10 business days after CLIN exercised	COR, OLCD PM, OCIO ITPM	Project
Updated Risk Management Plan & Risk Register	Once	20 business days after CLIN exercised	IPT	Word, Excel
Online LMS Analysis, including Data Migration Plan	Once	45 calendar days after CLIN exercised	COR, OLCD PM, OCIO ITPM	Word
Weekly Technical Meeting Minutes	Weekly during implementation period	Within 1 business day after meeting	IPT	PDF
Bi-weekly Status Report	Bi-weekly during implementation period	5:00pm EST, every other Friday	COR, OLCD PM, OCIO ITPM	PDF

2.3 Transition-In and Transition-Out Plans

The Contractor shall develop a draft Transition-In Plan to include a schedule of milestones and events to be submitted in their response to the Transition-In Plan elements listed in this section. The Contractor's shall develop a Transition-In plan in final form within thirty (30) calendar days after start of Period of Performance to the COR. The Contractor shall develop a plan and schedule for activities (within the Contractor's control) needed to be fully operational within ninety (90) calendar days of the task order award. The Transition-In Plan includes, but is not limited, to the following elements:

- Mobilization of Contractor's team and facilities;
- A work plan that identifies milestones, measurable tasks, and resources required;
- Identification of specific Transition-In activities to be executed and how they will be managed;
- Identification of the key personnel transition team members by name, position, start date, and responsibilities. Note: Suitability for employment packages for Contractor staff can take up to ninety (90) calendar days to be approved; and,
- Identification of the risks to the Transition-In effort, and mitigation and contingency plans if the Transition-In cannot be executed on schedule.

The Contractor shall provide a final Transition-Out Plan as well as the support necessary to coordinate the transfer of all activities. The final Transition-Out Plan will be provided sixty (60) calendar days (or the first business day should this fall on a weekend) before the end of the Period of Performance.

The Transition-Out Plan includes the following elements:

- Transfer of all Government Furnished Equipment/Property (GFE/GFP), inventory, software and licenses;
- Provide Technical Architectural specifications to allow for transition of Development and Test environments (if applicable);
- Transfer of documentation currently in progress;
- Transfer of all ICE data in an agreed upon format;
- Coordinate transition with DHS/ICE IT personnel;
- Fully support the transition of application requirements to any successor Contractor;
- Contractor will identify current GFE requirements for Development and Test environments; and,
- Transition Staff and points of contacts

3.0 CONTRACTOR PERSONNEL

3.1 Qualified Personnel

The Contractor shall provide qualified personnel that are able to efficiently and accurately perform all requirements specified in this SOW.

3.2 Continuity of Support

The Contractor shall ensure that the contractually required level of support for this requirement is maintained at all times.

The Contractor shall provide prior e-mail notification to the Contracting Officer's Representative (COR) if the required level of Contractor support is not maintained for any reason, and replacement personnel will not be provided.

3.3 Key Personnel

There are four (4) key personnel required to be provided by the Contractor under this task order: Project Manager, Senior Systems Analyst/Application Expert, Senior Application Developer, and Systems Analyst/Application Expert. These roles are required for Section 2.0 Specific Requirements/Tasks. Key personnel shall possess the skills, experience and technical competencies that are critical to the successful performance of this task order. Key personnel shall meet all Knowledge/Skill Description specified below. The identified key personnel are critical to the performance under this order. The Contractor shall obtain written approval from the Contracting Officer (CO) and COR prior to replacement of the key personnel.

No changes in key personnel shall be made unless the Contractor can demonstrate that the qualifications of prospective replacement meet the qualifications specified below. The CO and COR shall be notified in writing of any proposed substitution at least 15 calendar days

(or 30 calendar days if a security clearance is required) in advance of the proposed substitution. Such notification shall include:

1. An explanation of the circumstances necessitating the replacement;
2. A complete resume of the proposed substitute; and
3. As requested by the CO or COR, any other information, which will enable them to judge whether or not the candidate meets the required qualifications for the respective position.

The CO and COR will evaluate key personnel substitution proposals at the task order level, and the CO will promptly notify the Contractor of his or her approval or rejection in writing. All rejections will require re-submission of another substitution to fill key positions within 15 calendar days from the date the Contractor was notified.

3.3.1 Project Manager

The Project Manager shall provide organizational oversight, budgeting, project schedule adherence monitoring, project delivery, and production support. The Project Manager shall interface with client management, functional, and technical staff to ensure responsive communications are effectively managed. The project manager shall have full authority to act for the Contractor on all matters relating to daily operations under this task order. The Project Manager shall act as the single point of contact between the Government and Contractor personnel assigned to support the work effort.

Education: B.A. or B.S. degree.

Experience: 5+ years project management experience, including at least 3 years of IT project management experience.

3.3.2 Senior Systems Analyst/Application Expert

The Senior Systems Analyst/Application Expert shall have extensive experience formulating/defining system scope and objectives based on user defined needs. The Senior Systems Analyst shall devise or modify procedures to solve problems considering application capacity and limitations, operating time, and form of desired results. The Senior Systems Analyst shall have full technical knowledge of all phases of applications systems analysis.

Education: B.A. or B.S. degree, or 5 years of equivalent experience in a related field.

Basic Experience: 5 years of computer experience in at least two of the following disciplines: system analysis, system programming, application programming, and equipment analysis.

Specialized Experience: At least 10 years of experience in the functional area of law enforcement training, with an understanding of processes, work flow, tracking, and reporting on training activities.

3.3.3 Senior Application Developer

The Senior Application Developer shall have extensive software development experience with web-based technologies.

Education: B.A. or B.S. degree, or 5 years of equivalent experience in a related field.

Basic Experience: 5 years of computer experience in at least two of the following disciplines: system analysis, system programming, application programming, and equipment analysis; 5 years of experience in Agile development.

Specialized Experience: At least 3 years of experience developing applications using advanced technologies, including internet protocols, web-based, and .Net technology. Technologies include HTML, CGI applications, PERL or JavaScript, and Java.

3.3.4 LMS Systems Analyst/ Application Expert (Optional)

The Systems Analyst/Application Expert shall have experience formulating/defining system scope and objectives based on user defined needs. The Systems Analyst shall devise or modify procedures to solve problems considering application capacity and limitations, operating time, and form of desired results. The Systems Analyst shall have technical knowledge of all phases of applications systems analysis.

Education: B.A. or B.S. degree, or 3 years of equivalent experience in a related field.

Experience: At least 3 years of experience in at least two of the following disciplines: system analysis, system programming, application programming, and equipment analysis.

3.4 Contractor Personnel Conduct

The Contractor shall immediately replace any individual provided under this SOW who fails to perform his or her duties adequately, is chronically absent or late, or conducts himself or herself in a manner that is inconsistent with the listed requirements, government employment policies and practices, or engages in practices that are disruptive to the working environment.

4.0 PERIOD OF PERFORMANCE

The Period of Performance (POP) for this task order is:

Transition-In Period – 3-month period of performance
Base Period – 12-month period of performance
Option Period 1 – 12-month period of performance
Option Period 2 – 12-month period of performance
Option Period 3 – 12-month period of performance
Option Period 4 – 12-month period of performance
Transition-Out Period – 3-month period of performance
FAR 52.217-8 Extension – 6-month period of performance

The anticipated start date of this requirement is November 1, 2018.

5.0 OVERTIME

Overtime will not be authorized for this task order.

6.0 PLACE OF PERFORMANCE

The work shall be performed primarily at the Contractor's facility and at the ICE Academy in Glynco, Georgia, though some work, subject to concurrence of the OLCD PM, can occur at ICE Headquarters facilities at 500 12th Street SW, Washington, DC 20536. The Contractor shall attend meetings via teleconference, unless otherwise stated. The Contractor shall be required to travel to meetings when requested by ICE. The Contractor shall have personnel available during normal Eastern Standard Time (EST) business hours.

7.0 TRAVEL

The contractor shall provide on-site and/or off-site training, when requested by ICE. The contractor shall arrange travel associated with any on-site training and provide travel request costs to the COR for approval prior to finalizing travel. Costs for transportation, lodging, meals and incidental expenses incurred by Contractor personnel on official company business are allowable subject to FAR 31.205-46, Travel Costs. These costs will be considered to be reasonable and allowable only to the extent that they do not exceed on a daily basis the maximum per diem rates in effect at the time of travel as set forth in the Federal Travel Regulations. The Contractor will not be reimbursed for travel and per diem within a 50-mile radius of the worksite where a Contractor has an office. A worksite is the same as a Contractor's place of performance location. Local travel expenses will not be reimbursed (this includes parking). All travel outside the local area must be approved by the COR in advance. No travel will be reimbursed without prior approval from the COR. The Contractor shall provide the COR with a completed Request for Travel Authorization at least five (5) calendar days prior to the requested travel date.

8.0 GOVERNMENT FURNISHED EQUIPMENT/GOVERNMENT FURNISHED PROPERTY

The Government will provide the Contractor with government furnished equipment (GFE)/ government furnished property (GFP) or will provide access to ICE systems through Workplace-as-a-Service (WaaS), if required. The Contractor shall return to the COR all GFE/GFP provided to perform work under this task order at the end of the period of performance. The Contractor shall keep an inventory of GFE/GFP, which shall be made available to the COR or CO upon request. The contractor shall provide the COR with a G-570 Property Receipt for all GFE/GFP within 48 hours of receipt. The Contractor shall ensure that all GFE/GFP provided shall be secured. The Contractor shall manage, maintain, and control all GFE/GFP in support of this contract and subsequent task orders in accordance with the clause at FAR 52.245-1.

9.0 DELIVERABLES

The Contractor shall deliver draft versions of required documentation and/or artifacts to the OLCD PM and the OCIO ITPM for review. The final versions shall be submitted to the COR, OLCD PM, and the OCIO ITPM. The COR shall have up to ten (10) calendar days after receipt of a deliverable to accept or reject any product. If the COR rejects a deliverable, the Contractor will be provided specific written comments detailing the basis for rejection and recommended corrective action. The Contractor shall have up to ten (10) calendar days to address each specific written comment by either incorporating the requested change, or providing an explanation of why the change is not being incorporated. The COR will have an additional five (5) calendar days to review and provide a final decision regarding acceptance or rejection of the deliverable. The Contractor shall provide deliverables in the format agreed to by the Government and Contractor.

9.1 Deliverables Table

The Contractor shall provide the following deliverables to the COR, unless noted otherwise:

Deliverable	Frequency	Submission Date	ICE Distribution	Required Format
Software Licenses	Once	On or before TBD	COR, OLCD PM, and OCIO ITPM	PDF and electronic
Monthly Status Report including Help Desk Activities	Monthly	10 business days after the end of each month	COR, OLCD PM, and OCIO ITPM	Word
Risk/Issues Inventory	Monthly	10 business days after the end of each month	COR, OLCD PM, and OCIO ITPM	Excel

Deliverable	Frequency	Submission Date	ICE Distribution	Required Format
Program Status meeting and meeting minutes, including tracking log for data import activities	Bi-Weekly	2nd Thursday after contract award; bi-weekly thereafter	COR, OLCD PM, and OCIO ITPM	Word
Data Migration Documentation	Once	Based on approved schedule	COR, OLCD PM, and OCIO ITPM	Word
Training Documentation	As needed	TBD	COR, OLCD PM, and OCIO ITPM	Word
Security Documentation	As needed	TBD	COR, OLCD PM, and OCIO ITPM	Word/Excel
Application documentation as required by the ICE SLM	As needed	TBD	COR, OLCD PM, and OCIO ITPM	Word/Excel or ICE approved Knowledge Management System.
Agile Self-Assessment(s)	Quarterly	Within 5 days of the end of each fiscal quarter	OLCD PM, ITPM, and ICE OCIO QA Representative	Excel

All deliverables shall comply with the System Lifecycle Management (SLM) documentation templates. A link to these document templates is available from ICE, and will be provided upon request.

10.0 APPLICABLE DOCUMENTATION

The Contractor shall comply with the following documents (which provide more details on requirements and implementation processes) and the latest versions of all technology standards and architecture policies, processes, and procedures applicable to the overall ICE TMS program. These publications include, but are not limited to, the following:

- Computer Security Act of 1987 (40 U.S.C. 1441 et seq.)
- DHS MD 4010.2, Section 508 Program Management Office & Electronic and Information Technology Accessibility, Issued 10/26/2005, http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_40102_section_508_program_management_office_and_information_technology_accessibility.pdf
- DHS 4300 Security Guidelines and Policies - Available upon request
- DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication
- FedRAMP documents and templates are available at http://FedRAMP.gov
- FedRAMP Security Assessment Framework https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2016/06/FedRAMP-Security-Assessment-Framework-v2-1.pdf

- Final FAR Rule for Implementing Section 508 of the Rehab Act Electronic and Information Technology Accessibility for Persons with Disabilities, https://www.section508.gov/sites/default/files/FAR_R2Z-i1-x_0Z5RDZ-i34K-pR.pdf
- FISMA of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130
- Government Information Security Reform Act of 2000
- ICE SLM Handbook – Available upon request
- ICE-Management-Instruction-001 for Agile Development – Available upon request
- ICE-Management-Instruction-001 Appendix – Available upon request
- ICE AgileDevOps Handbook ICE OCIO Quarterly Kanban Self-Assessment Template – Available upon request
- ICE OCIO Quarterly Scrum Self-Assessment Template – Available upon request
- NIST FIPS 201-2 — Personal Identity Verification (PIV) of Federal Employees and Contractors (August 2013), http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf
- NIST SP 800-53, Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-63-2: Electronic Authentication Guideline (August 2013), http://dx.doi.org/10.6028/NIST.SP.800-63-2
- OMB M-10-15 — FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, issued November 19, 2010, http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Documents/FY%202010%20FISMA%20and%20Privacy%20Report.pdf
- Privacy Act of 1974, https://www.justice.gov/opcl/privstat.htm
- Federal Information Processing Standard (FIPS) 199, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- Federal Information Security Management Act (FISMA), November 22, 2002, http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

11.0 SECTION 508 PROGRAM MANAGEMENT OFFICE & ELECTRONIC AND INFORMATION TECHNOLOGY ACCESSIBILITY

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 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:

11.1 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 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 1194.31 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 offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

11.2 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 as a whole 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 of the 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 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.

11.3 Section 508 Applicable Exceptions

Exceptions for this work statement 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 purposes of this requirement, are not considered members of the public.

12.0 REQUIRED SECURITY LANGUAGE FOR SENSITIVE /BUT UNCLASSIFED (SBU) CONTRACTS

12.1 Security Requirements

12.2 General

The United States Immigration and Customs Enforcement (ICE) has determined that performance of the tasks as describe in this Award 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.

12.3 Preliminary Determination

ICE will exercise full control over granting; denying, withholding or terminating unescorted government facility and/or sensitive Government information access for Contractor employees, based upon the results of a background investigation. ICE may, as it deems appropriate, authorize and make a favorable expedited pre-employment determination based on preliminary security checks. The expedited pre-employment determination will allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable pre-employment determination shall not be considered as assurance that a favorable full employment determination will follow as a result thereof. The granting of a favorable pre-employment determination or a full employment determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by ICE, at any time during the term of the contract. No employee of the Contractor shall be allowed to enter on duty and/or access sensitive information or systems without a favorable preliminary fitness determination or final fitness determination by the Office of Professional Responsibility, Personnel Security Unit (OPR-PSU). No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable pre-employment determination or full employment determination by the OPR-PSU. Contract employees

are processed under the ICE Management Directive 6-8.0. The contractor shall comply with the pre-screening requirements specified in the DHS Special Security Requirement – Contractor Pre-Screening paragraph located in this contract, if HSAR clauses 3052.204-70, Security Requirements for Unclassified Information Technology (IT) Resources; and/or 3052.204-71, Contractor Employee Access are included in the Clause section of this contract.

12.4 Background Investigations

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

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

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

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

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

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

6. Optional Form 306 Declaration for Federal Employment (this document sent as an attachment in an e-mail to applicant from OPR-PSU – must be signed and archived into

applicant's OPM e-QIP account prior to electronic "Release" of data via on-line account).

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

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

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

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

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

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

12.5 Transfers from Other DHS Contracts

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

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

12.6 Continued Eligibility

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

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

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

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

12.7 Required Reports

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

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

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

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

12.8 Employment Eligibility

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

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

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

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

Security Management

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

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

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

12.9 Information Technology

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

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

See Appendix D – General Cybersecurity Contract Requirements for security requirements related to the TMS.

12.10 Information Technology Security Training and Oversight

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

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

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

12.11 Ice Office of Information Governance and Privacy Clauses

A. Limiting Access to Privacy Act and Other Sensitive Information

(1) Privacy Act Information

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

(2) Prohibition on Performing Work Outside a Government Facility/Network/Equipment

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

(3) Prior Approval Required to Hire Subcontractors

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

(4) Separation Checklist for Contractor Employees

Contractor shall complete a separation checklist before any employee or Subcontractor employee terminates working on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposal of sensitive personally identifiable information (PII), in paper or electronic form, in the custody of the employee or Subcontractor employee including the sanitization of data on any computer systems or media as appropriate; and, (3) termination of any technological access to the Contractor's facilities or systems that would permit the terminated employee's access to sensitive PII.

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

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

B. Privacy Training, Safeguarding, and Remediation

If the Safeguarding of Sensitive Information (MAR 2015) and Information Technology Security and Privacy Training (MAR 2015) clauses are included in this contract, section B of this clause is deemed self- deleting.

(1) Required Security and Privacy Training for Contractors

Contractor shall provide training for all employees, including Subcontractors and independent contractors who have access to sensitive personally identifiable information (PII) as well as the creation, use, dissemination and/or destruction of sensitive PII at the outset of the employee's work on the contract and every year thereafter. Training must include procedures on how to properly handle sensitive PII, including security requirements for the transporting or transmission of sensitive PII, and reporting requirements for a suspected breach or loss of sensitive PII. All Contractor employees are required to take the Privacy at DHS: Protecting Personal Information training course. This course, along with more information about DHS security and training requirements for Contractors, is available at www.dhs.gov/dhs-security-and-training-requirements-contractors. The Federal Information Security Management Act (FISMA) requires all individuals accessing ICE information to take the annual Information Assurance Awareness Training course. These courses are available through the ICE intranet site or the Agency may also make the training available through hypertext links or CD. The Contractor shall maintain copies of employees' certificates of completion as a record of compliance and must submit an annual e-mail notification to the ICE Contracting Officer's Representative that the required training has been completed for all the Contractor's employees.

(2) Safeguarding Sensitive PII Requirement

Contractor employees shall comply with the Handbook for Safeguarding sensitive PII at DHS at all times when handling sensitive PII, including the encryption of sensitive PII as required in the Handbook. This requirement will be flowed down to all subcontracts and lower tiered subcontracts as well.

(3) Non-Disclosure Agreement Requirement

All Contractor personnel that may have access to PII or other sensitive information shall be required to sign a Non-Disclosure Agreement (DHS Form 11000-6) prior to commencing work. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) Prohibition on Use of PII in Vendor Billing and Administrative Records

The Contractor's invoicing, billing, and other financial/administrative records/databases may not store or include any sensitive Government information, such as PII that is created, obtained, or provided during the performance of the contract. It is acceptable to list the names, titles and contact information for the Contracting Officer, Contracting Officer's Representative, or other ICE personnel associated with the administration of the contract in the invoices as needed.

(5) Reporting Suspected Loss of Sensitive PII

Contractors must report the suspected loss or compromise of sensitive PII to ICE in a timely manner and cooperate with ICE's inquiry into the incident and efforts to remediate any harm to potential victims.

1. The Contractor must develop and include in its security plan (which is submitted to ICE) an internal system by which its employees and Subcontractors are trained to identify and report the potential loss or compromise of sensitive PII.

2. The Contractor must report the suspected loss or compromise of sensitive PII by its employees or Subcontractors to the ICE Security Operations Center (480-496-6627), the Contracting Officer's Representative (COR), and the Contracting Officer within one (1) hour of the initial discovery.

3. The Contractor must provide a written report to ICE within 24 hours of the suspected loss or compromise of sensitive PII by its employees or Subcontractors. The report must contain the following information:

a. Narrative or detailed description of the events surrounding the suspected loss or compromise of information.
b. Date, time, and location of the incident.
c. Type of information lost or compromised.
d. Contractor's assessment of the likelihood that the information was compromised or lost and the reasons behind the assessment.
e. Names of person(s) involved, including victim, Contractor employee/Subcontractor and any witnesses.

f. Cause of the incident and whether the company's security plan was followed and, if not, which specific provisions were not followed.
g. Actions that have been or will be taken to minimize damage and/or mitigate further compromise.
h. Recommendations to prevent similar situations in the future, including whether the security plan needs to be modified in any way and whether additional training may be required.

4. 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 sensitive information incidents.

5. At the Government's discretion, Contractor employees or Subcontractor employees may be identified as no longer eligible to access sensitive PII or to work on that contract based on their actions related to the loss or compromise of sensitive PII.

(6) Victim Remediation

The Contractor is responsible for notifying victims and providing victim remediation services in the event of a loss or compromise of sensitive PII held by the Contractor, its agents, or its Subcontractors, under this contract. Victim remediation services shall include at least 18 months of credit monitoring and, for serious or large incidents as determined by the Government, call center help desk services for the individuals whose sensitive PII was lost or compromised. The Contractor and ICE will collaborate and agree on the method and content of any notification that may be required to be sent to individuals whose sensitive PII was lost or compromised.

C. Government Records Training, Ownership, and Management

(1) Records Management Training and Compliance

(a) The Contractor shall provide DHS basic records management training for all employees and Subcontractors that have access to sensitive PII as well as to those involved in the creation, use, dissemination and/or destruction of sensitive PII. This training will be provided at the outset of the Subcontractor's/employee's work on the contract and every year thereafter. This training can be obtained via links on the ICE intranet site or it may be made available through other means (e.g., CD or online). The Contractor shall maintain copies of certificates as a record of compliance and must submit an e-mail notification annually to the Contracting Officer's Representative verifying that all employees working under this contract have completed the required records management training.

(b) The Contractor agrees to comply with Federal and Agency records management policies, including those policies associated with the safeguarding of records covered by

the Privacy Act of 1974. These policies include the preservation of all records created or received regardless of format, mode of transmission, or state of completion.

(2) Records Creation, Ownership, and Disposition

(a) The Contractor shall not create or maintain any records not specifically tied to or authorized by the contract using Government IT equipment and/or Government records or that contain Government Agency data. 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.

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

(c) The Contractor shall not retain, use, sell, disseminate, or dispose of any government data/records or deliverables without the express written permission of the Contracting Officer or Contracting Officer's Representative. 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 Agency records schedules.

D. Data Privacy and Oversight

Section D applies to information technology (IT) contracts. If this is not an IT contract, section D may read as self-deleting.

(1) Restrictions on Testing or Training Using Real Data Containing PII

The use of real data containing sensitive PII from any source for testing or training purposes is generally prohibited. The Contractor shall use synthetic or de-identified real data for testing or training whenever feasible. ICE policy requires that any proposal to use of real data or de-identified data for IT system testing or training be approved by the ICE Privacy Officer and Chief Information Security Officer (CISO) in advance. In the event performance of the contract requires or necessitates the use of real data for system-testing or training purposes, the Contractor in coordination with the Contracting Officer or Contracting Officer's Representative and Government program manager

shall obtain approval from the ICE Privacy Office and CISO and complete any required documentation.

If this IT contract contains the Safeguarding of Sensitive Information (MAR 2015) and Information Technology Security and Privacy Training (MAR 2015) clauses, section D(2) of this clause is deemed self-deleting.

(2) Requirements for Contractor IT Systems Hosting Government Data

The Contractor is required to obtain a Certification and Accreditation for any IT environment owned or controlled by the Contractor or any Subcontractor on which Government data shall reside for the purposes of IT system development, design, data migration, testing, training, maintenance, use, or disposal.

(3) Requirement to Support Privacy Compliance

(a) The Contractor shall support the completion of the Privacy Threshold Analysis (PTA) document when it is required. PTAs are triggered by the creation, modification, upgrade, or disposition of an IT system, and must be renewed at least every three years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide adequate support to complete the PIA in a timely manner, and shall ensure that project management plans and schedules include the PTA, PIA, and SORN (to the extent required) as milestones. Additional information on the privacy compliance process at DHS, including PTAs, PIAs, and SORNs, is located on the DHS Privacy Office website (www.dhs.gov/privacy) under "Compliance." DHS Privacy Policy Guidance Memorandum 2008-02 sets forth when a PIA will be required at DHS, and the Privacy Impact Assessment Guidance and Template outline the requirements and format for the PIA.

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

- Must have excellent writing skills, the ability to explain technology clearly for a non-technical audience, and the ability to synthesize information from a variety of sources;

- Must have excellent verbal communication and organizational skills;
- Must have experience writing PIAs. Ideally the candidate would have experience writing PIAs for DHS;
- Must be knowledgeable about the Privacy Act of 1974 and the E-Government Act of 2002; and,
- Must be able to work well with others.

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

(End of Clause)

13.0 INVOICING / PAYMENT

The Contractor shall submit invoices by the 10th working day following the end of each billing month directly to the Burlington Finance Center (BFC). Invoices shall be submitted via one of the following three methods:

- Mail: DHS, ICE
  Burlington Finance Center
  P.O. Box 1620
  Williston, VT 05495-1279
  Attn: ICE OCIO Invoice

- Fax: 802-288-7658

- Email: Invoice.Consolidation@dhs.gov

Invoices submitted by other than these three methods will be returned. The Contractor's Taxpayer Identification Number (TIN) must be registered in the Central Contractor Registration (http://www.ccr.gov) prior to award and shall be notated on every invoice submitted to ICE to ensure prompt payment provisions are met. The Program Office shall also be notated on every invoice. To assist in timely payment, it is also recommended that the Contractor provide the Accounting Transaction Number (also known as the "PJ" number) on the submitted invoice.

In accordance with Task Order Clauses, FAR 52.212-4 (g) (1), Contract Terms and Conditions – Commercial Items, or FAR 52.232-25 (a) (3), Prompt Payment, as applicable, the information required and must be included with each invoice submission is as follows:

- Name and address of the Contractor
- Invoice date and number
- Contract number, contract line item number and, if applicable, the order number
- Description, quantity, unit of measure, unit price and extended price of the items delivered
- Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading
- Terms of any discount for prompt payment offered
- Name and address of official to whom payment is to be sent
- Name, title, and phone number of person to notify in event of defective invoice
- Electronic funds transfer (EFT) banking information

APPENDICES

Appendix A – TMS Functional Requirements

Key Technical Requirements:

System Administration & Management

- Single Sign-On access to all system components
- Ability to interface and/or exchange data with ICE or DHS management systems (records, HR, financial, etc.)
- Create variety of defined user roles with read/add/edit/delete permissions
- Auto-lock of inactive user accounts
- System health monitor to review nightly system processes
- Import wizard to add data
- Create and save reusable import templates
- Customer branding of login page
- An interface/portal for users to view person records, transcripts, search for courses, register, etc.
- Manage user interface/portal permissions
- Supports viewing in modern versions of Microsoft IE and Google Chrome
- Create, manage online WebForms with drag and drop interface, user-defined data elements
- Manage the submission, approval, and tracking of the SF-182 Form and data
- Ability to create and edit separate automatic email notifications at multiple levels (academy, program, class, registration, performance evaluation, etc.) for a variety of actions (account creation, registration, waitlist, class information, etc.)
- Support for simultaneous logins of multiple thousands of users

Personnel and Organization Administration & Management

- Ability to import, add, and edit organization and organizational hierarchy
- Manage organizational information
- Create, maintain divisions within academies
- Establish Programs within academies
- Perform an automated daily feed from DHS/ICE personnel systems that creates, updates, or inactivates person records
- Ability to manually import daily feed from DHS/ICE personnel systems from .csv or another flat file
- Automatically check and identify errors and duplicate records in daily feed
- Ability to merge duplicate records in system
- Add, manage, and maintain person records
- Auto-generate unique person record identifiers
- Secure tracking of all sensitive personally identifiable information (SPII) with ICE-specified access levels
- Encryption of all SPII
- Ability to mask SPII on pages that show it

- Maintain all person records in comprehensive, user-friendly "Hire-to-Retire" format
- Maintain legal defensibility of all training records
- Track variety of information in person records (contact, employment, training, instructor, certifications, etc.)
- Ability to customize fields in student records to accommodate DHS/ICE-specific personnel information (job series, direct supervisor, probationary period start and end dates, hire dates, entry on duty dates, etc.)
- Ability to designate multiple roles and titles in person records
- Automation for adding and removing people from roles based on personnel feed
- Ability to import and export information in person records from/to various file formats
- Ability to attach multiple document files to person records in various file formats
- Ability to print information from person records in various file formats
- Track contact information, including emergency contact
- Define, track, and search on multiple user-defined fields in person records
- Ability to assign training equivalencies between courses

Training Administration & Management

- Support classroom, web-based, on-line, and law enforcement skills training
- Create, import, and manage curriculum templates for standardized class creation
- Ability to associate required EHRI data with course (training type code, course duration, etc.)
- Create, edit, and manage user-defined graduation requirements
- Create, manage, associate, and track learning objectives and weights to curriculum, assignments, and assessments
- Specify class dates, locations
- Publication of course catalogue on student portal website
- Assign staff with specific or multiple roles to classes
- Set course prerequisites
- Record, report student performance, progress, and results in a course
- Automatic and manual grading and graduation processes
- Assign test templates to classes
- Assign tests to students
- Proctor online tests
- Define retest and waiver rules
- Ability to attach multiple document files in various file formats to class templates, classes, activities
- Ability to track EHRI data for course content (training type code, course duration, etc.)
- Ability to import and track external certifications
- Ability to attach evaluations and surveys to courses

Asynchronous On-line Course Management

- Ability to upload SCORM, AICC, and Experience API (Tin Can) courses
- Ability to connect with SkillSoft OLSA server (AICC)
- Ability to upload document files in various file formats as general courses
- Version control for online content

Scheduling and Registration Administration & Management

- Create, manage schedule templates that support complex, multi-week training programs and courses with specified training periods
- Create, update class schedules
- Define, manage resource assignments
- Automatic and manual scheduling of resources
- Monitor, notify resource scheduling conflicts across each academy's training programs
- Monitor, notify instructor shortfalls and overages
- Ability to attach multiple document files in various file formats to class records
- Ability to print class schedules in user-friendly format
- Automated and manually manage registration, enrollment, waitlist, transfers, denials, cancellations
- Ability to enroll students via flat file (.csv or other format)
- Ability for user self-registration through user interface/portal
- Announce, automatically verify prerequisites
- Establish approval processes for enrollment
- Ability to automatically or manually grade and graduate students within class
- Ability to attach multiple document files in various file formats to class schedules, activities

Testing and Evaluation Administration & Management

- Create, manage Terminal Performance Objectives and Enabling Performance Objectives
- Create, import, and manage test question bank
- Create, manage test templates
- Create observed test types
- Support for versioning of questions, tests
- Ability to assign test questions by difficulty (hard, medium, easy)
- Support for custom or randomized question order, including ability to create a test with questions randomly selected by difficulty and objectives, such that randomization produces as many unique exams as there are questions per objective
- Retest allowances for all exams and observed tests, with settings for waivers of remediation, minimum scores acceptable, etc.
- Manage observed and skills based tests
- Mobile application for observed tests
- Create and manage performance evaluation reports

- Support Field Training Officer report authoring/review options to local agency personnel
- Ability to attach multiple document files in various file formats to performance evaluation reports
- Ability to print tests, performance evaluation reports

Reporting and Analytic Tools Administration & Management

- Optimization of resource utilization
- Support training load projections for no less than one year ahead
- Ability to review real-time consolidated utilization across resource categories
- Automated conflict identification and intelligent resolution options
- Manage individual instructor calendars and availability
- Automatically load-balance instructor assignments; provide look-ahead functionality to proactively ensure instructor availability
- Ensure instructor continuity when auto-scheduling instructors
- Ability to search, review, and export multiple types of data in various file formats
- Ability to search in uploaded documents
- Multiple standard reports, such as
    - Audit trail reporting
    - Usage statistics
    - Completion and content access reports
    - Required training and compliance reports
    - Person record reports
    - System health
    - System security
- Ability to create custom reports using a user-friendly Ad hoc tool
- Self-service printable/sharable training transcripts
- Data and reports that support the accreditation of law enforcement training:
    - Inclusive dates a program is conducted and actual dates and times when each segment of training occurs
    - Roster of participants in each iteration
    - Practical evaluations and/or written examinations and keys
    - Documentation that verifies a student met all prerequisites for attending the training course
    - Documentation of any exceptions or waivers requested or granted to a student
    - Documentation that verifies a student successfully completed the training course
    - Evidence of system back up (back up logs)
    - Instructor assignments associated with required certifications
    - Instructor certifications (e.g., firearms instructor, ICE Academy Qualified Instructor, Defensive Tactics Instructor, FLETC Firearm Instructor)
    - Class schedule output in calendar view using Excel
    - Class schedule includes venue, lesson plan title, lesson plan number, instructor name, instructor division (firearms, operations, legal)

- Class rosters to include full name, gender, job title, sending/home office
- Repeatable training program structures
- Training documentation associated with program structure/blocks of instruction
- Text searchable training documentation (by keyword)
- Archival of training documentation by program structure, program title, block of instruction, class number, and student ID
- Exam question analysis to include question performance across multiple offerings of a training program, within one offering, across gender, across multiple training programs, by associated training objective, by most frequently selected answer choices, by version of exam question
- Exam performance analysis to include performance of a defined series of questions across multiple offering of a training program, gender, and other demographic information
- Observed assessment (Practical evaluations) analysis of checklists performance-based checklist items across a training program, offering, designated selection of offerings, gender, by training objective, and by version of observed assessment (practical evaluation/observed test) and assessment item (checklist or tracked item within the observed test)
- Reports that match assessment items to job tasks, training objectives, training materials, training program, and class numbers

Appendix B – Optional LMS Requirements

Key Technical Requirements:

Content Management

- Upload SCORM1.2, AICC, SCORM 2004, and Experience API content packages
- Ability to connect with third party content, including Skillsoft
- Ability to accept content from a wide variety of sources including, but not limited to:
    - HTML5
    - Video Streaming
    - Word
    - PowerPoint
    - Flash
    - Zip files
    - PDF
    - Raw media files
- Ability to create course numbers and other unique metadata for each course that is uploaded
- Ability to designate individual users to manage the content once it is created
- Ability to manage uploaded files (update or replace them)
- Ability to assign content to specific user audiences

User Interface

- Provide an easily searchable catalog of all training content
- Provide a mechanism for browsing content
- Allow deep-links so that individuals may directly access content from outside the LMS (the link will take them to the login screen, but after login they will be redirected to the content)
- Provide a user home screen that provides easy access to assigned content, transcripts, upcoming courses, and a list of in-progress courses
- Access to context sensitive help
- Ability to create and track individual development plans

Notifications

- Automated email notifications when accounts are created
- Customizable emails for course registrations, assignment reminders, and registration reminders

SF-182 and External Training

- Ability to complete SF-182 form on-line
- Configurable workflow for SF-182 form approval
- Ability to generate reports on SF-182s

Reporting

- Ability for individuals to generate their own transcripts
- Ability for supervisors to view transcripts and training assignment completions for their employees

Appendix C – General Cybersecurity Contract Requirements

C.1 In accordance with ITAR 4.5.3.1 – Compliance with DHS Security Policy Terms and Conditions.

Compliance with DHS Security Policy Terms and Conditions:

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

C.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 Technical Representative (COTR), 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.

In accordance with ITAR 4.5.3.7 – Supply Chain Risk Management

Supply Chain Risk Management Terms and Conditions

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 diligence to ensure that these standards are met.

The Government shall be notified when a new contractor/subcontractor/service provider 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. In the event that 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 procured under this contract.

Contractors shall employ formal and accountable transit, storage, and delivery procedures (i.e., the possession of the component is documented at all times from initial shipping point to final 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.

In accordance with HSAR 3052.204-70 - Security requirements for unclassified IT resources, with ITAR 4.5.3.3 – Access to Unclassified Facilities, IT Resources, and Sensitive Information Requirement Clause Inclusion Instruction, with ITAR 4.5.3.9 – Security Requirements for Unclassified Information Technology Resources Clause, with ITAR 4.5.4.6 – Required Protections for DHS Systems Hosted in Non-DHS Data Centers, and with ITAR 4.5.4.7 – Contractor Employee Access Clause . As prescribed in (HSAR) 48 CFR 3004.470-3 Contract clauses:

Security Requirements for Unclassified Information Technology Resources (JUN 2006)

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

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

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

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

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

Examples of tasks that require security provisions include:

a) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and
b) Access to DHS networks or computers at a level beyond that granted the public (e.g., such as bypassing a firewall).

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

C.5.1 Contractor IT Security Accreditation*:*

Contractor IT Security Accreditation

Within 6 months after contract, the contractor shall submit written proof of IT Security accreditation to DHS for approval by DHS CO. Accreditation will proceed according to the criteria of DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the CO will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the CO, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

C.6 In accordance with HSAR 3052.204-71 - Contractor Employee Access

Contractor Employee Access (Sep 2012)

Sensitive Information, as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy.

This definition includes the following categories of information:

a) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);
b) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," 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 his/her designee);
c) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and
d) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.
e) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

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 CO. Upon the CO'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 sensitive information or IT 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.

The CO 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.

Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the CO. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

C.7 In accordance with ITAR 4.5.3.10 – Contractor Employee Access Clause (use language from HSAR 3052.204-70 and alternates at 3052.204-71).

C.7.1 Contractor IT Resource Access (Sep 2012)

1) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.
2) The Contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.
3) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).
4) 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.

5) 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. In order for a waiver to be granted:
   a) There must be a compelling reason for using this individual as opposed to a U. S. citizen; and
   b) The waiver must be in the best interest of the Government.
6) 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.

C.8 In accordance with White House Digital Government BYODTK – Privacy Expectations

The following passage should be included in **ALL** acquisition documents:

Privacy Expectations

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

C.9 In accordance with White House Digital Government BYODTK – Mobile Information Technology Device Policy

The following passage should be included in **ALL** acquisition documents for Mobile devices:

Mobile Information Technology Device Usage

Users who conduct official DHS ICE business on a mobile IT device must:

a) Sign the Remote Access and Mobile IT Device User Agreement Form.
b) Operate the device in compliance with this policy, all applicable federal requirements, and the DHS ICE Remote Access and Mobile Information Technology Guide.
c) Not process or access Classified information on the device.

d) Use only approved and authorized DHS ICE owned devices to physically attach to DHS ICE IT systems.
e) Store only the minimum amount, if any, of Personally Identifiable Information (PII) and electronic Protected Health Information (ePHI) necessary to do one's work, and immediately delete the PII or ePHI when no longer needed. Users shall receive written approval from their supervisor before accessing, processing, transmitting, or storing DHS ICE Sensitive Information such as PII or ePHI.
f) Exercise extra care to preclude the compromise, loss, or theft of the device, especially during travel.
g) Immediately contact the DHS ICE Service Desk and their immediate supervisor if the IT device is lost, stolen, damaged, destroyed, compromised, or non-functional.
h) Abide by all federal and local laws for using the device while operating a motor vehicle (e.g. users are banned from text messaging while driving federally owned vehicles, and text messaging to conduct DHS ICE business while driving non-government vehicles).

Users who are issued a DHS ICE owned mobile IT device must also:
a) Comply with DHS 4300A Sensitive Systems Handbook Attachment Q.
b) Not disable or alter security features on the device.
c) Only use the DHS ICE owned device for official government use and limited personal use.
d) Reimburse the OCIO for any personal charges incurred that are above the established fixed cost for the Agency's use of the device (e.g. roaming charges incurred for personal calls).
e) Be required to reimburse DHS ICE if the mobile IT device is lost, stolen, damaged or destroyed as a result of negligence, improper use, or willful action on the employee's part and if determined by ICE.

Appendix D – Lean-Agile/DevOpsSec Requirements

Lean-Agile-DevOpsSec Compliance

- All systems development and maintenance projects shall be compliant with ICE OCIO Management Instruction (MI) 001 "Applying Lean-Agile-DevOpsSec Principles at ICE".
- The Contractor shall store and manage all system configuration settings and documentation in the ICE Approved Software Configuration Management (SCM) system, currently GitHub Enterprise.
- The Contractor shall document operational tasks and Standard Operating Procedures (SOPs) in an ICE Approved knowledge management portal, currently ELMS and/or Confluence.
- The Contractor shall leverage an ICE provided automation toolchain (currently Jenkins based) to reduce, if not outright eliminate, the number of manual tasks performed during operations. This includes recurring tasks, scheduled jobs, monitoring, updates, patching, user maintenance, and other operational tasks.
- The Contractor shall perform sufficient* static code analysis in the areas of reliability, security, maintainability, test coverage, and duplication has been performed and is available for review in the ICE Approved Quality Assurance Dashboard (currently SonarQube).

  * "Sufficient" is a moving metric that is expected to improve with time.

- The Contractor shall leverage automation tools to reduce the number of manual tasks performed during the development life-cycle. This includes the test automation (Unit, Functional, Integration, Performance, and Security), build automation, continuous integration, and continuous development.

Associated Deliverables

- The Contractor shall submit a completed ICE Agile Maturity Model Self-Assessment each fiscal quarter. The Government will then provide feedback within 15 business days of delivery.

Appendix E – Travel Authorization Approval Form

TRAVEL AUTHORIZATION APPROVAL FORM

Name					
Travel period					
Location					
Purpose					
Cost Breakdown:					
Airfare					
Train					
Vehicle Rental					
Personal Vehicle					
Hotel (per diem)					
Meals (per diem)					
Miscellaneous					
Total Cost:					

Contractor Manager (sign)_____ Date: _____

Contractor Manager (print) _____ Date: _____

COR (sign) _____ Date: _____

COR (print) _____ Date: _____

Appendix F – List of Acronyms

Acronym	Description
AJAX	Asynchronous JavaScript and XML
ATO	Authorization to Operate
CO	Contracting Officer
COR	Contracting Officer's Representative
COTS	Commercial Off-the-Shelf
DHS	Department of Homeland Security
EIT	Electronic and Information Technology
FAR	Federal Acquisition Regulation
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GFE	Government Furnished Equipment
GFP	Government Furnished Property
GOTS	Government Off-the-Shelf
IAD	Information Assurance Division
ICE	Immigration and Customs Enforcement
ISSO	Information System Security Officer
IT	Information Technology
MD	Management Directive
OAST	Office of Accessible Systems and Technology
OCIO	Office of the Chief Information Officer
OLCD	Office of Leadership and Career Development
O&M	Operations and Maintenance
P.L.	Public Law
SELC	System Engineering Lifecycle
SLM	System Lifecycle Management
SOW	Statement of Work
TMSS	Training Management Support System
TTY	Teletypewriter
XML	Extensible Markup Language