DEPARTMENT OF HOMELAND SECURITY
Science & Technology Directorate
Transportation Security Laboratory

STATEMENT OF WORK (SOW)
FOR
Certification Test Support Services 2

1.0 GENERAL

1.1 BACKGROUND

This statement of work defines ***Certification Test Support Services*** (CTSS2) to the Department of Homeland Security; Science and Technology Directorate (S&T); Transportation Security Laboratory (TSL) in Atlantic City, New Jersey.

The S&T mission is to organize the scientific, engineering and technological resources of the United States and leveraging these existing resources into technological tools to help protect the homeland.

TSL, a tenant organization at the Federal Aviation Administration (FAA) William J. Hughes Technical Center (WJHTC), Atlantic City International Airport, New Jersey supports this effort through its commitment to the DHS national effort to counter current and future terrorist threats and criminal acts, primarily threats against airports. TSL implements these countermeasures through research, testing and implementation of new technologies.

The TSL performs its research, development, testing and evaluation (RDT&E) mission at a complex comprised of 21.5 acres secure, limited access main campus, encompassing over 90,000 square feet of floor space. Facilities include:

1. Building 315 complex consisting of:
   - An administrative office building (Building 315) includes a multipurpose conference/meeting center seating 100, and offices/cubicles for 70 federal staffers and non-federal workers.
   - A triple-wide modular trailer used for additional office space (Building 315A) with approximately 2,300 square feet, which is attached to Building 315, housing approximately 23 additional non-federal workers
   - A laboratory building (315 Labs) attached to the administrative building via a heated/cooled glass enclosed walkway with four (4) hardened laboratory cells for tests involving high explosives and three (3) unhardened laboratory cells for other research and development. The administrative and laboratory buildings cover an aggregate floor space of approximately 35,000 square feet.
2. Two light construction Butler metal buildings, slab-on-grade facilities (Buildings 318 & 319), have approximately 22,000 and 18,000 square feet of floor space respectively.
3. One stand-alone modular facility, known as the Small Bulk Explosives laboratory 315B, which accounts for an additional 400 square feet of floor space.

4. Building 374, containing two large explosives hardened laboratories, a smaller hardened laboratory, a Trace Explosives Contamination Laboratory, and associated conferencing, cubicle space and break rooms. It provides an additional 12,000 square feet of facilities to the total campus facilities footprint in usable floor space.
5. An explosives storage area for approximately 5,300 lbs. of bulk explosives.
6. Within the larger W.J. Hughes Technical Center campus, TSL maintains a remote explosive storage area for approximately 6,000 lbs. of explosives.

1.2 OBJECTIVE

The objective of this statement of work is to provide engineering and technical support services in support of TSL's certification test and evaluation (T&E) assessment missions that support DHS acquisition and procurement of screening equipment.

1.3 SCOPE

The scope of CTSS2 is to provide support services for T&E services for the design of experiments, test execution and test report support services for discovery and conformity tests of sensor systems for use in TSA screening stream-of-commerce (i.e., people, carry-on baggage, checked baggage and air cargo commodities) and in other DHS component (CBP, USSS, and others) screening applications. The products of these services help assess equipment maturity and inform agency investment strategy development as well as support DHS acquisition and deployment decisions. The contractor shall have T&E experience that employ detection systems for screening conventional explosives, homemade explosives, prohibitied items, gas forming reagents, and other contraband (e.g. illicit drugsm currency, etc).

TSL performs between 10 and 20 conformity tests each year encompassing one or more of the following detection systems:

1. Advanced Imaging Technology (AIT)
2. Shoe Scanning Devise (SSD)
3. Bottle Liquid Scanner (BLS)
4. Accessible Property Screening System (APSS)
5. Advanced Technology (AT-2) Screening Devices
6. Explosive or Contraband Trace Detection
7. Explosives Detection System (EDS)
8. Enhanced Metal Detector (EMD)
9. Cargo Screening Systems

1.4 APPLICABLE DOCUMENTS

1.4.1 Compliance Documents

The following documents provide specifications, standards, or guidelines that must be complied with in order to meet the requirements of this contract. These documents will be provided upon contract or task order award:

a) National Industrial Security Procedures Operations Manual (NISPOM) https://www.federalregister.gov/documents/2021/08/19/2021-17688/national-industrial-security-program-operating-manual-nispom-amendment
b) 49 CFR 1520 Protection of Sensitive Security Information
c) DHS S&T Explosives Research and Development Program Security Classification Guide, DHS SCG S&T-006.1
d) DHS IT Security Program Publication DHS MD 4300.1.
e) TSL Standard Operating Procedures
f) TSL Laboratory Safety Action Plans
g) TSL Management Instructions
h) TSL Management Directives
i) Explosive Safety Program and Operations, Management Directive MD20-03
j) Policy Regarding TSL Contracted Explosives Handlers
k) DD254
l) Guidelines for Formatting and Preparing TSL Documents for Submission
m) DHS/S&T/TSL Document Format Templates
n) DHS Instruction 121-01-011.
o) HSAR Class Deviation 15-01 Safeguarding of Sensitive Information

1.4.2 Reference Documents

The following documents may be helpful to the Contractor in performing the work described in this document:

a. Management Plan for the Certification Testing of Checked Baggage Inspection Systems, DHS/ST/TSL-10/50
b. Management Plan for Advanced Technology-2 Systems (Qualification) Test and Evaluation July 2011, DHS/ST/TSL-11/94
c. Management Plan for Bottle Liquid Scanner (BLS) (Qualification) Test and Evaluation, DHS/STD/TSL-08/06, April 2008
d. Certification Management Plan for Test & Evaluation of Explosives Trace Detectors for Checkpoint and Checked Baggage Screening, DHS/ST/TSL-15/42
e. Management Plan for the Detection Certification Test of Advanced Imaging Technology (AIT-1), 18 April 2017, DHS/ST/TSL-17/38

2.0 REQUIREMENTS – CTSS-2 MISSION TASKS

Nine major tasks define the test support services to be acquired under this contract. All of these tasks support the objective defined in Section 1.3.

a) Test Design
b) Test Planning, Preparation and Execution
c) Test Safety
d) Configuration Management
e) Manufacturer Surveillance
f) International Test Program Harmonization
g) Independent Verification Validation and Accreditation
h) Briefings & Meetings

i) Test Service Management

2.0.1 Definitions.

a) **LABORATORY ASSESSMENT** – This is a narrowly focused conformity assessment on selected requirements and limited scope. Examples include Technology Readiness Level (TRL) Rating / Baselining.

b) **PRE-CERTIFICATION TEST -** This is a limited scope test to determine readiness to enter certification testing.

c) **CERTIFICATION TESTING -** This is an evaluation of conformity to specific detection performance standards for government or 3rd party acquisition.

d) **VULNERABILITY TEST** – This is an exploratory test to discover systemic vulnerabilities in the laboratory. This includes expanded tests to probe and characterize potential weaknesses or vulnerabilities observed during one of the other test activities.

e) **PLACEMAT** - This is a classified, summary table of key data by test including system configuration, date, scope and key test results. This is a deliverable required for each test.

2.1 TEST DESIGN

The Contractor shall support the design of certification and qualification tests. Test design activities will include all or some of the following:

a. Analyzing critical operational issues and test objectives;
b. Defining levels, measures, factors and criteria;
c. Collecting data to measure equipment parameters to inform design;
d. Developing sampling designs;
e. Identifying and validating design assumptions;
f. Analyzing major threats to internal and external validity, developing methods to control or mitigate effects and validating method;
g. Reducing and analyzing data using appropriate statistical tests;
h. Conducting and compiling literature search/survey/analysis.

2.2 TEST PLANNING, PREPARATION & EXECUTION

The Contractor shall plan, prepare and execute tests to explore, evaluate and/or verify detection and other critical system performance. Test planning, preparation and execution include:

a. Acquiring, designing, developing, fabricating and/or validating test materials – for use in test execution or by another DHS agency - this also includes cutting, weighing, shaping, packaging and labeling energetic materials and simulants for use as test targets;
b. Measuring, compiling and recording physical target properties and related design in a government explosive target database (challenge matrices);

c. Acquiring, designing, specifying, fabricating, evaluating and/or validating test jigs & tools including automated data recording, database management and instrumentation – both developed or acquired by the Contractor or developed or acquired by a third party;
d. Acquiring, training, verifying training, measuring and/or managing human test participants;
e. Operating, maintaining and calibrating test instrumentation;
f. Calibrating, checking and operating systems under-test;
g. Managing and controlling both property and data inventory;
h. Facilitating and managing special test facilities when Government facilities are not adequate or not available;
i. Communicate test interfaces, processes, equipment, functional & data requirements and expectations to equipment manufacturers;
j. Evaluating draft detection performance requirements for testability and conduct studies to analyze, derive and/or estimate test needs for test planning;
k. Assessing test planning and preparation readiness and documenting in a test readiness review checklist;
l. Analyzing, evaluating, summarizing, archiving and reporting.

2.3 TEST SAFETY

The Contractor shall establish and maintain an Institutional Review Board (IRB) in accordance with 21 CFR 50 (Protection of Human Subjects), 21 CFR 56, 45 CFR 46 and DHS Management Directive 026-04 prior to implementing any work with human participants under this Contract. While test safety is a *process* requirement equivalent in importance to security and privacy process requirements, there are unique service requirements related to the CTSS-2 mission that warranted this task inclusion in Section 2.

As part of the IRB, the contractor shall provide test safety review and approval from a board-certified physician, health physicist, and industrial hygienist, certified public health professional and legal counselor who specializes in product safety consistent with IRB requirements to support test operations. Additionally, prior to enrolling participants or conducting test activities involving human subjects, a project-specific Certification of Compliance letter must be issued by the DHS Regulatory Compliance Office. To obtain this letter, the Contractor must submit a copy of the following items to the Contracting Officer (CO) and Contracting Officer's Representative (COR) for the DHS Regulatory Compliance Office (RCO):

1. Research protocol, as approved by an Institutional Review Board (IRB)
2. IRB approval letter (or notification of exemption);
3. IRB-approved informed consent document(s) or IRB waiver of informed consent;
4. Federal-wide Assurance (FWA) number from the HHS Office for Human Research Protections (OHRP), or documentation of other relevant assurance, for all organizations (including sub-awardees) involved in the human subjects portion of the research.

The Contractor shall promptly report the following to the RCO via the COR and CO along with the corrective actions taken:

1. Any serious or continuing noncompliance with human subjects research regulations and policies adopted by DHS (as referenced above);
2. Suspension, termination, or revocation of IRB approval of any human subjects research activities conducted under this award.

2.4 T&E SUPPORT TO CONFIGURATION MANAGEMENT

The Contractor shall support the following configuration management activities:

a. Provide support for the review and analysis of Configuration Item (CI) documentation including OEM drawings;
b. Participate in physical and functional configuration audits and assist in establishing developmental and certified product baselines;
c. Review in-depth configuration audit reports.

2.5 MANUFACTURER'S TEST PROGRAM SURVEILLANCE

The Contractor shall perform the following sub-tasks and assist the Government in support of monitoring extramural engineering and test activities as applicable:

a. Verifying requirements for solicitations
b. Evaluating manufacturers' preliminary and critical designs;
c. Evaluating manufacturers' requirements verification plans and procedures;
d. Witnessing and/or evaluating the manufacturers' requirements verification activities and/or substantiation of conformity;
e. Participating in Government and/or manufacturer technical discussions and reviews related to manufacturer's product.

2.6 INTERNATIONAL TEST PROGRAM HARMONIZATION SUPPORT

The Contractor shall record, edit, clarify, compile and catalog test standard operating procedures (SOPs) and protocols to support harmonization of US and international certification test agencies associated with explosives, weapons and/or other contraband detection.

2.7 INDEPENDENT VERIFICATION, VALIDATION and ACCREDITATION

The Contractor shall develop and execute an independent verification, validation and accreditation (IVVA) system for simulants (to be used in lieu of explosives) for test missions by TSL and by other United States Government (USG) agencies. This IVVA system includes developing & maintaining test protocols, managing sample inventory, measuring, auditing, evaluating and reporting. TSL will supply a baseline validation protocol. This does not include simulant design, fabrication, production or disposal.

2.8 BRIEFINGS AND MEETINGS

Frequently the Contractor will need to explain their test activities and/or related processes to coordinate, integrate, inform or defend, and as such, the Contractor shall prepare, provide briefing material and/or conduct briefings of activities, and facilitate productive meetings by

recording minutes of contract process meetings involving COR, CO or Technical Monitor, and/or of chartered test working group meetings (related to this SOW), if a named member or representing a named member.

2.9 TEST SERVICE MANAGEMENT

The Contractor shall prepare and provide a plan to include how they will manage and address the following:

a. Employee labor will be managed;
b. Employee skills are maintained;
c. To ensure that employees, subcontractors and company do not possess a conflict of interest;
d. SOW requirements will accomplished;
e. Process and deliverable quality will be assured;
f. Deliverable rework is monitored; and
g. Employees will follow this plan as an Operating Instruction.

The Contractor shall document this planning in a project plan.

3.0 CONTRACTOR PERSONNEL

3.1 LABOR CATEGORY QUALIFICATIONS

3.1.1 See separate document defining labor category qualifications.

3.1.2 Test & evaluation services in CTSS-2 require a balance of physical/chemical science and engineering as well as skills and experience in computer science, decision science, statistics, data science and/or operations research. Sensitive data analysis can only be processed on-site.

3.1.2 Test & evaluation services in CTSS-2 will encompass state-of-the-art and advanced prototype sensors that require following sometimes complex or under-developed calibration, diagnostic and operation protocols which require technical insight to ensure test competency. Renaissance or full-stack technical expertise in the following areas is not required, but a technical foundation with the ability to comprehend quickly is:

> X-ray imaging, threat characterization, computerized tomography, x-ray diffraction, x-ray fluorescence, microscopy, dielectrometry, nuclear magnetic resonance, nuclear quadruple resonance, image processing, artificial intelligence, data/sensor fusion, texture analysis, statistics, analytic chemistry, ion mobility spectrometry, chromatography, metal detection and trace detection methods.

3.2 KEY PERSONNEL

The investment of cost and time to provide CTSS-2 personnel that meet & follow CTSS-2 process requirements with the knowledge & skills of managing complex, hazardous testing along with unique sensitivities associated with certification testing preclude the CTSS-2 Contractor from floating employees. The CTSS-2 mission requires the designation and approval of key personnel to stabilize service delivery and minimize disruptions to critical mission operations. Consequently, the Contractor shall submit candidates (to key positions) to the CO for approval. If approved, the Contractor shall follow a special procedure to seek CO approval *before* replacing that key employee.

The CO's approval of a candidate employee to a key position is specific only to that position and does not mean automatic or broad approval for other key CTSS-2 positions. Before replacing any individual designated as *Key*, the Contractor shall notify the CO not less than 15 business days in advance as practical. The Contractor shall submit written justification, provide the name & qualifications of any proposed substitute(s) and obtain the CO's approval. All proposed substitutes must satisfy the *key* position requirements unless otherwise approved by the CO.

3.3 PROGRAM MANAGER – Key Personnel

3.3.1 DESIGNATION

The Contractor shall designate & provide a Program Manager, assigned as key personnel, who is responsible for all Contractor work performed under this SOW and is a single point of contact to the CO and the COR. The Contractor shall provide the name of the Program Manager, and the name(s) of any alternate(s) who will act for the Contractor in the absence of the Program Manager.

3.3.2 SUPERVISION

The Program Manager is responsible for providing administrative and technical supervision of all CTSS-2 employees as well as test mission and testmanship cognizance. The Program Manager and all designated alternates shall be able to read, write, speak and understand English. The Program Manager shall be available to the COR via telephone between the core hours of 8:00 am and 4:00 pm EST, Monday through Friday, and shall respond to a request for discussion or resolution of technical problems within 2 hours of notification.

3.3.3 CONTINUOUS SERVICE DELIVERY

The Contractor shall ensure that contractually agreed to level & type of support is maintained at all times. The Contractor shall ensure that all contract support personnel are present for all hours of the workday. If, for any reason, the Contractor staffing levels are not maintained due to vacation, leave, appointments, etc., and replacement personnel will not be provided, the Contractor shall provide e-mail notification to the COR prior to employee absence. Otherwise, the Contractor shall provide a fully cleared, suitable and qualified, temporary replacement.

3.4 LEADS- Key Personnel

The Contractor shall designate CTSS-2 LEAD (Program Manager) – one for each of the 3 IT&E branches:

- Passenger Spectroscopy (AIT/EMD),
- X-ray (EDS/APSS/Cargo),
- Chemistry (ETD/BLS).

Each LEAD proposed will be assigned as key personnel. The designated LEAD will have an on-site seat at TSL (see section 4.3.2) and must obtain & maintain an ability to operate the detection equipment of the test service lines, understand & be able to explain how it works, possess a working knowledge of detection standard requirements, and exercise team leadership.

3.5 OBJECTIVITY

The work performed on this contract provides independent, third party services free from conflicts of interest. The contractor shall maintain a firewall between any (CTSS-2) personnel and other employee personnel by:

3.5.1 Written Certification - The contractor and its staff shall not possess a conflict of interest, and shall certify to this in writing.
3.5.2 Dedicated Labor - The contractor shall not move or re-direct labor personnel delivering services from this contract to a non-(CTSS-2) contract without approval from the COR and Contracting Officer.
3.5.3 Separate Program Management - The contractor shall have a reporting chain that differs from labor contracts associated with R&D or DT&E contracts associated with the product lines tested.
3.5.4 Separate Workspace - The contractor shall physically segregate office cubicles for offsite personnel working under the contract, if co-located with R&D or DT&E contracts personnel associated with the product lines tested.
3.5.5 IT Security - The contractor shall put in place IT firewall security provisions.
3.5.6 INFOSEC - The contractor shall follow the (CTSS-2) Test Operations Security Guide and sign the DHS non-disclosure form.
3.5.7 Training - The contractor shall include TEST OPERATIONS SECURITY in its periodic security training program.

3.6 EMPLOYEE IDENTIFICATION

3.6.1 VISITING CONTRACT EMPLOYEES

CTSS-2 contract employees based off-site who visit Government facilities shall wear an identification badge that, at a minimum, displays the Contractor name, the employee's photo, name and badge expiration date. All Visiting contractor employees shall identify themselves as Contractors when their status is not readily apparent.

3.6.2 ON-SITE CONTRACT EMPLOYEES

CTSS-2 Contract employees approved to work on-site *full-time* at Government facilities shall wear a Government issued identification badge. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent (in meetings, when answering Government telephones, in e-mail messages, etc.) and display the Government issued badge in plain view above the waist at all times.

3.7 CONTRACT EMPLOYEE CONDUCT

3.7.1 POLICIES & PROCEDURES

The Contractor is responsible for training and ensuring that its employees comply with all Federal, S&T, FAA Technical Center and TSL policies and procedures when visiting or working at Government facilities. Though contract employees may be permitted to attend special Federal training on-site or on-line (such as safety, security and PII protection), this courtesy service does not replace or supersede the Contractor's obligation for training and ensuring competency and/or compliance.

3.7.2 CONDUCT & APPEARANCE

a) The contractor shall ensure employees present a professional appearance at all times and that the conduct reflects credit on the United States and the Department of Homeland Security.
b) Contractors must wear attire appropriate to perform these requirements in a laboratory environment.
c) Contractor employees shall comply with all applicable Government regulations, policies, and procedures (e.g., fire, safety, sanitation, environmental protection, security, "off-limits" areas, wearing of parts of DHS uniforms, possession of weapons/prohibited items) when visiting or working at Government facilities.
d) The Contractor shall ensure its employees understand and abide by DHS, S&T and TSL established rules, regulations and policies concerning safety and security.

3.7.3 REMOVAL

The Government, via the COR, may unilaterally direct the Contractor to remove any Contractor employee from Federal facilities *for misconduct or security reasons*. Removal of a contract employee does not relieve the Contractor of the responsibility to continue providing the services required under the contract. The CO will provide the Contractor with a follow-up written explanation to support any request to remove an employee. Removal may be assisted by the TSL armed security guard force. Individuals are not permitted to return to TSL to retrieve any personal items. This duty can be deferred to the individual's program manager.

3.8 EMPLOYEE SAFETY

The Contractor is responsible for training, providing personal protective equipment / clothing and ensuring that its employees (and subcontracted employees) comply with all Federal regulation and S&T, FAA Technical Center and TSL policies and procedures when visiting or working at Government facilities.

4.0 OTHER APPLICABLE CONDITIONS

4.1 SECURITY

Security requirements are found in the DD Form 254 attached to the contract. The DD Form 254 provides to the Contractor the security requirements and the classification guidance that would be necessary to perform on this contract. The Contractor shall appoint a Corporate Security Officer (CSO). The CSO shall interface with the DHS Office of Security through the COR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the Contractor.

The Contractor shall adhere to all applicable government laws, regulations, orders, guides, and directives pertaining to classified, Sensitive BUT Unclassified (SBU), For Official Use Only (FOUO) information. The contractor shall safeguard SBU, FOUO information specifically in accordance with the DHS Management Directive 11042.1 and in compliance with HSAR Class Deviation 15-01 Safeguarding of Sensitive Information.

1) CTSS-2 contract employees may require access to classified information to perform tasks in this SOW. The maximum level of classification is SECRET. The details will be provided in a Department of Defense (DD) Form 254.

and

2) CTSS-2 contract employees may require access to unclassified, but Security Sensitive Information to perform task in this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination.

4.1.1 FAR 52.204-2 Security Requirements. (AUG 1996)

(a) This clause applies to the extent that this contract involves access to information classified "Confidential," "Secret," or "Top Secret."

(b) The Contractor shall comply with—

(1) The Security Agreement (DD Form 441), including the *National Industrial Security Program Operating Manual* (DoD 5220.22-M); and

(2) Any revisions to that manual, notice of which has been furnished to the Contractor.

(c) If, subsequent to the date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of this contract.

(d) The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph (d) but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.

4.1.2 SECURITY CLEARANCE REQUIREMENTS

The Government will provide specific guidance to the Contractor as to which work will be conducted in a classified manner and at which classification level. See section 6.3(2).

4.1.3 ***Government Furnished Materials.*** All work performed shall be done using government-furnished equipment. The Government will make available the materials, computers, office space, communications capability, and information necessary for the contractor to complete the assigned tasks. If network access is necessary, then a Government computer will be issued once the individual contractor has completed the mandatory screening and receives suitability. A

DHS badge is required for computer access and login. In many cases temporary Government space will be made available for the contractor to perform their tasks. Some work can be performed at the contractor's facility. All Government furnished materials will be returned at the completion of the task. The contractor will be responsible for any Government issued materials such as computers.

4.1.4 Safeguarding of Sensitive Information (HSAR Deviation 15-01, March 2015)

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

(b) Definitions. As used in this clause—

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as 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:

> (1) 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);

(2) 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);

(3) 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

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

"Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) Authorities. The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
(2) DHS Sensitive Systems Policy Directive 4300A
(3) DHS 4300A Sensitive Systems Handbook and Attachments
(4) DHS Security Authorization Process Guide
(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
(7) DHS Information Security Performance Plan (current fiscal year)
(8) DHS Privacy Incident Handling Guidance
(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html
(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

(d) Handling of Sensitive Information. Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The DHS Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook provide the policies and procedures on security for Information Technology (IT) resources. The DHS Handbook for Safeguarding Sensitive Personally Identifiable Information provides guidelines to help safeguard SPII in both paper and electronic form. DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA), as a condition of access to such information. 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) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) Authority to Operate. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the DHS Sensitive Systems Policy Directive 4300A (Version 11.0, April 30, 2014), or any successor publication, DHS 4300A Sensitive Systems Handbook (Version 12.0, Nov 2015), or any successor publication, and the Security Authorization Process Guide including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) 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 all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) Renewal of ATO. Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) Security Review. The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the

Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) Continuous Monitoring. All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with FIPS 140-2 Security Requirements for Cryptographic Modules and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) Revocation of ATO. In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) Federal Reporting Requirements. Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) Sensitive Information Incident Reporting Requirements.

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with 4300A Sensitive Systems Handbook Incident Response and Reporting requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract.

If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use FIPS 140-2 Security Requirements for Cryptographic Modules compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in 4300A Sensitive Systems Handbook Incident Response and Reporting, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime contractor location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
(v) Contracting Officer POC (address, telephone, email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(xiii) Government programs, platforms or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

(g) Sensitive Information Incident Response Requirements.

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in

consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

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

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

(i) Inspections,
(ii) Investigations,
(iii) Forensic reviews, and
(iv) Data analyses and processing.

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

(h) Additional PII and/or SPII Notification Requirements.

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the DHS Privacy Incident Handling Guidance. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

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

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

(vi) Information identifying who individuals may contact for additional information.

(i) Credit Monitoring Requirements. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or

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

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

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

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

(j) Certification of Sanitization of Government and Government-Activity-Related Files and Information. As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in NIST Special Publication 800-88 Guidelines for Media Sanitization.

4.1.5 Information Technology Security and Privacy Training (HSAR Deviation 15-01, March 2015)

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

(b) Security Training Requirements.

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

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

(c) Privacy Training Requirements. All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take Privacy at DHS: Protecting Personal Information before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

4.1.6 FACILITY SECURITY CLEARANCE REQUIREMENTS

Access to classified information is required under this contract. The Contractor shall possess a SECRET level facility security clearance or demonstrate the ability to obtain a SECRET level facility security clearance.

4.1.7 INSPECTION

The COR and the DHS Office of Security reserve 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 CO of the proper action required for security compliance.

4.1.8 TERMINATION & RESIGNATIONS

The DHS Security Office, CO, and COR shall be notified of all personnel terminations/ resignations within five (5) days of occurrence. The Contractor shall return to the COR all DHS issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the pass or card number, name of individual to whom it was issued and the last known location and disposition of the pass or card.

4.1.9 CONTRACT EMPLOYEE ELIGILITY

4.1.9.1 Only U.S. citizens and lawful permanent residents (LPR) are authorized to perform on this contract. However, LPRs are not authorized to perform in any position that requires the LPR to access or assist in development, operation, management or maintenance of DHS Information Technology systems.

4.1.9.2 The Contractor shall ensure that each employee working on this contract has a Social Security Card issued and approved by the Social Security Administration.

4.1.9.3 The Contractor (or its subcontractors) shall not employ illegal or undocumented aliens to perform under this contract. The Contractor shall ensure that this provision is expressly incorporated into any and all subcontracts or subordinate agreements issued in support of this contract.

4.1.10 CONTRACT EMPLOYEE SUITABILITY

Contract employees (to include applicants, temporaries, part-time and replacement employees) requiring 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. All background investigations will be processed through the DHS Security Office. Prospective contractor employees shall submit the following completed forms to the DHS Security Office. The Standard Form 85P will be completed electronically, through the Office of Personnel Management's e-QIP SYSTEM. The completed forms must be given to the DHS Security Office no less than thirty (30) calendar days before the start date of the contract or thirty (30) calendar days prior to entry on duty of any employees, whether a replacement, addition, sub-Contractor employee, or vendor:

a. Standard Form 85P, "Questionnaire for Public Trust Positions"
b. FD Form 258, "Fingerprint Card" (2 copies)
c. DHS Form 11000-6 "Conditional Access To Sensitive But Unclassified Information Non-Disclosure Agreement"
d. DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"

Only complete packages will be accepted by the DHS Security Office. Specific instructions on submission of packages will be provided upon award of the contract.

4.1.9 OTHER SECURITY PROCESS REQUIREMENTS

4.1.9.1 FULL CONTROL

DHS has and 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. DHS may, as it deems appropriate, authorize and make a favorable *entry of duty (EOD)* decision based on preliminary security checks.

4.1.9.2 FAVORABLE *EOD*

A favorable *EOD* decision would allow the contactor to commence work temporarily prior to the completion of the full investigation. The granting of a favorable *EOD* decision shall not be considered as assurance that a full employment contractor fitness (suitability) authorization will follow as a result thereof. The granting of a favorable *EOD* decision or a full contractor fitness (suitability) authorization determination shall in no way prevent, preclude or bar the withdrawal or termination of any such access by DHS, at any time during the term of the task order.

4.1.9.3 UNESCORTED ACCESS

No employee of the contractor shall be allowed unescorted access to a Government facility, access to any sensitive information or access to DHS IT Systems without a favorable *EOD* decision or contractor fitness (suitability) determination by the DHS Office of Security.

4.1.9.4 CONTRACT EMPLOYEES NOT NEEDING ACCESS

Contract employees assigned to the task order not needing access to sensitive DHS information, DHS systems or access to DHS facilities will not be subject to security contractor fitness (suitability) screening.

4.1.9.5 PENDING STATUS

Contract employees waiting an *EOD* decision may not begin chargeable work under this contract.

4.1.9.6 ESCORTED ACCESS

Limited access to Government buildings is allowable prior to the *EOD* decision if the contractor is escorted by a Government employee. This limited access is to allow contractors to attend kick-off meetings and initial briefings.

4.1.9.7 CLASSIFIED INFORMATION

Classified information is Government information which requires protection in accordance with Executive Order 13526, National Security Information (NSI) as amended and supplemental directives. If the Contractor has access to classified information at a DHS owned or leased facility, it shall comply with the security requirements of DHS and the facility. If the contractor is required to have access to classified information at another Government Facility, it shall abide by the requirements set forth by that agency.

4.1.9.8 CONTINUED SUITABILITY

a. The DHS Office of Security may require the Contractor to perform drug screening for probable cause at any time, and/or when the Contractor independently identifies, circumstances where probable cause exists.

b. The Government reserves the right to deny facility and information access to any Contractor employee whom the Government believes may compromise or mishandle sensitive or classified information, or whose actions are in conflict with the standards of conduct, 5 CFR 2635 and 5 CFR 3801.

c. The Contractor shall immediately report to the DHS Office of Security any credible information in their possession that calls into question a Contractor employee's desire or ability to legally and appropriately handle sensitive or classified information. The termination of an employee does not obviate the requirement to submit this report. The report shall include the employee's name and social security number, along with the adverse information being reported.

4.2 PERIOD OF PERFORMANCE

The period of performance for this contract is a 12-month base period with four one-year option periods, estimated as follows:

Base Period
Option Period One
Option Period Two
Option Period Three
Option Period Four

4.3 PLACES OF PERFORMANCE

4.3.1 WORK LOCATIONS

The primary places of performance are listed below:

(a) Department of Homeland Security
Transportation Security Laboratory at the FAA William J. Hughes Technical Center,
Atlantic City International Airport, NJ 08405

(b) TBD

(c)
Defense Security Service
Industrial Security Field Office (IOFNM)
1000 Atrium Way, Suite 310
Mt. Laurel, NJ 08054-3906

4.3.2 ON-SITE WORKSPACE

The Government will provide dedicated workspace at the TSL for the up to eight (8) employees. The contractor shall propose employees to *reside* onsite at TSL. No other contractor personnel will be considered as on-site staff at the TSL for the duration of this contract.

4.3.3 TELEWORK

Telework is to be used to accommodate inclement weather days when the Government is open. Telework may be used as a standard occurrence such as a weekly/bi-weekly telework day(s), per the provisions below. Telework will not be used when the Government is closed without express written advance authorization from the COR or Contracting Officer, even if it is a regularly scheduled telework workday for that contractor employee, given the time frame available for Government oversight to be provided will be contingent upon the COR's availability.

1. Regular Re-Occurring Telework: Telework may be performed under a task order based on job function and not on the preference of individuals performing the task. The TM will be responsible for making the determination as to which functions on a contract or task order are telework eligible and if the following conditions are met:

a) There must be a telework agreement in place between the Contractor and their company specifying dates, times, and location for telework. The Contractor PMPM must provide a copy of each signed agreement to the Government (Technical Monitor, Contracting Officer, and the COR) for the task order records.

b) The number of scheduled telework days may not exceed 2 days per week. Work under a task order can only be completed on a DHS issued laptop via the DHS VPN connection or using the Virtual Desktop Interface (VDI)

c) The Contractor PM must ensure that Contractor employees are reachable via telephone by the COR at the telework location.

d) The PM must state the hours that a given Contractor employee will be online and working, and any hours the employee will be unavailable.

e) Any contractor employee authorized for regular re-occuring telework may still be required to report to the laboratory as needed and at the discretion of the TM and COR.

2. Situational Telework: Situational Telework, anything outside of regularly scheduled telework, may be performed if the following conditions are met:

a) Prior approval to telework must be obtained in writing from the task order COR by the PM. All requests must originate from the Contractor's PM, or the Contractor's responsible contracts representative. Tasking must be able to be accomplished efficiently and effectively in a remote fashion and must be of sufficient quantity to fill the duration of the planned telework period for a given Contractor employee.
b) The task order TM must review all tasks to be completed/worked on during the telework period prior to providing written approval or disapproval of the PM's written request.
c) Work under the Task Order can only be completed on a DHS issued laptop via the DHS VPN connection or using the Virtual Desktop Interface (VDI).
d) A detailed weekly contractor activity report for all eligible telework employees is required to be submitted by the Contractor PM to the TM no later than COB Monday following the previous week worked. A courtesy copy of the report will be provided to the COR for the contract file.
e) The PM must ensure that Contractor employees are reachable via telephone at the telework location.
f) The PM must state the hours that a given Contractor employee will be online and working, and any hours the employee will be unavailable.
g) Any contractor employee authorized for regular Situational telework may still be required to report to the laboratory as needed and at the discretion of the TM and COR.

3. Telework may only take place within the Atlantic City area at one of the following locations, provided the COR has given prior written approval:
a) The Contractor's facility
b) The Contractor employee's place of residence (within 50 miles of the TSL)

4. Individuals with off-site positions are to report to the government or contractor facility as listed in the contract unless situational telework has been previously authorized. Off-site positions shall not be interpreted as being telework or telework eligible positions. All off-site work shall be completed at an approved government or contractor location, not from the employee's home, unless situational telework has been approved and the TM and COR have provided concurrence.

5. The contractor shall provide a breakdown in the Monthly Report the hours spent teleworking vs the employee's standard schedule.

6. Situational telework is not equivalent to an alternate work schedule. No alternate work schedules are permitted.

7. Situational telework shall not result in an increase in the contract price. Any situational telework hours that are worked shall be charged at the lowest available rate for that labor category.

8. Any equipment provided by the Government for situational telework purposes shall be treated as Government Furnished Equipment (GFE). A valid property pass must be on file for any GFE utilized for situational telework. Copies of all property passes must be provided to the COR prior to the start of telework. For LabNet computers to be removed from the TSL, the contractor must verify that the system has a VPN installed. In addition, notification must be sent to the TM that the equipment is being taken home for telework and will be returned when the contractor is not teleworking. The contractor must state that they will ensure that the LabNet computer is connected to the VPN for Updates/Scans and patches.

9. Classified work shall beperformed at the Government location only.

Alternate work schedules may be considered and may be approved with technical monitor and COR concurrence and approval.

4.4 HOURS OF OPERATION

TSL Core hours of operation are 10:00 am to 3:00 pm with the TSL opened from 6:00 am to 6:00 pm. Contractor employees shall generally perform all work between the hours of 8:00am and 5:00pm EST, Monday through Friday (except Federal holidays). However, there may be occasions when Contractor employees (primarily those support testing) shall be required to work other than core hours, including second, and third shifts, weekends, and holidays to fulfill requirements under this SOW and awarded task orders.

The TSL federal facility will be closed on Federal holidays and when dictated by emergency.

4.5 TRAVEL Contractor travel may be required under this contract. Locations may include manufacturer's facilities, customer facilities or airports to deliver services under this contract. All required travel outside the local commuting area will be reimbursed to the Contractor in accordance with the Federal Travel Regulations. The Contractor shall obtaining COR approval (e-mail is acceptable) for all reimbursable travel in advance of each travel event. Trip reports

shall be submitted within 3 business days after return of trip and shall describe purpose and outcome of trip.

4.6 MATERIAL COSTS

The contractor may be required to purchase materials in support of this work effort. The contractor shall obtain written consent from the COR before purchasing any individual material item exceeding $2,000.00. All COR approved purchases shall become the property of DHS. The Contractor shall maintain any such items according to currently existing property accountability procedures. The Contracting Officer and COR will determine the final disposition of any such items.

Examples of material purchases with scope include:

Test Articles; components; consummables	Subject Matter Experts as third party consultants
Test participants	Test equipment and test apparatus
Data collection samples and supplies	Electronic data storage
Misc. supplies	modeling and data analysis software or tools
Maintenance, repairs, or service agreements for equipment and test apparatus	Replacement parts for laboratory equipment
data analysis/test design computer equipment	Data analysis/test design computers
Safety equipment / PPE	Computer simulation and analytical tools - hardware/software

4.7 POST AWARD CONFERENCE

The Contractor shall attend a Post Award Conference with the CO and the COR no later than 14 business days after the date of award. The purpose of the Post Award Conference, which will be chaired by the CO, is to discuss technical and contracting objectives of this contract and review the Contractor's Project Plan described in section 2.9. The Post Award Conference will be held at the Government's facility, located at DHS/Transportation Security Laboratory, FAA William J. Hughes Technical Center, Atlantic City International Airport, NJ; and can include teleconference participation.

4.8 BUSINESS CONTINUITY PLAN

4.8.1 PLAN

The Contractor shall prepare and submit a Business Continuity Plan (BCP) to the Government. The BCP Plan shall be due 20 business days after the date of award, and will be updated as needed. The BCP shall document Contractor plans and procedures to maintain support during an emergency, including natural disasters and acts of terrorism. The BCP, at a minimum, shall include the following:

a. A description of the Contractor's emergency management procedures and policy
b. A description of how the Contractor will account for their employees during an emergency
c. How the Contractor will communicate with the Government during emergencies

d. A list of primary and alternate Contractor points of contact, each with primary and alternate telephone numbers and e-mail addresses.

4.8.2 USE

Individual BCPs shall be activated immediately after determining that an emergency has occurred, shall be operational within 48 hours of activation or as directed by the Government, and shall be sustainable until the emergency situation is resolved and normal conditions are restored or the contract is terminated, whichever comes first. In case of a life threatening emergency, the COR shall immediately make contact with the Contractor Program Manager to ascertain the status of any Contractor personnel who were located in Government controlled space affected by the emergency. When any disruption of normal, daily operations occur, the Contractor Program Manager and the COR shall promptly open an effective means of communication and verify:

a. Key points of contact (Government and contractor)
b. Temporary work locations (alternate office spaces, telework, virtual offices, etc.)
c. Means of communication available under the circumstances (e.g. email, webmail, telephone, FAX, courier, etc.)
d. Essential Contractor work products expected to be continued, by priority

4.9 GENERAL REPORT REQUIREMENTS

This section describes general reporting requirements. Section 4.9 defines progress reporting. Section 8.0 outlines the process for Government acceptance of deliverables. Section 9.0 lists specific report deliverables.

4.9.1 FORMAT

The Contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with DHS workstations (i.e., latest version of Windows and Microsoft Office Applications or current DHS system requirements). All deliverables shall conform to existing DHS/TSL publication standards (TSL Publication Guidelines and DHS/S&T/TSL Document Format Templates).

4.9.2 PUBLICATION

All documentation shall be written for publication by the TSL unless authorized by the COR in writing in advance.

4.9.3 SHAREPOINT

The Contractor shall post each unclassified deliverable as it is accepted (and where relevant – registered) to the CTSS-2 Sharepoint database, submit deliverables as required in sec. 9.0 then issue notification to the COR. The Contractor shall use their Government–provided access to the Homeland Security Data Network to deliver classified deliverables via secure e-mail or into a unique share-drive after their registration. The Contractor shall store other unclassified records in locked GFR cabinets within the TSL laboratory.

4.9.4 DATA RECORDS

The Contractor shall manually and legibly record all activities performed (as determined by the Technical Monitor) in hardcover laboratory notebooks or laptops. The contractor shall manually or digitally sign and date each spreadsheet, log or page certifying its accuracy and completeness.

4.9.6. QUICK LOOK REPORTS. A Quick Look Report provides a brief synopsis of what was performed/tested; why the test was conducted; where and when the test was conducted; along with a brief test protocol and presentation of the preliminary test results. It must be required in writing by the technical monitor, be technical in nature, to the point and provide conclusions and recommendation if applicable *(no raw data)*. Limited to no more than 10 pages, and delivered within two (2) days of the request.

4.10 REPORTING PROGRESS

4.10.1 MONTHLY PROGRESS REPORT

The contractor shall provide a monthly progress report (MPR) to the CO and COR via e-mail on the 10th day of each month. This report shall include a summary of all Contractor work performed including a breakdown of labor hours by labor category, all direct costs by line item, an assessment of technical progress, schedule status, any travel conducted and any Contractor concerns or recommendations for the previous reporting period; plans for next month's activities; risk identification/realization; and any actions/activities for immediate COR attention. The Contractor shall notify the COR and CO of each deliverable using an e-mail transmittal letter. The Contractor can recommend changes to the MPR format.

4.10.2 CONTRACT MANAGEMENT REVIEWS

The CTSS-2 Program Manager shall be available to meet with the COR or TSL Technical Monitor upon request to present deliverables, discuss progress, exchange information and/or resolve emergent technical problems and issues. It is not intended to be a forum for technical interchange, specific test planning, analysis, customer requirements, equipment issues or technical aspects of the mission.

4.11 PROTECTION OF INFORMATION

4.11.1 PERSONALLY IDENTIFIABLE INFORMATION

Contractor access to information protected under the Privacy Act is required under this SOW. Contract employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with the law and Government policy and regulation. The Contractor is responsible for training and ensuring that its employees comply with all Federal regulation and S&T and TSL policies and procedures for collecting, handling and storing personally identifiable information (PII) and sensitive PII. See:
https://www.dhs.gov/xlibrary/assets/privacy/privacy_safeguarding_pii_fact_sheet.pdf

4.11.2 PROPRIETARY INFORMATION

Contractor access to proprietary information is required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with DHS MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only)

Information. The Contractor shall ensure that all Contractor personnel having access to business or procurement sensitive information sign a non-disclosure agreement (DHS Form 11000-6).

4.11.3 SECTION 508 COMPLIANCE

Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) as amended by P.L. 105-220 under Title IV (Rehabilitation Act Amendments of 1998) all Electronic and Information Technology (EIT) developed, procured, maintained and/or used under this contract shall be in compliance with the "Electronic and Information Technology Accessibility Standards" set forth by the Architectural and Transportation Barriers Compliance Board (also referred to as the "Access Board") in 36 CFR Part 1194. The complete text of Section 508 Standards can be accessed at http://www.access-board.gov/ or at http://www.section508.gov.

5.0 ACRONYMNS AND DEFINITIONS

ACA	After Contract Award
AIT	Advanced Imaging Technology
APSS	Accessible Property Screening System
BCP	Business Continuity Plan
BDA	Business Days After
BLS	Bottle Liquid Scanner
CFR	Code of Federal Regulations
CI	Configuration Item
CO	Contracting Officer
COR	Contracting Officers Representative
CSO	Corporate (or Cognizant) Security Officer
CTSS-2	Certification Test Support Services
DHS	Department of Homeland Security
DoD	Department of Defense
EDS	Explosive Detection System
EIT	Electronic and Information Technology
EMD	Enhanced Metal Detector
EOD	*Entry On Duty (in italics)*
ETD	Explosives Trace Detector
FAA	Federal Aviation Administration
FAR	Federal Acquisition Regulation
FOUO	For Official Use Only
FWA	Federal-Wide Assurance
GFI	Government Furnished Information
GFR	Government Furnished Resources
HME	Homemade Explosive
HSAR	Homeland Security Acquisition Regulation
ICC	Information Control Center
IED	Improvised Explosive Device
IRB	Institutional Review Board
IT	Information Technology

IT&E	Independent Test and Evaluation
LA	Laboratory Assessment
LPR	Lawful Permanent Resident
MD	Management Directive
MPR	Monthly Progress Report
NSI	National Security Information
OEM	Original Equipment Manufacturer
OHRP	Office of Human Research Protection
PII	Personally Identifiable Information
POC	Point of Contact
QLR	Quick Look Report
RCO	Regulating Compliance Office
S&T	DHS Science and Technology Directorate
SBU	Sensitive But Unclassified
SCG	Security Classification Guide
SSD	Shoe Screening Device
SSI	Sensitive Security Information
SOP	Standard Operating Procedure
SOW	Statement of Work
T&E	Test and Evaluation
TM	Technical Monitor
TRL	Technology Readiness Level
TSA	Transportation Security Administration
TSL	Transportation Security Laboratory
USG	United States Government

6.0 GOVERNMENT FURNISHED RESOURCES (GFR)

6.1 ON-SITE USE

The Government will provide most workspace, facilities, property, equipment and supplies necessary to perform the on-site portion of Contractor services required in this contract unless specifically stated otherwise in this SOW.

GFR examples include threat and simulated materials.

6.2 LIMITED USE OF GFR

The Contractor shall use Government furnished facilities, property, equipment and supplies only for the performance of work under this contract, and shall be responsible for returning all Government furnished facilities, property and equipment in good working condition subject to normal wear and tear.

6.3 GOVERNMENT FURNISHED INFORMATION (GFI)

The Government will provide all unique data and information to the Contractor for work required under this contract.

The following documents will be made available after award:

1) TSL Document Publication Templates
2) S&T Explosives Research and Development Program Security Classification Guide, DHS SCG S&T- 006.1, August 2012

6.4 LIMITED USE OF GFI

The Contractor shall use GFI and data only for the performance of work under this contract, and shall be responsible for returning all GFI and data to the Government at the end of the performance period. The Contractor shall not release GFI and data to outside parties without the prior and explicit consent of the CO.

7.0 CONTRACTOR FURNISHED RESOURCES

The Contractor shall furnish all facilities, materials, equipment and services necessary to fulfill the requirements of this contract except for the Government Furnished Resources specified in this SOW. All materials and equipment purchased by the contractor under this task order are the property of the government.

The contractor will be requested to purchase materials in support of task order requirements. The contractor shall obtain written consent from the contracting officer's representative (COR) before purchasing any individual item or combined purchase exceeding two thousand dollars ($2,000). Items purchased by the contractor using government funds shall become the property of the government. The contractor shall maintain any such items according to currently existing property accountability procedures. Any computers or data related purchases much be registered according with TSL IT requirements upon delivery and receipt.

8.0 GOVERNMENT ACCEPTANCE

8.1 APPROVAL

The government will review deliverables prior to acceptance. If the deliverable is acceptable, the contractor will be notified in writing that the deliverable has been accepted. If no written approval is provided by the COR or technical monitor, a deliverable is considered accepted and final after 60 days.

8.2 REJECTION

The government has the right to reject or require correction of any deficiencies found in the deliverables that are contrary to the information contained in the Contractor's accepted proposal. In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection. The Contractor may have an opportunity to correct the rejected deliverable and return it per delivery instructions.

8.3 REVIEW & REWORK DURATIONS

The government will have 20 business days to review deliverables and make comments. The Contractor shall have 10 business days to make corrections and re-deliver. All other review times and schedules for deliverables shall be agreed upon by the parties based on the final, approved CTSS-2 Project Plan. The Contractor shall be responsible for timely delivery to Government personnel in the agreed upon review chain, at each stage of the review. The

Contractor shall work with personnel reviewing the deliverables to assure that the established schedule is maintained.

9.0 DELIVERABLES

The Contractor shall provide all deliverables listed in Table 5 as requested and associated with SOW activities. All final deliverables must be submitted to TSLdeliverables@st.dhs.gov, TSLPublications@st.dhs.gov in addition to the distribution listed.

Item	SOW Reference	Deliverable / Event	Due by	Distribution
1	4.7	Post Award Conference	Within 14 BDA contract award	N/A
2	4.10.1	Monthly Progress Reports	10th of every month	CO; COR; TM
3	4.10.2	Contract Management Reviews	As scheduled by Technical Monitor and CTSS-2 PM	COR/TM
4	2.01 e)	Placemats	As needed or defined by the Tech. Monitor	COR/TM
5	2.1, 2.2, 2.7	Test & Evaluation Plans	As needed or defined by the Tech. Monitor	COR/TM
6	2.1, 2.2, 2.5, 2.6, 2.7	Test Reports	As needed or defined by the Tech. Monitor	COR/TM
7	2.2, 2.5, 2.6, 2.7	Data Records	As needed or defined by the Tech. Monitor	COR/TM
8	2.2	Target Databases	As needed or defined by the Tech. Monitor	COR/TM
9	2.3	IRB Records	As needed or defined by the Tech. Monitor	COR/TM
10	2.2 b.	Challenge Matrices	As needed or defined by the Tech. Monitor	COR/TM
11	2.2(g), 2.7	Inventory Records	As needed or defined by the Tech. Monitor	COR/TM
12	2.2 k.	Test Readiness Review Checklists	As needed or defined by the Tech. Monitor	COR/TM
13	2.6	Standard Operating Procedures	As needed or defined by the Tech. Monitor	COR/TM

Item	SOW Reference	Deliverable / Event	Due by	Distribution
14	2.9	CTSS-2 Project Plan	With proposal and updated within 20 BDA contract award	COR, Contracting Officer/TM
15	2.8.2	Meeting Minutes	3 BDA meeting	COR/TM
16	2.8.1	Briefing materials	As needed or defined by the Tech. Monitor	COR/TM
17	4.9.6	Quick Look Reports (QLR)	Within 5 BDA request or defined by the Tech. Monitor	COR/TM
18	4.5	Trip Reports	3 BDA return from trip	COR/TM/ include in MPR
19	4.0	OCIO/ Appendix G incident reporting	Immediately upon event occurrence	COR/TM
20	4.8.1	Business Continuity Plan	20 BDA contract award	CO/TM

10.0 Submission of Invoices

The payment address for DHS S&T payments is as follows:

U.S. DHS, ICE
Attn: S&T Invoice Burlington Finance Center
P.O. Box 1000
Williston, VT 05495-1000
InvoiceSAT.Consolidation@ice.dhs.gov

DHS S&T may change the individual designated as a POC upon notice to the Contractor of such change.

11.0 Points of Contact

11.1 Contractor Points of Contact (POC) are as follows:

11.2 DHS POCs are as follows:

DHS Contracting Officer
TBD
Office of Procurement Operations Science and Technology Directorate
245 Murray Lane Mail Stop 210
Washington, DC 20528
202-254-2274
Jessica.Wilson@hq.dhs.gov

DHS Contracting Officer's Representative
Brenda Klock
DHS/S&T Transportation Security Laboratory
William J. Hughes Technical Center
Building 315
Atlantic City, NJ 08405
Tel: 609-813-2763
Mobile: 609-576-4676
Brenda.Klock@ST.DHS.GOV

DHS Technical Monitor
TBD
DHS/S&T Transportation Security Laboratory
William J. Hughes Technical Center
Building 315
Atlantic City, NJ 08405
Tel: 609-XXX-XXXX

APPENDIX A

APPLICABLE LAWS, REGULATIONS, POLICIES, AND PUBLICATIONS

LAWS, REGULATIONS, POLICIES, AND PUBLICATIONS

All IT systems (as defined by DHS Management Directive [M.D.] 0007.1) being planned, designed, developed, and maintained for the Department of Homeland Security, Science and Technology Directorate (DHS-S&T), its customers, and/or with DHS data, shall be aligned with DHS and/or S&T Federal Enterprise Architecture. All solutions and services shall meet the following DHS Enterprise Architecture policies standards and procedures.

• In compliance with appropriate Office of Management and Budget (OMB) Circulars, including, but not limited to, OMB Circulars A-11, Preparation, submission, and Execution of the Budget, and A-130, Managing Information as a Strategic Resource, as implemented by the S&T CIO.

• In compliance with Federal Regulations including, but not limited to, the E-Government Act (including Privacy Impact Assessment), Paperwork Reduction Act, Federal Information Security Management Act (FISMA), and Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards (36 Code of Federal Regulations [CFR] 1194).

• In compliance with DHS M.D.s including 0007.1, 4010.2, 1400, 4300.1 (and 4300A), 4900, and others as appropriate.

• In compliance with other guidance and best practices related to the Secure Coding Initiative and secure coding verification.

• All versions of any source code and object code developed under this effort, along with the documentation, will be delivered to DHSS&T COR/PM as they are completed, and at other times upon request of the DHS-S&T COR/PM.

Testing standards: **https://www.unece.org/trans/danger/publi/manual/manual_e.html**

The following are laws, regulations, and policies and related publications that pertain to this work effort. The Contractor should be familiar with the guidance and requirements of each:

Public Laws and United States Code

• Public Law (P.L.) 107-347 Section III, Federal Information Security Management Act (FISMA) of 2002, 2002
• PL 107-305, Cyber Security Research and Development Act of 2002
• PL 96-456, Classified Information Procedures Act of 1980
• 5 United States Code (U.S.C.) 552, Freedom of Information Act; Public Information;

Agency Rules, Opinions, Orders, Records, and Proceedings, 1967
• 5 U.S.C. 552a, Privacy Act; Records Maintained on Individuals, 1974
• 18 U.S.C. 1029, Fraud and Related Activity in Connection with Access Devices
• 18 U.S.C. 1030, Fraud and Related Activity in Connection with Computers
• 40 U.S.C. 1401 et seq., P.L. 104-106, Clinger Cohen Act of 1996 (Information Technology and Management Reform Act of 1996)
• 44 U.S.C. 3534, Federal Agency Responsibilities
• 44 U.S.C. 3535, Annual Independent Evaluation
• 44 U.S.C. 3537, Authorization of Appropriations
• 44 U.S.C. 3541, P.L. 107-296, Federal Information Security Management Act of 2002 (FISMA)
• 44 U.S.C. 3546, Federal Information Security Incident Center
• Government Paperwork Elimination Act (GPEA) http://www.whitehouse.gov/omb/fedreg/gpea2.htm

OMB Circulars and Memoranda

• OMB Circular A-130 (http://www.whitehouse.gov/OMB/circulars/a130/a130.html)
• OMB Policy Memorandum M-07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems.
• OMB Memorandum M-07-18, Ensuring New Acquisitions Include Common Security Configurations
• OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems, 2000

Homeland Security Presidential and Management Directives

• Homeland Security Presidential Directive (HSPD)-7, Critical Infrastructure Identification, Prioritization, and Protection, 2004 HSPD-20 National Continuity Policy
• DHS M. D. 142-01, Information Collection Program (Paperwork Reduction Act 1995) 7/31/2007
• DHS MD 0007.1 Information Technology Integration and Management
• DHS MD 0475 Information Collection Program
• DHS MD 0550.1 Record Management

- DHS MD 0565 Personal Property Management Directive
- DHS MD 1120 Capitalization and Inventory of Personal Property
- DHS MD 1400 Investment Review Process
- DHS MD 3120.2 Employment of Non-Citizens
- DHS MD 4010.2 Section 508 Program Management Office & Electronic and Information
- Technology Accessibility
- DHS MD 4200.1 IT Capital Planning and Investment Control (CPIC) and Portfolio
- Management
- DHS MD 4300.1 Information Technology Systems Security
- DHS MD 4400.1 DHS Web (Internet, Intranet, and Extranet Information) and

- Information Systems
- DHS MD 4500.1 DHS E-Mail Usage
- DHS MD 4510 Domain Names
- DHS MD 4600.1 Personal Use of Government Office Equipment
- DHS MD 4800 Telecommunications Operations
  Attachment A: Frequently Asked Questions (FAQs)
  Attachment B: Nomination and Designation of Designated Agency Representative (DAR) for Telecommunications Services
  Attachment C: Designated Agency Representative (DAR) for Telecommunications Services Function Requirements
- DHS MD 4900 Individual Use and Operation of DHS Information Systems/ Computers
- DHS MD 8200.1 Information Quality
- DHS MD 11005 Suspending Access to DHS Facilities, Sensitive Information, and IT Systems
- DHS MD 11042.1 Safeguarding Sensitive But Unclassified (For Official Use Only) Information
- DHS MD 11056.1 Sensitive Security Information (SSI)
- DHS MD 11060.1 Operations Security Program
- DHS MD Safety and Health Programs
- DHS Instruction 121-01-011 – The Department of Homeland Security Administrative Security Program
- DHS Instruction 121-01-011-01 – Visitor Management for DHS Headquarters and DHS Component Headquarters Facilities
- HSAR Class Deviation 15-01 Safeguarding of Sensitive Information
- National Industrial Security Procedures Operations Manual (NISPOM) https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodm/522022m.pdf
- 49 CFR 1520 Protection of Sensitive Security Information
- DHS S&T Explosives Research and Development Program Security Classification Guide, DHS SCG S&T-006, (current version)
- DHS IT Security Program Publication DHS MD 4300.1
- S&T's Environmental Policy Statement,
- Occupational Safety and Health Policy Statement
- National Environmental Policy Act of 1969
- Executive Order 13693, Planning for Federal Sustainability
- The Energy Policy Act of 2005
- Energy Independence and Security Act of 2007

APPENDIX B

This section lists additional clauses that are applicable to the contract.

1. FAR Clause 52.251-1 "Government Supply Sources"
2. FAR Clause 52.245-1 "Government Property"
3. Supplemental Language to FAR 52.245-1 "Government Property" as stated below:

1. **PERSONAL PROPERTY**
    a. **PROPERTY DEFINITIONS**
        i. Accountable Personal Property:
            1. An asset that meets one or more of the following criteria:
                a. Has an expected useful life is two years or longer and an asset value of $5,000 or more;
                b. Classified as sensitive;
                c. Property for which accountability or property control records are maintained; or
                d. Otherwise warrants tracking in the property system of record.
            2. Current accountable personal property thresholds may be obtained through the ***Property Management Program Office*** at ***ST_Personal_Property@hq.dhs.gov***.
        ii. Capitalized Personal Property:
            1. Non-expendable personal property with an acquisition cost over an established threshold and a normal life expectancy of two years or more.
            2. Current Capitalization Threshold information may be obtained through the ***Property Management Program Office*** at ***ST_Personal_Property@hq.dhs.gov***.
        iii. Consumable Assets:
            1. An item of supply which is consumed in use (e.g., paint, rations, water, office supplies, cleaning and preserving materials, and fuel) or which loses its separate identity when merged into another entity (e.g., nuts and bolts, repair parts, spares, construction materials, components and assemblies, etc.). Consumables are considered to be expendable when issued and do not require formal accountability after they have been issued.
        iv. Contract Property:
            1. All property, both real and personal, that is used in the performance of a contract and includes facilities, material, special tooling, special test equipment, and agency-peculiar property. Contract property refers to both Contractor-Acquired Property (CAP) and Government Furnished Property (GFP), in the possession of contractors.

a. CAP: Property acquired, fabricated, or otherwise provided by the contractor for performing a contract and to which the Government has title.
b. GFP: Property in the possession of, or directly acquired by, the Government and subsequently furnished to the contractor for performance of a contract. Government-furnished property includes, but is not limited to, spares and property furnished for repair, maintenance, overhaul, or modification. Government-furnished property also includes contractor-acquired property if the contractor-acquired property is a deliverable under a cost contract when accepted by the Government for continued use under the contract. NOTE: GFP may also be referred to as GFE, the two terms are interchangeable.

v. Leased Property:
1. Property that is not owned by DHS, but that is leased by the Government under terms as stipulated in the lease agreement (this excludes the leasing of property by contractors in the performance of a contract).

vi. Sensitive Asset:
1. All items, regardless of value, that require special control and accountability due to unusual rates of loss, theft, or misuse; national security or export control considerations.
2. Sensitive assets must be formally accounted for in an accountable system of record, and include, but are not limited to, asset categories such as:
a. Dangerous and hazardous assets including weapons, ammunition, and explosives;
b. Law enforcement equipment including credentials, body armor, detection equipment;
c. Assets authorized for storing and/or processing classified information;
d. Assets with retainable memory including digital cameras, communications equipment, it equipment; and
e. Inherently portable assets, and assets that can easily be converted to private use or that have a high potential for theft as determined by the Group APO, Program Manager (PM), or Contracting Officer (CO).

b. **PROPERTY ACCOUNTABILITY**

i. When contractors are furnished with GFP, DHS barcodes will not be removed. In all GFP cases, the Government retains title to the property.
ii. It is the contractor's responsibility to use contract property as it was authorized and for the purpose intended. In the event the contractor uses

contract property for other purposes without written authorization from the CO, the contractor may be liable for rental, without credit, of such items for each month or part of a month in which such unauthorized use occurs.

iii. The Contractor is directly responsible and accountable for all contract property in its possession in accordance with the requirements of the particular contract; this also includes any contract property in the possession or control of a subcontractor.

c. PHYSICAL INVENTORY

i. In addition to requirements provided under FAR § 52.245-1:

1. The Contractor, jointly with the Property Management Program Office on a quarterly basis, shall perform, record, and disclose physical inventory results of CAP, GFE, and GFP.
2. The Contractor shall, on an annual basis, perform, record, and disclose physical inventory results of CAP and GFP that meets the threshold of accountable personal property to the ***Property Management Program Office*** at ***ST_Personal_Property@hq.dhs.gov*** and COR. The inventory results will include a verification for accountable property to include a photo of each asset which depicts both the serial number and the date (can be written on a piece of paper next to asset). If there is a large number of assets, a scanner (for DHS barcodes – provided by the PPMO to the COR and so to the vendor) will be provided by the PPMO for assignment/and/or use during inventory. Training will be provided as needed.
3. As requested, inventory results will be completed, certified, and submitted in the timeframe defined at the time of the request, to the ***Property Management Program Office*** at ***ST_Personal_Property@hq.dhs.gov*** and COR using the provided Sunflower Assets Management System Template to enter data for all accountable assets. This includes original assets purchased as part of the original contract award (within SOW) and additional assets purchased throughout the life of the contract. Vendors will provide template information to the COR not less than once per month.

d. PROPERTY DISPOSAL

i. All documentation and goods are the property of the United States Government and, if applicable, the contractor shall return or destroy appropriately upon request. The contractor shall comply with applicable government rules and regulations for disposal of government property. Further, the contractor shall provide necessary information to the COR and the ***Property Management Program Office*** at ***ST_Personal_Property@hq.dhs.gov*** for all excess property prior to taking any action.

ii. The Contractor shall use Government-furnished information, data, and documents only for the performance of work under this contract, and shall be responsible for returning all Government furnished information, data, and documents to the Government at the end of the performance period. The Contractor shall not release Government-furnished information, data and documents to outside parties without the prior and explicit consent of the Contracting Officer.

e. LOST, STOLEN, DAMAGED OR DESTROYED (LDD) PROPERTY

i. Unless otherwise provided in the contract, the contractor is liable for LDD of contract property, except for reasonable wear and tear.

ii. Any occurrence of LDD must be investigated and fully documented by the COR, who will promptly notify the CO. The contractor will submit a report of any incident of LDD contract property to the COR in accordance with FAR §45.504, "Contractor's Liability," and as detailed below, as soon as it becomes known.

iii. When GFP or CAP property is LDD, the Contractor must report within 24 hours of discovery of the event to the COR who will initiate a Report of Survey. This document will be obtained from the ***Property Management Program Office*** at ***ST_Personal_Property@hq.dhs.gov***.

iv. A Report of Survey will be prepared, regardless of whether or not preliminary research of an LDD event indicates positive evidence of negligence, misconduct, or unauthorized use and the responsible individual refuses to admit pecuniary liability.

v. The Contractor must forward this document with all supporting documentation to the COR within 5 business days of the LDD event for review.

vi. The COR must submit the completed package to the ***Property Management Program Office*** at ***ST_Personal_Property@hq.dhs.gov*** within 5 business days of receipt from the Contractor.

vii. The Contractor and COR must supply all requested information and any subsequent requests for information.