## J.1. STATEMENT OF WORK

# UNITED STATES DEPARTMENT OF HOMELAND SECURITY
# SCIENCE AND TECHNOLOGY DIRECTORATE
# OFFICE OF ENTERPRISE SERVICES
# CONTRACT ACQUISTION PROGRAM SUPPORT
# STATEMENT OF WORK FOR
# MULTI-SPECTRUM LASER DETECTION SYSTEM

## 1.0 GENERAL

## 1.1 BACKGROUND

The United States Department of Homeland Security (DHS) is committed to using cutting-edge technologies and scientific talent in its quest to make America safer. The DHS Science and Technology Directorate (S&T) is tasked with researching and organizing the scientific, engineering, and technological resources of the United States and leveraging these existing resources into technological tools to help protect the homeland.

First responders, particularly law enforcement officers responding to civil unrest situations, need a multi- spectrum laser detection capability. Currently, there is no viable solution that allows officers to detect the presence or engagement of lasers that can be initiated from multiple light spectrums including red, blue, green, and infrared. Further, all officers do not have access to laser protection equipment or may require multiple pieces of equipment for varying laser types. This places officers in the position of being under attack from lasers while they are unaware and unprotected. There have been instances of permanent eye injury to officers from laser attacks.

With the proliferation of low-cost, high-power lasers in the consumer market, first responders, primarily law enforcement officers are likely to face more frequent laser attacks. These attacks, from lasers of different wavelengths within visible and infrared (IR) spectral bands, pose great threats to their eye safety. A passive one-for-all eye protection device is not feasible without either severely impairing responders' view and/or interfering with their normal operation. A more practical approach is to detect threat wavelength and selectively blocks the narrow spectral band(s) where the threat is detected. Diode pumped solid state (DPSS) lasers (typically visible < 600 nm wavelength) and diode lasers (typically red to infrared > 600 nm wavelength) are the most common types. The choice of color (wavelengths) has dramatically expanded to purple, blue, green, orange, red and infrared, spanning the entire visible and near-IR regions. Several hundred milliwatts of laser power is easily accessible, enough to dazzle and/or damage human eyes. Many of these products are in class 3B or class 4 category and control measures are required for safe operation, per the ANSI Z136.1 American National Standard for safe use of lasers. At visible wavelengths (400 to 700 nm) human eye is protected by the aversion response (blinking), which limits effective exposure time. This only works for Class 3R lasers (power levels < 5 mW). Near infrared lasers are even more dangerous as while they can focus power on the retina, they do not trigger blinking response. The total exposure time also depends on the pointing jitter and the spot size of the beam. While an accurate power measurement from non-cooperative laser user in the field is not practical, a qualitative

assessment can be made at the threat warning receiver to whether the detected laser is dangerous and whether it warrants a follow up or prosecution of the offending individual.

Current products cannot adequately address the emerging threat the first responders are facing. For example, current FLIR LTWS is only able to issue threat warnings at 1.06 μm wavelength, which is insufficient for targeted eye protection against consumer grade lasers. Furthermore, military systems that provide spectral and angle of arrival information are often too bulky/ and/or expensive for personal use. The wavelength resolution, device aperture, angle of arrival (AOA) detection mechanism, as well as the threat categorization are tailored towards military laser threats, whose spectrum, power level, beam size, temporal characteristics, and threat distance are different from those available in the civilian cases.

## 1.2 OBJECTIVE

In support of the DHS S&T Office of Enterprise Services (OES) through the Contract Acquisition Program Support (CAPS) division, this requirement, entitled "Multi-Spectrum Laser Detection System," the objective of this work is to address this critical gap. The contractor ~~proposes to~~ shall develop the Advanced Laser Threat Assessment Receiver (ALTAR) under this Statement of Work (SOW). The ALTAR is a compact, versatile, wearable receiver. The receive unit is a multi-spectral imager capable of measuring laser wavelengths, directions of arrival and power strength, and performs assessment of the threat.

ALTAR also captures the scene with a co-packaged high-resolution context camera and fuses laser locations with the scene image. It provides wired or wireless connections to alert units, such as radios or mobile devices, to generate sound, vibration, and visual warnings, and to eye protection devices with sensing and transmission capabilities for relaying threat details, which is needed for taking proper protection action. A smart phone app with intuitive graphic user interface (GUI) will be developed, which would give the user detailed information of the threat and the fused images in real time.

## 1.3 SCOPE

The contractor shall develop a multi-spectrum laser detection system that can be deployed quickly, operate hands-free and continuously, detect and alert the LE officer wearing the detector of detected laser threats. The system will be designed to be mounted on the LE user, possibly on the helmet or hung on other personal protective equipment and/or garment. The LE officer will receive threat notifications via a mobile application GUI with haptic feedback and/or audio alert. The solution shall also provide an affordable insertion path to the first responder community.

The Government has elected to include the Custom Filter and Night Vision options into this effort. Table 1 outlines the notional baseline performance specifications and shall be updated during the requirements definition phase of the project.

### 1.3.1 Specific Requirements

- Ability to detect and locate threatening multi-spectrum lasers >400mn.

- Identify the strength and type of threat in accordance with the acceptable threshold in ANSI Z136.1
- Detect laser threats from at least 200 yards
- Identify multiple laser threats and/or perpetrators
- Ability to detect at day and night
- Ability to detect in all types of weather (e.g., hot, cold, wet, dry)
- Develop application for use with smart phones and other devices that displays detected laser threats in real time and overlaid on high resolution scene video/image
- Alert officer wearing the detector of laser detections
- Alert scene/event commander of laser detections via graphic user interface application
- Wireless connect with other devices, including agile smart devices for eye protection
- Operable by a single person
- Operate in continuously or triggered mode
- Must be durable, reusable, and scratch-resistant
- Must be able to be cleaned

### 1.3.2 Options

- **Option I: Custom Filter Option**: The specifications of the COTS multi-spectral camera will be replaced with custom filters and board level monochrome silicon cameras, plus the alignment and lamination of the custom micro-patterned multispectral filters to the monochrome silicon cameras. The customized multi-spectral filter (See Table 1, Column 2) is the final low SWaP-C field deployable solution if this option is exercised.
- **Option II: Night Vision Option**: A thermal night vision option will be realized with the addition of contractor's Long Wave Infrared (LWIR) micro-bolometer-based camera to the head mounted units and be able to acquire thermal imagery co-aligned and co-calibrated with the threat warning receiver and context camera to aid night-time operation. The micro-bolometer and/or eye safe NIR illuminator can also be added to ALTAR to enhance night vision for improved scene resolution and target discrimination.
- **Option III: Range Extension Option**: To develop and demonstrate 400-1600 nm coverage instead of 400- 1100 nm with the proposed project, Indium Gallium Arsenide (InGaAs) focal planes will be needed instead of silicon in addition to the custom Vis-SWIR specific micro- patterned multi-spectral filters, and labor to laminate custom filters InGaAs focal planes. Contractor has verified that customization of micropatterned multi- spectral filter that covers 400-1600 nm is possible.

### 1.3.3 Desirable Capabilities or Characteristics

In addition to the specific requirements listed above, the following attributes exceed the proposed solution requirement and may be integrated into the final solution if it can be developed within schedule and budget:

- Easy to carry/access

- Easy to read and interpret in loud, distracting environment

## 1.4 APPLICABLE DOCUMENTS

The following documents are applicable to this contract and shall be provided to the contractor during the kick-off meeting if necessary.

### 1.4.1 Compliance Documents

The following documents provide specifications, standards, or guidelines that must be complied with to meet the requirements of this contract:

#### 1.4.1.1 Privacy Documents

- Safeguarding of Sensitive Information (MAR 2015)
- Information Technology Security and Privacy Training (MAR 2015)
- HSAR clause 3052.204-71 Contractor Employee Access
- HSAR 3052.204-70, Security Requirements for Unclassified Information Technology Resources (JUN 2006)

#### 1.4.1.2 Standards

The following is a list of standards that applies to the work described in this document (See tables 1 and 2 for the application of standards):

- MIL-STD-810 H (Environmental)
- UL 60950, Safety for Information Technology Equipment (Electrical)
- IEC 60529 classification IP54 (Water Intrusion)
- IEC 68–2–27 1987 (Shock & Bump)
- IEC 68–2–32 Procedure 1, 1975 (Free Fall)
- ISO 9001:2000 (Quality Control)
- MIL-STD-1472H, DOD Design Criteria Standard: Human Engineering
- ANSI z136.1 For Ocular Exposure Section 8.2 Table 5a and 5b

### 1.4.2 Reference Documents

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

- First Responder Group Broad Agency Announcement (BAA), 18-02, Call 0003
- Multi-Spectrum Laser Detection Statement of Objectives
- Teledyne Scientific Company, Advanced Laser Threat Detection Technical Proposal

### 1.4.3 Federal Acquisition Regulation (FAR)

The following FAR clauses are applicable to this contract:

- 52.227-11 Patent Rights-Ownership by the Contractor
- 52.227-14 Rights in Data-General
- 52.227-16 Additional Data Requirements

## 2.0 SPECIFIC REQUIREMENTS & TASKS

## 2.1 SPECIFICATIONS

Specifications for the Laser Detection System prototype apply to this contract.

**Multi-Spectrum Laser Detection Specifications**

| Specification | Customized Micro-Patterned Multi-Spectral Filters Option | |
|---|---|---|
| | Threshold | Objective |
| Spectral coverage | 400 –1100 nm (NIR enhanced silicon sensors) | |
| FOV | 120°H ×60°V (extendable to 360°H with multiple receivers) | |
| Threat wavelength resolution | <50 nm (sufficient to deploy narrow band eye protection with minimal loss of visual acuity) | |
| Camera Image range (Can resolve human) | 200 m | 300 m |
| Location accuracy | Effective 0.3°(can locate the perpetrator at 200 m) | |
| Speed (reaction time) | >25 milliseconds | Sufficient time for FPA to recognize and internally react to a threat |
| Laser Damage Threshold | Trigger alert whenever the power density it measures reaches the MPE as defined in the ANSI z136.1 | |
| Dimensions (size, excluding battery pack) | 2.5”W x 1.25”H x 1.5” D | 2.3”W ×1.1”H ×1.3” D |
| Weight (Excluding battery pack) | <110 g | < 100 g |
| Battery life | > 4 hours (CW mode), >8 hours (trigger mode) | |

**Electronics Standards**

| Standard Type | Electronics Standards | |
|---|---|---|
| | **Threshold** | **Objective** |
| Safety | Electrical: Equipment shall comply with UL 60950, Safety for Information Technology Equipment, if the potential difference between any two points within the equipment is greater than 30 V rms (42.4 V peak-to-peak) for alternating currents (ac) or greater than 60 V referenced to ground for direct currents (dc). | |
| | Mechanical: The equipment shall not expose<br>(1) any sharp corners or edges that can puncture, cut, or tear the skin or clothing or injure persons coming in contact with the equipment; (2) external wires and cables; or<br>(3) loose covers and cowlings. The minimum exposed radius of curvature for corners and edges shall be 1 mm (0.04 in). | |
| Environmental | Temperature: The equipment shall operate over the ambient temperature range of at least ***-20°C to 49°C (-4°F to 120°F)***. The detector shall be tested in accordance with MIL–STD–810H Method 501, Procedure II, at<br>49°C ± 3°C after being exposed to that temperature continuously for 24 h ± 1 h. | Temperature: The equipment shall operate over the ambient temperature range of at least ***-32°C to 60°C (-25°F to 140°F).*** The detector shall be tested in accordance with MIL–STD–810H Method 501, Procedure II, at 60°C ± 3°C after<br>being exposed to that temperature continuously for 24 h ± 1 h. |
| | Relative Humidity Stability and Range: The equipment shall be tested in accordance with the requirements of MIL–STD–810H Method 507.6, as amended. | |
| | Salt Fog: The equipment shall be tested in accordance with the requirements of MIL– STD–810H Method 509.7, as amended. | |

| Standard Type | Electronics Standards | |
|---|---|---|
| | **Threshold** | **Objective** |
| | Water Intrusion: The equipment shall meet or exceed the requirements for compliance with IEC 60529 classification IP56. | Water Intrusion: The equipment shall meet or exceed the requirements for compliance with IEC 60529 classification IP57. |
| Durability and Ruggedness | Shock: The equipment shall be tested in accordance with the requirements of IEC 68– 2–27 1987, as amended, using the half-sine pulse shape with a nominal peak acceleration of 30 g (300 m/s2 ) and a nominal pulse duration of 6 ms. | |
| | Bump: The equipment shall be tested in accordance with the requirements of IEC 68– 2–29 1987, as amended, using 100 bumps each with a nominal peak acceleration of 40 g (400 m/s2 ) and a nominal pulse duration of 6ms. | |
| | Free Fall: The equipment shall be tested in accordance with the requirements of IEC 68– 2–32 Procedure 1, 1975, as amended, for each direction of the equipment axes and a fall height of 1 m. | |
| | Pressure Resistance: The equipment shall be capable of withstanding the force of 600 N (135 lb) over any 1 cm x 1 cm (0.4 in x 0.4 in) area on the equipment for a sustained period of 1 min. | |
| Quality Control and Assurance | Quality Systems: The manufacturer shall meet the requirements of ISO 9001:2000, as amended. | |

## 2.2 TASKS - WEARABLE DETECTORS

| Task 1 | PROJECT MANAGEMENT | **Duration:** 15 Months |
|---|---|---|
| | **Main Deliverables:** Monthly Progress & Status Report and Briefing | |
| | Contractor shall provide a monthly progress & status update to the PM and COR. Format and delivery means will be determined at the Kick-Off Meeting Contractor shall provide documentation or demonstrations sufficient for the PM and COR to evaluate the system elements of the Contractor's solution. Documents or demonstrations may include test results, design documentation, and systems analysis. | |

| Task 2 | KICK-OFF MEETING | Duration: 1 month |
|---|---|---|

The contractor shall facilitate the kick-off meeting. The kick-off meeting will take place either at the contractor's facility, DHS S&T headquarters or via teleconference. The kick-off meeting will be comprehensive in nature and the following information shall be discussed by the contractor:

- Introduction of the Project Team
- Project technical Goals and Mission Scenarios or Concept of operation
- Demonstration of Existing Technology - SAM, Edge Device
- Potential technical risks and mitigation strategies
- Performance metrics/testing events that will be used to measure progress against completed Phases and Project milestones
- Overview of Commercialization Objectives and Plan
- Project Plan

Contractor shall allot time for the DHS S&T Project Manager to facilitate the following discussion points regarding contractor's required contributions to DHS S&T program management operations:

- Program Document requirements:
  - Project Charter
  - Project Management Plan (PMP)
  - Quad Chart
  - One Page Project Summary/Information Sheet
  - Monthly Status Reports
  - Risk Register
  - Commercialization & Transition
  - Privacy Threshold Assessment (PTA)
    (Contractor may need to provide information on how the images captured through the night vision camera are processed, stored, disseminated and how external disclosures of PII are tracked I order to complete the PTA.)

- Overview of DHS Program Management Operations
  - Monthly Teleconferences

- Objectives and Technical Approach for Design Reviews and Operational Field Assessments
  - Preliminary Design Review (PDR)
  - Critical Design Review (CDR)
  - Operational Field Assessment (OFA)

| Task 3 | REQUIREMENT DEFINITION AND APPLICATION TRADES | Duration: 1 month |
|---|---|---|

**Exit criteria:** System requirements and specifications finalized and flowed down to sub-systems and components.
**Objective:** Develop system requirements and specifications, and flow down to components.
**Approach:** Perform survey of lasers that are potential threats to the first responders, including laser types, spectrum, strength, and hazard level. Develop system requirements with feedback from Government. Explore design trade space and select the optimal design set through analysis and high-level modeling. Develop product requirement document that finalize system specifications and objectives linked to design components.

| Task 4 | PRELIMINARY DESIGN REVIEW | Duration: 1 month |
|---|---|---|

The contractor shall participate in the Preliminary Design Review (PDR) to discuss the work that was conducted to this point and to receive feedback from stakeholders, to include but not limited to program manager, First Responder Resource Group (FRRG) technical expertise and project advisors. The main purpose of this review is to assess the initial design and address any unmitigated risks associated with this effort. The PDR will assist in ensuring that the functional requirements have been allocated to the various elements of the system and that the application and associated hardware can proceed with development, demonstration, testing and will likely meet stated performance requirements.

The contractor shall provide the following information at the PDR meeting.

- Technical documentation showing the preliminary system architecture diagrams, preliminary external and internal interfaces
- System requirements, functional requirements, preliminary interface requirements (external and internal), and requirements verification methodology
- System design constraints and their incorporation into requirements.
- A preliminary list of configuration items (CI)
- Risk assessment matrix showing all identified risks, their severity, likelihood, impact, and associated mitigation plans
- Updated cost estimation for the project
- User interface requirements including system functions:
    - Roles of human operators and automation in each function
    - Operator tasks and task sequences
    - Performance requirements associated with tasks
    - Operational environmental impacts on task performance
    - Requirements for operator interaction with automated processes
    - Preliminary design requirements for user interfaces
    - Methods and metrics to be employed in operator performance and user interface evaluation.
- Contractor shall provide PDR presentation three workdays prior to PDR.

| Task 5 | DESIGN | |
|---|---|---|
| 5.1 | **Optical Design** | **Duration:** 2 months |
| | **Main Deliverables:** Critical Design Review (CDR) material | |
| | **Objective:** Critical design of threat detection system optics.<br>**Approach:** Select off-the-shelf camera, filter, and lenses based on system requirements and optical models. Perform bench top tests with surrogate component hardware. Develop power calibration procedures and methods for dynamic range enhancement with multiple exposure.<br>**Exit criteria:** Completion of optical design meeting system requirements. | |
| 5.2 | **Electrical Design** | **Duration:** 2 months |
| | **Main Deliverables:** Critical Design Review (CDR) materials/documentation | |
| | **Objective:** Critical design of electronics, including control electronics, embedded processing, and power supply/distribution.<br>**Approach:** Develop electronics and embedded processing architecture supporting image capture, laser categorization, and alarm actuation. Specify system components and electrical interfaces. Identify low power processor boards. Develop flow charts and/or prototyping codes for laser threat categorization. Algorithms flow down to firmware development. Identify battery requirement by analyzing component power consumption and power-on time requirements. Design power supply circuitry to meet component voltage and current need.<br>**Exit criteria:** Completion of electrical design meeting system requirements. | |
| 5.3 | Mechanical Design | **Duration:** 2 months |
| | **Main Deliverables:** Critical Design Review (CDR) material<br>**Objective:** Opto-mechanical design of detection system, alignment and calibration procedures, and design for ruggedized packaging.<br>**Approach:** Develop 3D model of the detection system. Develop mounting mechanism for the system that satisfies the optical function and tolerance. The design will meet system requirements including compliance to MIL-STD-810 and waterproof to an IP67 level. Develop battery package based on Teledyne FLIR Helmet Mounted Battery Box (HMBB). Generate all drawings for fabrication.<br>**Exit criteria:** Completion of mechanical design meeting system requirements**.** | |
| 5.4 | Software Design | **Duration: 2 Months** |
| | **Main Deliverable:** Critical Design Review (CDR) material<br>**Objective:** Design smart phone app with GUI (Graphic User Interface)<br>**Approach:** Identify function blocks and interfaces for smart phone app. Design use case model and GUI layout and functions. Establish communication protocols between smartphone and laser threat detection system.<br>**Exit criteria:** Software design documented and ready for implementation. | |

| Task 6 | CRICTICAL DESIGN REVIEW | Duration: 1 month |
|---|---|---|
| | The contractor shall participate in a CDR to discuss the work that was conducted to this point and to receive feedback from stakeholders, to include but not limited to program manager, First Responder technical expertise and project advisors. The main purpose of this review is to evaluate the final design and ensure it meets the performance specifications and requirements of the contract, and address any unmitigated risks associated with this effort. The CDR will ensure that the requirements contained in the ~~Statement of Work~~ SOW are adequately addressed and likely satisfied and that the application and associated hardware can proceed into final development, demonstration, testing phases and meets the stated performance specifications and requirements.<br><br>The contractor shall provide the following information at the CDR meeting.<br><br>• Technical documentation showing detailed hardware and software design including final system architecture diagrams, final external and internal interfaces diagrams, and requirements<br>• Updated system design constraints and their incorporation into requirements.<br>• Final CI list<br>• Updated risk assessment matrix showing all identified risks, their severity, likelihood, impact, and associated mitigation plans<br>• Updated cost estimation for the project<br>• User interface Documentation: drawings or pictures, functional description of controls and displays, operator task sequences for selected scenarios, testing and evaluation requirements for operator performance and user interface useability assessment. Results of any prior end-user and user interface testing.<br>• Contractor shall provide CDR presentation three workdays prior to CDR. | |

| Task 7 | FABRICATION AND TESTING | |
|---|---|---|
| 7.1 | Optics | **Duration:** 3 months |
| | **Main Deliverables:** Reports of technical progress | |
| | **Objective:** Fabricate core optical system for laser detection at various wavelengths.<br>**Approach:** Procure off-the-shelf camera and filters, and build system based on optical and opto-mechanical design, and meeting precision alignment requirements. Test and characterize system. Perform laser power measurement calibration and generate calibration table for system.<br>**Exit criteria:** Completion of the optical system hardware. | |
| 7.2 | Electrical Hardware | **Duration:** 2 months |
| | **Main Deliverables:** Reports of technical progress | |

| Task 7 | FABRICATION AND TESTING | |
|---|---|---|
| | **Objective:** Critical design of electronics, including control electronics, embedded processing, and power supply/distribution.<br>**Approach:** Develop electronics and embedded processing architecture supporting image capture, laser categorization, and alarm actuation. Specify system components and electrical interfaces. Identify low power processor boards. Develop flow charts and/or prototyping codes for laser threat categorization. Algorithms flow down to firmware development. Identify battery requirement by analyzing component power consumption and power-on time requirements. Design power supply circuitry to meet component voltage and current need.<br>**Exit criteria:** Completion of electrical design meeting system requirements. | |
| 7.3 | Mechanical Parts | **Duration:** 6 months |
| | **Main Deliverables:** Reports of technical progress | |
| | **Objective:** Fabricate mechanical components and ruggedized system packaging.<br>**Approach:** Fabricate, inspect, and test components. Validate against design and tolerance requirements.<br>**Exit criteria:** Completion of mechanical system hardware. | |

| Task 8 | FIRMWARE AND SOFTWARE DEVELOPMENT | |
|---|---|---|
| 8.1 | Optics | **Duration:** 5 months |
| | **Main Deliverables:** Reports of technical progress | |
| | **Objective:** Develop processor firmware<br>**Approach:** Using processor specific development tools, implement system control logics, image fusion and laser threat categorization algorithms. Test firmware function with peripherals and/or surrogate external components incorporating cyber security best practices.<br>**Exit criteria:** Completion of firmware development and pass test | |
| 8.2 | Software Development | **Duration:** 5 months |
| | **Main Deliverables:** Reports of technical progress | |
| | **Objective:** Develop smart phone software<br>**Approach:** Procure smart phones and implement software based on the design. Test software function with prototype or surrogate hardware incorporating cyber security best practices.<br>**Exit criteria:** Completion of software development and pass test. | |

| Task 9 | SYSTEM INTEGRATION AND TESTING | |
|---|---|---|
| 9.1 | System Hardware Integration and Functional Test | **Duration:** 3 months |
| | **Main Deliverables:** Reports of technical progress | |

| Task 9 | SYSTEM INTEGRATION AND TESTING | |
|---|---|---|
| | **Objective:** System integration and functional test<br>**Approach:** Integrate systems. Calibrate each camera system for image registration and fusion. Perform functional test including image capture, laser power measurements, laser threat categorization, alarm actuation, and smart phone app alert.<br>**Exit criteria:** At least five systems integrated and pass functional test | |
| 9.2 | System Field Test | **Duration:** 2 months |
| | **Main Deliverables:** Reports of technical progress | |
| | **Objective:** Test system performance in simulated field scenarios.<br>**Approach:** Implement field test scenarios and execute test plan, with feedback from FRG. Record test results. Make necessary refinements and improve system field performance. Document test procedure and results.<br>**Exit criteria:** System performance successfully demonstrated through field test. | |

| Task 10 | Prototypes Delivered | |
|---|---|---|
| | Prototype Delivery | **Duration:** 1 months |
| | **Main Deliverables:** 5 prototypes and operation manual | |
| | **Objective:** Deliver test units to PM and/or COR as instructed.<br>**Approach:** Produce user operation manual. Deliver five sets of complete systems to FRG.<br>**Exit criteria:** Five sets of system and user manual delivered to FRG | |

| Task 11 | OPERATIONAL FIELD ASSESSMENT |
|---|---|
| 11.1 | The performer shall participate in a one-day Operational Field Assessment (OFA) conducted by the National Urban Security Technology Laboratory (NUSTL) approximately 1-2 months before the end of the period of performance (POP). At the OFA, up to nine first responders will evaluate the prototype product by using it under simulated operational conditions to verify that project requirements were met and that the product is usable and compatible with operations. The performer shall provide at least **two functional wearable prototypes** for the OFA. The OFA for the wearable prototype will be conducted in conjunction with the Option III Area Detector prototypes. At the end of the OFA the prototypes shall be returned to the performer, except where S&T specifies otherwise.<br><br>**OFA Planning**<br>At least three (3) months in advance of the OFA, the performer shall provide to S&T a thorough written description of the prototype to be tested, including, but not limited to: hardware and software components, installation, functions and capabilities, methods of operation, connections between device components and connections to the user, optional settings, power requirements, material, dimensions and weight or available size options, additional hardware or software needed for operation, and any safety or privacy considerations associated with its construction or usage. If the device includes software, the performer shall also provide a description of any user accounts, terms of service, use of external data streams, and internet or Bluetooth connectivity involved in its usage. The performer shall provide a physical sample or images of the prototype along with the description and shall identify any proprietary information included in the text or the |

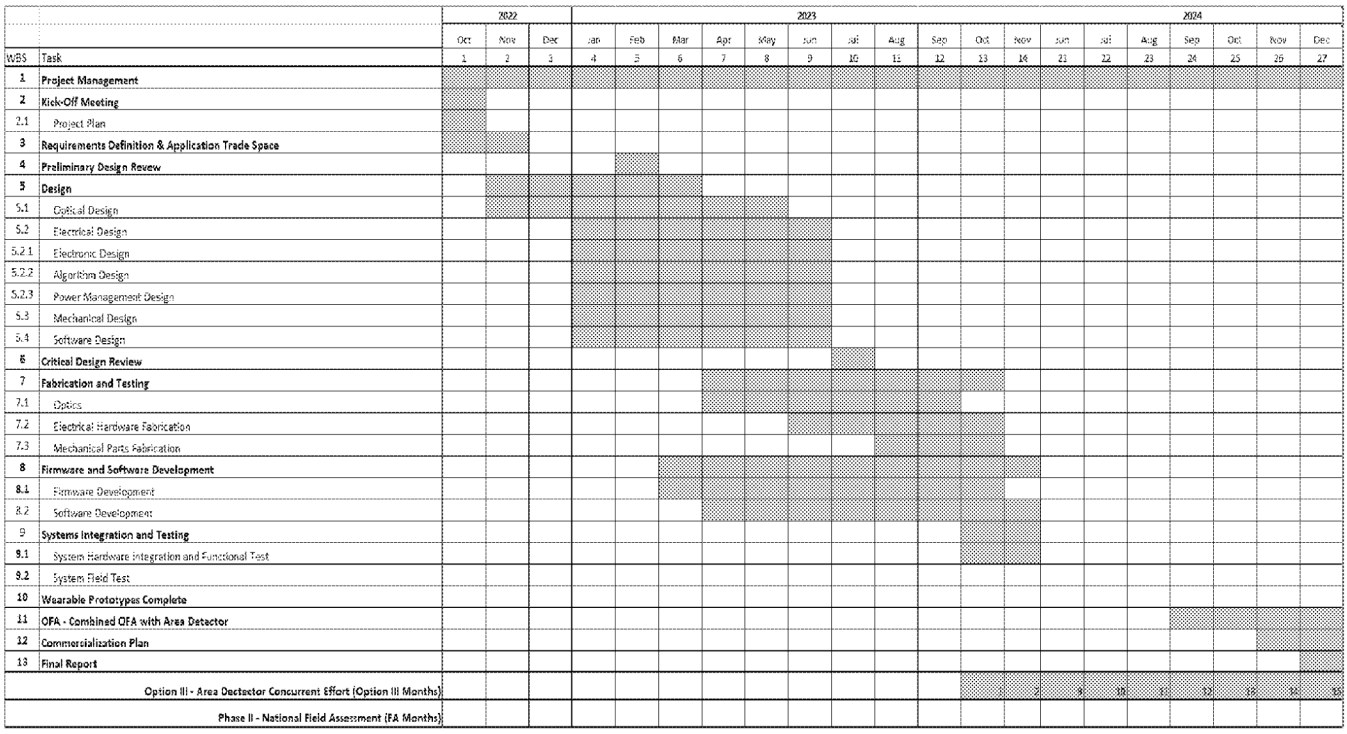
| Task 11 | OPERATIONAL FIELD ASSESSMENT |
|---|---|
| | images.<br><br>**OFA Venue and Event**<br>The OFA will be conducted at a suitable venue to be selected by S&T. The performer shall travel to the venue and be available the day before the OFA to participate in setting up and going through a dry run of the OFA activities. On the day of the OFA, the performer shall provide a brief presentation (about 10 – 20 minutes duration) describing the device development and a summary of the results of any relevant laboratory and pilot testing conducted. Additionally, the performer shall provide training on the use of the device to the evaluators and assist them with proper fitting and set-up as appropriate. The performer's proposed overview and training presentations shall be provided to S&T not later than one week before the OFA for review and concurrence.<br><br>**Option to Extend Period of Performance to conduct OFA**<br>If it is not feasible to conduct the OFA prior to the end of the POP due to insufficient technology readiness, extreme weather conditions, lack of evaluators, limited venue availability, or other unforeseen circumstances, S&T retains the option to extend the POP at no additional cost to the Government, excluding performer travel and shipment of prototypes.<br><br>**Option to forgo OFA**<br>If it is determined that an OFA is not of benefit to the government S&T retains the option to forgo the OFA. |
| 11.2 | **OFA Support**<br>Contractor shall collect OFA user feedback that is separate from NUSTL's data collection efforts to help refine and improve the detector and commercialization plan. |

| Task 12 | Commercialization |
|---|---|
| 12 | **Commercialization Plan**<br>The contractor shall complete a Commercialization Plan for the full system. In the Commercialization Plan, the contractor shall consider state, local, and federal government, and private-sector purchase and employment of their system. The plan shall also provide analysis of purchase, operations, and maintenance (O&M), and disposal of individual components and the system.<br><br>Should the government choose to proceed with the commercialization plan, the government will evaluate the proposed costs for reasonableness. If the government elects to proceed with the plan, a change order, or Request for Equitable Adjustment (REA) will be conducted. |

| Task 13 | Final Report |
|---|---|
| 13 | The Contractor shall provide a final report, including test data, at the conclusion of the effort. The report shall include the feasibility of exercising the Range Extension option. |

### 2.2.1 Wearable Schedule

Figure 1, Overview of Tasks Schedule, shows an overview of the scheduled tasks. Throughout the execution of this contract, the Contractor's Principal Investigator/Program Manager shall work with the S&T Program Manager and Contracting Officer Representative to arrange suitable times for the Preliminary Design Review, Critical Design Review, and the Operational Field Assessment. The Operational Field Assessment for the wearable prototypes will be conducted in conjunction with the Option III Area Detector no later than month 33.



| | | 2022 | | | 2023 | | | | | | | | | | | | | 2024 | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Oct | Nov | Dec | Jan | Feb | Mar | Apr | May | Jun | Jul | Aug | Sep | Oct | Nov | Jan | Jul | Aug | Sep | Oct | Nov | Dec |
| WBS | Task | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| 1 | **Project Management** | | | | | | | | | | | | | | | | | | | | | |
| 2 | **Kick-Off Meeting** | | | | | | | | | | | | | | | | | | | | | |
| 2.1 | Project Plan | | | | | | | | | | | | | | | | | | | | | |
| 3 | **Requirements Definition & Application Trade Space** | | | | | | | | | | | | | | | | | | | | | |
| 4 | **Preliminary Design Review** | | | | | | | | | | | | | | | | | | | | | |
| 5 | **Design** | | | | | | | | | | | | | | | | | | | | | |
| 5.1 | Optical Design | | | | | | | | | | | | | | | | | | | | | |
| 5.2 | Electrical Design | | | | | | | | | | | | | | | | | | | | | |
| 5.2.1 | Electronic Design | | | | | | | | | | | | | | | | | | | | | |
| 5.2.2 | Algorithm Design | | | | | | | | | | | | | | | | | | | | | |
| 5.2.3 | Power Management Design | | | | | | | | | | | | | | | | | | | | | |
| 5.3 | Mechanical Design | | | | | | | | | | | | | | | | | | | | | |
| 5.4 | Software Design | | | | | | | | | | | | | | | | | | | | | |
| 6 | **Critical Design Review** | | | | | | | | | | | | | | | | | | | | | |
| 7 | **Fabrication and Testing** | | | | | | | | | | | | | | | | | | | | | |
| 7.1 | Optics | | | | | | | | | | | | | | | | | | | | | |
| 7.2 | Electrical Hardware Fabrication | | | | | | | | | | | | | | | | | | | | | |
| 7.3 | Mechanical Parts Fabrication | | | | | | | | | | | | | | | | | | | | | |
| 8 | **Firmware and Software Development** | | | | | | | | | | | | | | | | | | | | | |
| 8.1 | Firmware Development | | | | | | | | | | | | | | | | | | | | | |
| 8.2 | Software Development | | | | | | | | | | | | | | | | | | | | | |
| 9 | **Systems Integration and Testing** | | | | | | | | | | | | | | | | | | | | | |
| 9.1 | System Hardware Integration and Functional Test | | | | | | | | | | | | | | | | | | | | | |
| 9.2 | System Field Test | | | | | | | | | | | | | | | | | | | | | |
| 10 | **Wearable Prototypes Complete** | | | | | | | | | | | | | | | | | | | | | |
| 11 | **OFA - Combined OFA with Area Detector** | | | | | | | | | | | | | | | | | | | | | |
| 12 | **Commercialization Plan** | | | | | | | | | | | | | | | | | | | | | |
| 13 | **Final Report** | | | | | | | | | | | | | | | | | | | | | |
| | **Option III - Area Dectector Concurrent Effort (Option III Months)** | | | | | | | | | | | | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| | **Phase II - National Field Assessment (FA Months)** | | | | | | | | | | | | | | | | | | | | | |

*Figure1: Overview of Tasks Schedule for Wearable Detectors and Overall Schedule for Option III and Phase II (FY23-25)*

| | | 2025 | | | | | | | | | | | | 2026 | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Jan | Feb | Mar | Apr | May | Jun | Jul | Aug | Sep | Oct | Nov | Dec | Jan | Feb | Mar | Apr | May | Jun |
| WBS | Task | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 |
| 1 | **Project Management** | | | | | | | | | | | | | | | | | | |
| 2 | **Kick-Off Meeting** | | x | | | x | | | | | | | | | | | | | |
| 2.1 | Project Plan | | | | | | | | | | | | | | | | | | |
| 3 | **Requirements Definition & Application Trade Space** | | | | | | | | | | | | | | | | | | |
| 4 | **Preliminary Design Review** | | | | | | | | | | | | | | | | | | |
| 5 | **Design** | | | | | | | | | | | | | | | | | | |
| 5.1 | Optical Design | | | | | | | | | | | | | | | | | | |
| 5.2 | Electrical Design | | | | | | | | | | | | | | | | | | |
| 5.2.1 | Electronic Design | | | | | | | | | | | | | | | | | | |
| 5.2.2 | Algorithm Design | | | | | | | | | | | | | | | | | | |
| 5.2.3 | Power Management Design | | | | | | | | | | | | | | | | | | |
| 5.3 | Mechanical Design | | | | | | | | | | | | | | | | | | |
| 5.4 | Software Design | | | | | | | | | | | | | | | | | | |
| 6 | **Critical Design Review** | | | | | | | | | | | | | | | | | | |
| 7 | **Fabrication and Testing** | | | | | | | | | | | | | | | | | | |
| 7.1 | Optics | | | | | | | | | | | | | | | | | | |
| 7.2 | Electrical Hardware Fabrication | | | | | | | | | | | | | | | | | | |
| 7.3 | Mechanical Parts Fabrication | | | | | | | | | | | | | | | | | | |
| 8 | **Firmware and Software Development** | | | | | | | | | | | | | | | | | | |
| 8.1 | Firmware Development | | | | | | | | | | | | | | | | | | |
| 8.2 | Software Development | | | | | | | | | | | | | | | | | | |
| 9 | **Systems Integration and Testing** | | | | | | | | | | | | | | | | | | |
| 9.1 | System Hardware Integration and Functional Test | | | | | | | | | | | | | | | | | | |
| 9.2 | System Field Test | | | | | | | | | | | | | | | | | | |
| 10 | **Wearable Prototypes Complete** | | | | | | | | | | | | | | | | | | |
| 11 | **OFA - Combined OFA with Area Detector** | | | | | | | | | | | | | | | | | | |
| 12 | **Commercialization Plan** | | | | | | | | | | | | | | | | | | |
| 13 | **Final Report** | | | | | | | | | | | | | | | | | | |
| | **Option III - Area Dectector Concurrent Effort (Option III Months)** | 16 | 17 | 18 | 19 | 20 | 21 | | | | | | | | | | | | |
| | **Phase II - National Field Assessment (FA Months)** | | | | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |

*Figure 2 Continued: Overview of Task Schedule for Wearable Detectors and Overall Schedule for Option III and Phase II (FY25-26)*

### 2.2.2 Deliverables – Wearable Detectors

| Item | Deliverable | Due By |
|---|---|---|
| 1 | Post Award /Project Kick-Off Meeting | NLT 30 business days After Contract Award (ACA) |
| 2 | Project Plan | NLT 30 business days ACA |
| 3 | Monthly Progress Reports: Report of technical progress and financial status updates | Two Business Days prior to Monthly Progress Meeting |
| 4 | Monthly Progress Meetings (Teleconference) | Monthly, coordinate date with Government |
| 5 | Preliminary Design Review (PDR) | Within 90 business days ACA |
| 6 | Technology Readiness Assessment Documentation-System and Sub-System Documents | Six-Weeks Prior to CDR |
| 7 | Critical Design Review (CDR) | Month 6 |
| 8 | Technology Readiness Assessment Documentation-Critical Technology Elements Evidence | Two-Weeks After the CDR |

| Item | Deliverable | Due By |
|---|---|---|
| 9 | Test Report: Report of field test results performed by TSC and FLIR EOC Team | Month 17 |
| 10 | Prototypes: **Five (5) completed** ALTAR wearable detector prototypes including the associated battery packs and operating manual. The government reserves the option to bypass and/or delay the delivery of the final prototype(s). If this option is exercised, the government maintains ownership rights of those prototypes and can recall them at a later date. Any prototypes recalled must be operational and meet the requirements and/or specifications of the contract. | Month 17 |
| 11 | Operational Field Assessment (OFA) | NLT 33 months ACA, |
| 12 | Commercialization Plan | NLT Month 33 ACA |
| 13 | Phase I Final Report, and Close Out Meeting | Base Contract Month 33 |

## 2.3 EXERCISE OPTION III RANGE EXTENSION (AREA DETECTORS)

### 2.3.1 Technical Approach & Applicable Specifications for Area Detectors

The contractor shall develop and demonstrate an area laser light detector that can be mounted at an elevated position and be capable of scanning horizontally 360□. A rotating/scanning mechanism will be used to cover the larger angular scanning range (360□) without increasing the number of cameras. In addition to the hardware configuration differences 7of the area detector from the wearable detector, algorithm updates will be conducted to adapt the software developed for the wearable detector to the area detector. This area detector, which is a large area coverage device, will provide full spectral coverage of 400-1600 nm wavelength as compared to 400-1100 nm range of wearable detector. Indium Gallium Arsenide (InGaAs) focal planes will be used within the area detector versus the silicon used in the wearable detector. In addition to the custom Vis-SWIR specific micropatterned multispectral filters required, additional labor to laminate custom filters to the InGaAs focal planes will be required and the contractor has verified that customization of micropatterned multi-spectral filter will cover the 400-1600 nm spectral range as needed.

Table: Multi-Spectrum Laser Detection Specifications – Applicable to Option III Area Detector

| Specification | Customized Micro-Patterned Multi-Spectral Filters Option | |
|---|---|---|
| | Threshold | Objective |
| Spectral coverage | 400 –1600 nm (InGaAs) | 400 –1700 nm (InGaAs) |
| FOV | 360°H×60° | |

| | V | |
|---|---|---|
| Threat wavelength resolution | <85 nm | <50 nm |
| Threat detection range | >200 m | >500 m |
| Context camera Image range (detect human) | >200 m | >300 m |

### 2.3.2 Option III Tasks – Area Detectors

| Task 1 | PROJECT MANAGEMENT | Duration: 12 Months |
|---|---|---|
| | **Main Deliverables:** Monthly Progress & Status Report and Briefing | |
| | **Objective:** Effectively manage technical and financial execution of the tasks and provide continuous updates to DHS PM and COR.<br>**Approach:** Contractor shall provide a monthly progress & status update to the PM and COR on nominally second Thursday of every month. PowerPoint charts for briefing and MS word status report will be provided prior to the meeting. Contractor shall provide documentation or demonstrations sufficient for the PM and COR to evaluate the system elements of the Contractor's solution. Documents or demonstrations may include test results, design documentation, and systems analysis.<br>**Exit criteria:** Successful execution of the task. | |

| Task 2 | KICK-OFF MEETING | Duration: 1 month |
|---|---|---|
| | The contractor shall facilitate the kick-off meeting. The scope and content of the meeting shall only address the topics listed below if they diverge from the base contract lick-off meeting. The kick-off meeting will take place either at the contractor's facility, DHS S&T headquarters, or via teleconference.<br><br>• Introduction of the Project Team<br>• Option III technical Goals and Mission Scenarios or Concept of operation<br>• Demonstration of Existing Technology<br>• Potential technical risks and mitigation strategies<br>• Performance metrics/testing events that will be used to measure progress against completed Phases and Project milestones<br>• Overview of Commercialization Objectives and Plan<br>• Updated Project Plan **(2.1) and Area Detector Schedule**<br>• Objectives and Technical Approach for Design Reviews and Operational Field Assessments<br>  ○ Preliminary Design Review (PDR)<br>  ○ Critical Design Review (CDR)<br>  ○ Operational Field Assessment (OFA)<br>  ○ Technology Readiness Assessment (TRA) | |

| Task 3 | PRELIMINARY DESIGN | |
|---|---|---|
| 3.1 | **Requirements Definition** | **Duration:** 1 month |
| | **Main Deliverables:** Finalized component and system specifications or Product Requirements Document | |
| | **Objective:** Develop system requirements and specifications, and flow down to components.<br>**Approach:** Finalize concept of operations and develop system requirements with feedback from Government.<br>**Exit criteria:** System requirements and specifications finalized and flowed down to sub-systems and components. | |
| 3.2 | **Preliminary Design** | **Duration:** 2 months |
| | **Main Deliverables:** Preliminary design material, documentation | |
| | **Objective:** Design of laser threat detection system, including control electronics, embedded processing, and power supply/distribution.<br>**Approach:** Define architecture, components and interfaces. These include optical, sensor head, mechanical motor and controller and software.<br>**Exit criteria:** Design meeting requirements is ready for the PDR. | |

| Task 4 | PRELIMINARY DESIGN REVIEW | **Duration:** 1 month |
|---|---|---|
| | The contractor shall participate in the PDR meeting to present the current design and to receive feedback from stakeholders, to include but not limited to program manager, First Responder Resource Group (FRRG) technical expertise, and project advisors. The main purpose of this review is to assess the initial design and address any unmitigated risks associated with this effort. The PDR will assist in ensuring that the functional requirements have been allocated to the various elements of the system and that the application and associated hardware can proceed with development, demonstration, testing and will likely meet stated performance requirements.<br><br>The contractor shall provide the following information at the PDR meeting.<br>• Technical documentation showing the preliminary system architecture diagrams, preliminary external and internal interfaces<br>• System requirements, functional requirements, preliminary interface requirements (external and internal), and requirements verification methodology<br>• System design constraints and their incorporation into requirements.<br>• A preliminary list of configuration items (CI)<br>• Risk assessment matrix showing all identified risks, their severity, likelihood, impact, and associated mitigation plans<br>• Updated cost estimation for the project<br>• User interface requirements including system functions:<br>  • Roles of human operators and automation in each function<br>  • Operator tasks and task sequences<br>  • Performance requirements associated with tasks<br>  • Operational environmental impacts on task performance<br>  • Requirements for operator interaction with automated processes | |

| Task 4 | PRELIMINARY DESIGN REVIEW | Duration: 1 month |
|---|---|---|
| | • Preliminary design requirements for user interfaces<br>• Methods and metrics to be employed in operator performance and user interface evaluation.<br><br>Contractor shall provide PDR presentation three workdays prior to the PDR meeting. | |

| Task 5 | CRITICAL DESIGN | |
|---|---|---|
| 5.1 | **Sensor Head Design** | **Duration:** 3 months |
| | **Main Deliverables:** Critical design material covering the scanner head | |
| | **Objective:** Critical design of the scanning head.<br>**Approach:** Select off-the-shelf cameras, custom filter, and lenses based on system requirements and optical models. Perform bench top tests with surrogate component hardware.<br>**Exit criteria:** Completion of sensor head design meeting system requirements. | |
| 5.2 | **Scanner Design** | **Duration:** 3 months |
| | **Main Deliverables:** Critical design materials covering the mechanical rotation, stepping | |
| | **Objective:** Critical design of mechanical scanner, including motor and motor controller<br>**Approach:** Develop motion control architecture supporting image capture from the scanning head to cover 360 deg horizontal range. Specify components and electrical interfaces.<br>**Exit criteria:** Completion of scanning subsystem meeting system requirements. | |
| 5.3 | **Software and Algorithm Design** | **Duration:** 3 months |
| | **Main Deliverables:** Critical design materials covering the software and algorithms | |
| | **Objective:** Critical design of software and firmware design.<br>**Approach:** Detailed design of software and firmware including image acquisition, threat detection, scanning, and user interface.<br>**Exit criteria:** Completion of software components meeting system requirements**.** | |

| Task 6 | CRICTICAL DESIGN REVIEW | Duration: 1 month |
|---|---|---|
| | The contractor shall participate in the Critical Design Review (CDR) meeting to present the final design and to receive feedback from stakeholders, to include but not limited to program manager, First Responder technical expertise and project advisors. The main purpose of this review is to evaluate the final design against the performance specifications and requirements of the contract, and to address any unmitigated risks associated with this effort. The CDR will ensure that the requirements contained in the ~~Statement of Work~~ SOW are adequately addressed and likely satisfied and that the application and associated hardware can proceed into final development, demonstration, testing phases and meets the stated performance specifications and requirements.<br><br>The contractor shall provide the following information at the CDR meeting.<br><br>• Technical documentation showing detailed hardware and software design including final system architecture diagrams, final external and internal interfaces diagrams, and requirements<br>• Updated system design constraints and their incorporation into requirements.<br>• Final CI list<br>• Updated risk assessment matrix showing all identified risks, their severity, likelihood, impact, and associated mitigation plans<br>• Updated cost estimation for the project<br>• User interface Documentation: drawings or pictures, functional description of controls and displays, operator task sequences for selected scenarios, testing and evaluation requirements for operator performance and user interface usability assessment. Results of any prior end-user and user interface testing.<br><br>Contractor shall provide CDR presentation three workdays prior to the CDR meeting. | |

| Task 7 | FABRICATION AND COMPONENT TESTING | |
|---|---|---|
| 7.1 | **Sensor Head Fabrication and Test** | **Duration:** 7 months |
| | **Main Deliverables:** Reports of technical progress | |
| | **Objective:** Fabricate core optical system for laser detection at various wavelengths.<br>**Approach:** Procure off-the-shelf camera and custom filters, and build system based on optical and opto-mechanical design, and meeting precision alignment requirements. Allow for sufficient procurement time for patterned filter by initiating fabrication prior to CDR with customer approval. Test and characterize subsystem. Perform laser power measurement calibration and generate calibration table for the optical sensor.<br>**Exit criteria:** Complete sensor head optical system hardware ready for integration. | |
| 7.2 | **Scanner Fabrication and Test** | **Duration:** 2 months |
| | **Main Deliverables:** Reports of technical progress | |

| Task 7 | FABRICATION AND COMPONENT TESTING | |
|---|---|---|
| | **Objective:** Fabricate mechanical and scanning components and overall package.<br>**Approach:** Fabricate and test motor and controller with surrogate load simulating sensor head, fabricate overall package to integrate scanner with the optical sensor head. Fabricate and test power supply circuitry to meet component voltage and current need.<br>**Exit criteria:** Scanner ready for integration with sensor. | |
| 7.3 | **Software Development and Test** | **Duration:** 6 months |
| | **Main Deliverables:** Reports of technical progress | |
| | **Objective:** Fabricate mechanical components and ruggedized system packaging.<br>**Approach:** Fabricate, inspect, and test components. Validate against design and tolerance requirements.<br>**Exit criteria:** Completion of mechanical system hardware. | |

| Task 8 | SYSTEM INTEGRATION AND TESTING | **Duration:** 3 Months |
|---|---|---|
| | **Main Deliverables:** Monthly Progress & Status Report and Briefing<br>**Objective:** System Hardware Integration and Functional and Ruggedization Testing<br>**Approach:** Integrate sub systems.<br><br>Calibrate cameras for image registration and fusion.<br><br>Perform functional test including image capture, mechanical scanning laser power measurements, laser threat categorization, alarm actuation, and user alert. Implement field test scenarios and execute test plan, with feedback from FRG. Record test results. Make necessary refinements and improve system field performance. Document test procedure and results. Hold at least one set of components in reserve if repair is needed during internal testing or OFA.<br><br>Perform ruggedization testing of the prototypes to ensure they meet the standards outlined in section 1.4.1.2 Standards, within the base contract.<br><br>**Exit criteria:** Successful integration and thorough testing of prototype system, prototype ready for delivery | |

| Task 9 | PROTOTYPES DELIVERED | |
|---|---|---|
| | Prototypes Delivery | Duration: 1 months |
| | **Main Deliverables:** Three (3) ALTAR Area Detector prototypes with operation manual | |
| | **Objective:** Deliver prototypes<br>**Approach:** Produce user operation manual. Deliver a complete system to DHS S&T<br>**Exit criteria:** Complete system and user manual delivered to DHS S&T | |

| Task 10 | OPERATIONAL FIELD ASSESSMENT |
|---|---|
| | The performer shall participate in a one-day Operational Field Assessment (OFA) conducted by the National Urban Security Technology Laboratory (NUSTL) approximately 1-2 months before the end of the period of performance (POP). At the OFA, up to nine first responders will evaluate the prototype product by using it under simulated operational conditions to assess: (a) performance against project requirements, (b) usability of the prototype, and (c) compatibility with operations. The performer shall provide at least three functional prototypes for the OFA. At the end of the OFA the prototypes shall be returned to the performer, except where S&T specifies otherwise. |
| **10.1** | **OFA Planning (3 months)**<br><br>At least three (3) months in advance of the OFA, the performer shall provide to S&T a thorough written description of the prototype to be tested, including, but not limited to: hardware and software components, installation, functions and capabilities, methods of operation, connections between device components and connections to the user, optional settings, power requirements, material, dimensions and weight or available size options, additional hardware or software needed for operation, and any safety or privacy considerations associated with its construction or usage. If the device includes software, the performer shall also provide a description of any user accounts, terms of service, use of external data streams, and internet or Bluetooth connectivity involved in its usage. The performer shall provide a physical sample or images of the prototype along with the description and shall identify any proprietary information included in the text or the images.<br><br>**OFA Venue and Event**<br>The OFA will be conducted at a suitable venue to be selected by S&T. The performer shall travel to the venue and be available the day before the OFA to participate in setting up and going through a dry run of the OFA activities. On the day of the OFA, the performer shall provide a brief presentation (about 10 – 20 minutes duration) describing the device development and a summary of the results of any relevant laboratory and pilot testing conducted. Additionally, the performer shall provide training on the use of the device to the evaluators and assist them with proper fitting and set-up as appropriate. The performer's proposed overview and training presentations shall be provided to S&T not later than one week before the OFA for review and concurrence.<br><br>**Option to Extend Period of Performance to conduct OFA**<br><br>If it is not feasible to conduct the OFA prior to the end of the POP due to insufficient technology readiness, extreme weather conditions, lack of evaluators, limited venue availability, or other unforeseen circumstances, S&T retains the option to extend the POP at no additional cost to the Government, excluding performer travel and shipment of prototypes.<br><br>**Option to forgo OFA** |

| Task 10 | OPERATIONAL FIELD ASSESSMENT |
|---|---|
| | If it is determined that an OFA is not of benefit to the government S&T retains the option to forgo the OFA. |
| **10.2** | **OFA Support (1 month)** |
| | Contractor shall collect OFA user feedback to develop system improvement and technology transition and productization plan. |

| Task 11 | COMMERCIALIZATION PLAN |
|---|---|
| | The contractor shall update the Commercialization Plan developed for the wearable detector during the base contract period to include the area detector. In the Commercialization Plan, the contractor shall consider state, local, and federal government, and private-sector purchase and employment of their system. The plan shall also provide analysis of purchase, operations, and maintenance (O&M), and disposal of individual components and the system.<br><br>Should the government choose to proceed with the commercialization plan, the government will evaluate the proposed costs for reasonableness. If the government elects to proceed with the plan, a change order or Request for Equitable Adjustment (REA) will be conducted. |

| Task 12 | FINAL REPORT |
|---|---|
| | The Contractor shall provide a final report, including test data, at the conclusion of the effort. |

### 2.3.3 Area Detector Schedule

Figure 1, Overview of Tasks Schedule, shows an overview of the scheduled tasks. Throughout the execution of this contract, the Contractor's Principal Investigator/Program Manager shall work with the S&T Program Manager and Contracting Officer Representative to arrange suitable times for the Preliminary Design Review, Critical Design Review, and the Operational Field Assessment.

| | Base Month # | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| WBS | Task | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 1 | Project Management | | | | | | | | | | | | | | | | | | | | | |
| 2 | Kick-Off Meeting | | | | | | | | | | | | | | | | | | | | | |
| 2.1 | Project Plan | | | | | | | | | | | | | | | | | | | | | |
| 3 | Preliminary Design | | | | | | | | | | | | | | | | | | | | | |
| 3.1 | Requirements Definition | | | | | | | | | | | | | | | | | | | | | |
| 3.2 | Preliminary Design | | | | | | | | | | | | | | | | | | | | | |
| 4 | Preliminary Design | | | | | | | | | | | | | | | | | | | | | |

| | Base Month # | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| WBS | Task | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| | Review | | | | | | | | | | | | | | | | | | | | | |
| 5 | Critical Design | | | | | | | | | | | | | | | | | | | | | |
| 5.1 | Sensor Head Design | | | | | | | | | | | | | | | | | | | | | |
| 5.2 | Scanner Design | | | | | | | | | | | | | | | | | | | | | |
| 5.3 | Software and Algorithm Design | | | | | | | | | | | | | | | | | | | | | |
| 6 | CDR | | | | | | | | | | | | | | | | | | | | | |
| 7 | Fabrication and Component Testing | | | | | | | | | | | | | | | | | | | | | |
| 7.1 | Sensor Head Fabrication and Test | | | | | | | | | | | | | | | | | | | | | |
| 7.2 | Scanner Fabrication and Test | | | | | | | | | | | | | | | | | | | | | |
| 7.3 | Software Development and Test | | | | | | | | | | | | | | | | | | | | | |
| 8 | System Integration and Testing | | | | | | | | | | | | | | | | | | | | | |
| 9 | Prototypes Delivered | | | | | | | | | | | | | | | | | | | | | |
| 10 | OFA | | | | | | | | | | | | | | | | | | | | | |
| 10.1 | OFA Planning | | | | | | | | | | | | | | | | | | | | | |
| 10.2 | OFA Support | | | | | | | | | | | | | | | | | | | | | |
| 11 | Commercialization Plan V1 | | | | | | | | | | | | | | | | | | | | | |
| 12 | Phase I Final Report | | | | | | | | | | | | | | | | | | | | | |

*Figure 3: Overview of Tasks Schedule for Area Detector*

### 2.3.4 Deliverables – Area Detectors

| Item | Deliverable | Due By |
|---|---|---|
| 1 | Post Award /Option III Kick-Off Meeting | NLT 30 business days After Contract Award (ACA) |
| 2 | Project Plan | NLT 30 business days ACA |
| 3 | Monthly Progress Reports: Report of technical progress and financial status updates | Two Business Days prior to Monthly Progress Meeting |

| Item | Deliverable | Due By |
|---|---|---|
| 4 | Monthly Progress Meetings (Teleconference) | Monthly, coordinate date with Government |
| 5 | Preliminary Design Review (PDR) | NLT 4 months ACA Option III |
| 6 | Technology Readiness Assessment Documentation-System and Sub-System Documents | Six-Weeks Prior to CDR |
| 7 | Critical Design Review (CDR) | NLT 6 months ACA Option III |
| 8 | Technology Readiness Assessment Documentation-Critical Technology Elements Evidence | Two-Weeks After the CDR |
| 7 | Reports: 1. Results of field tests performed by the contractor Results of ruggedization tests performed by the contractor | Option III Month 17 |
| 8 | Prototypes: **Three (3) ALTAR Area Detector** prototypes including the associated operating manual.<br><br>The government reserves the option to bypass and/or delay the delivery of the final prototype(s). If this option is exercised, the government maintains ownership rights of those prototypes and can recall them at a later date. Any prototypes recalled must be operational and meet the requirements and/or specifications of the contract. | Option III Month 21 |
| 9 | Operational Field Assessment (OFA) | NLT 21 months ACA (Option III) |
| 10 | Commercialization Plan | NLT 21 months ACA (Option III) |
| 11 | Final Report, and Close Out Meeting | Option III Month 21 |

## 2.4 FIRST RESPONDER FIELD ASSESSMENTS OF WEARABLE AND AREA PROTOTOYPES

### 2.4.1 Objective

The First Responder Field Assessments will involve end-users from up to five Federal, State, and Local law enforcement agencies in a structured test protocol to evaluate the ALTAR Wearable and Area Detector prototypes in relevant operational environments. This protocol will guide end-users through an independent assessment of the prototypes' interface and functionality. Feedback collected will inform several R&D outcomes for the Multi-Spectrum Laser Detection System solution:

1. Solution Refinement: Identify areas for improvement in the prototypes, including feature enhancement, usability, and overall performance.
2. Validation and Metrics: Validate integrated technology solution in real-world

scenarios, assessing metrics like detection accuracy, response time, and reliability. Ensure the solution achieves a TRL 7 readiness level before it transitions into the commercial market.

3. User-Centric Design: Use feedback to inform iterative design decisions, tailoring the technology to meet the operational needs of first responders.

### 2.4.2 First Responder Field Assessment Tasks

| Task 1 | PROJECT MANAGEMENT | Duration: 12 Months |
|---|---|---|
| | **Main Deliverables:** Monthly Progress & Status Report and Briefing | |
| | **Objective:** Effectively manage technical and financial execution of the tasks and provide continuous updates to DHS PM and COR.<br>**Approach:** Contractor shall provide a monthly progress & status update to the PM and COR on nominally second Thursday of every month. PowerPoint charts for briefing and MS word status report will be provided prior to the meeting. Contractor shall provide documentation or demonstrations sufficient for the PM and COR to evaluate the system elements of the Contractor's solution. Documents or demonstrations may include test results, design documentation, and systems analysis.<br>**Exit criteria:** Successful execution of the task. | |

| Task 2 | DEPARTMENT ASSESSMENT PLAN | Duration: 3 Months |
|---|---|---|
| | **Main Deliverables:** None | |
| | **Objective:** Effectively assist in the development of the Department Assessment Plan.<br>**Approach:** The Contractor shall provide documentation to inform the development of the assessment plan. The contractor will review and provide comments to guide the assessment plan that developed by another entity. Documents may include but not limited to internal test protocols and results, design documentation, and systems analysis.<br>**Exit criteria:** Successful execution of the task. | |

| Task 3 | REVIEW & INCORPORATE OFA I FEEDBACK | Duration: 3 Months |
|---|---|---|
| | **Main Deliverables:** None | |
| | **Objective:** Review initial functional and user interface feedback from base contract OFA to determine which enhancements can be feasibly incorporated into prototype design.<br>**Approach:** Address initial feedback from previous operational field assessment conducted in the base contract to develop and present an updated design for the assessment prototypes.<br>**Exit criteria:** Successful Completion of Task. | |

| Task 4 | ASSESSMENT PROTOTYPE DESIGN REVIEW I | Duration: 3 Months |
|---|---|---|
| | **Main Deliverables:** Design Review I event – Teleconference or In-Person | |
| | **Objective:** Conduct meeting to review design updates that would be incorporated from Task 3.0, OFA feedback | |

| Task 4 | ASSESSMENT PROTOTYPE DESIGN REVIEW I | Duration: 3 Months |
|---|---|---|
| | **Approach:** The contractor shall coordinate a design review meeting to present a proposed design of the assessment prototypes and to receive feedback from stakeholders, to include but not limited to program manager, First Responder technical expertise and project advisors. The main purpose of this review is to evaluate the prototypes' updated design ensuring the performance specifications and requirements of the contract are maintained, and to address any unmitigated risks associated with this effort.<br>The contractor shall provide the following information at the design review meeting, as applicable:<br>• Updated Technical documentation showing detailed hardware and software design including final system architecture diagrams, final external and internal interfaces diagrams, and requirements.<br>• Updated system design constraints and their incorporation into requirements.<br>• Updated CI list<br>• Updated risk assessment matrix showing all identified risks, their severity, likelihood, impact, and associated mitigation plans.<br>• Updated User interface Documentation: drawings or pictures, functional description of controls and displays, operator task sequences for selected scenarios, testing and evaluation requirements for operator performance and user interface usability assessment. Results of any prior end-user and user interface testing.<br>Contractor shall provide Design Review presentation three workdays prior to the Design Review Meeting.<br>**Exit criteria:** Successful Completion of Task. | |

| Task 5 | PROTOTYPE UPDATE AND TESTING LOOP #1 | Duration: 3 Months |
|---|---|---|
| | **Main Deliverables:** Internal Test Results during monthly update meetings. | |
| | **Objective:** Fully integrate and test updated prototypes, one each Wearable and Area prototype, per Design Review I results | |
| | **Approach:** Update one of each prototype and conduct in-house testing and refinement of prototypes to ensure Design Review I updates are performing as expected prior to fabrication of additional assessment prototypes. Contractor will provide in-house test data results in the monthly report and during the monthly update meetings. Test data will reflect the capabilities tested, the performance parameters, and the actual level of performance displayed during the testing.<br>**Exit criteria:** Verified Completion of One (1) fully- integrated and tested Aerial ALTAR Prototype and One (1) fully- integrated tested Wearable ALTAR prototype, with enhanced functions. | |

| Task 6 | PRODUCE PROTOTYPES FOR FIELD ASSESSMENT | Duration: 3 Months |
|---|---|---|
| | **Main Deliverables:** S i x ( 6) additional ALTAR Wearable Prototypes and Six (6) additional ALTAR Area Prototypes.<br>**Objective:** Produce additional fully integrated and tested prototypes based on the results of the Prototype Update and Testing Loop #1, prepared to distribute for First Responder end-user assessment.<br>**Approach:** Contractor will produce six (6) additional ALTAR Wearable and Area prototypes | |

| Task 6 | PRODUCE PROTOTYPES FOR FIELD ASSESSMENT **Duration:** 3 Months |
|---|---|
| | each, test each prototype according to internal testing protocols to ensure they are performing consistently as expected, and update user operating manual and training material as necessary. All prototypes should include an equipment tag that identifies the prototypes as DHS property. Each property tag shall include a unique serial # for every major system component.<br>**Exit criteria:** Verified completion of Six (6) fully- integrated and tested Aerial ALTAR Prototype and six (6) fully- integrated tested Wearable ALTAR prototype, with enhanced functions. |

| Task 7 | FIELD ASSESSMENT TRAINING AND PROTOTYPE DISTRIBUTION **Duration:** 3 Months |
|---|---|
| | **Main Deliverables:** Prototype Distribution and End-User Technical Training, Distribution Report.<br>**Objective:** Produce additional fully integrated and tested prototypes based on the results of the Prototype Update and Testing Loop #1, prepared to distribute for First Responder end-user assessment.<br>**Approach:** Contractor will assist in the coordination of the training/ distribution event and travel to five department sites to distribute one (1) each ALTAR Wearable and Area prototypes and associated user manuals to each department collaborator. Contractor will also conduct end-user training at each collaborator site.<br>**Exit criteria:** Successful Completion of Task. |

| Task 8 | FIELD ASSESSMENT TECHNICAL ASSISTANCE **Duration:** 3 Months |
|---|---|
| | **Main Deliverables:** Technical Assistance Report |
| | **Objective:** Ensure end-user technical support throughout the established assessment period.<br>**Approach:** Contractor will provide ad-hoc operations and maintenance support to each department collaborator via teleconference, or by conducting follow-up site visits additional training, if necessary. The contractor will retain spare system and will arrange for any necessary repair or replacement of system or system components to ensure collaborators can conduct assessments throughout the assessment period. Contractors also will provide a report detailing support provided such as site visits, operations & maintenance request, prototype replacements, and any feedback received from First Responders during these exchanges. Note: if a prototype is replaced, contractor shall record and provide the serial #s of the prototypes exchanged.<br>**Exit criteria:** Successful Completion of Task. |

| Task 9 | POST ASSESSMENT WORKSHOP **Duration:** 3 Months |
|---|---|
| | **Main Deliverables:** None |
| | **Objective:** Participate in post assessment Workshop. |

| Task 9 | POST ASSESSMENT WORKSHOP | Duration: 3 Months |
|---|---|---|
| | **Approach:** Contractor will participate in a post assessment workshop that will use analyzed data and feedback collected during the assessment period to identify and prioritize additional refinements that would optimize or enhance the functionality of the prototypes.<br>**Exit criteria:** Successful Completion of Task. | |

| Task 10 | REVIEW & INCORPORATE ASSESSMENT FEEDBACK | Duration: 3 Months |
|---|---|---|
| | **Main Deliverables:** None | |
| | **Objective:** Review functional and user interface feedback from first responder field assessment collaborators.<br>**Approach: The contractor will** Address feedback received from Task #9 post Assessment workshop to develop and present an updated design for the final prototypes**.**<br>**Exit criteria:** Successful Completion of Task. | |

| Task 11 | DESIGN REVIEW II | Duration: 3 Months |
|---|---|---|
| | **Main Deliverables:** None | |
| | **Objective:** Review functional and user interface feedback from first responder field assessment collaborators.<br>**Approach: The contractor will** Address feedback received from Task #9 post Assessment workshop to develop and present an updated design for the final prototypes**.**<br>**Exit criteria:** Successful Completion of Task. | |

| Task 12 | PROTOTYPE UPDATE AND TESTING LOOP #2 & TRA | Duration: 3 Months |
|---|---|---|
| | **Main Deliverables:** Internal Test Results during monthly update meetings. | |
| | **Objective:** Fully integrate and test updated prototypes, one each Wearable and Area prototype, per Design Review II results.<br>**Approach:** Update one of each prototype and conduct in-house testing and refinement of prototypes to ensure Design Review II updates are performing as expected prior to fabrication of additional assessment prototypes. Provide updated design and testing data and/or reports to facilitate updating the TRA previously completed.<br>**Exit criteria:** Verified Completion of One (1) fully- integrated and tested Aerial ALTAR Prototype and One (1) fully- integrated tested Wearable ALTAR prototype, with enhanced functions. | |

| Task 13 | PRODUCE UPDATED PROTOTYPES FOR TESTING & EVALUATION | Duration: 3 Months |
|---|---|---|
| | **Main Deliverables:** None. | |
| | **Objective:** Update six (6) Wearable and three (3) Area detector prototypes based on the results of task 12, Prototype Update and Testing Loop #2.<br>**Approach:** Contractor will update six (6) additional ALTAR Wearable and three (3) Area prototypes each, test each prototype according to internal testing protocols to ensure they are performing consistently as expected, and update user operating manual and training material | |

| Task 13 | **PRODUCE UPDATED PROTOTYPES FOR TESTING & EVALUATION Duration:** 3 Months |
|---|---|
| | as necessary.<br>**Exit criteria:** Verified Completion of three (3) fully- integrated and tested Aerial ALTAR Prototype and six (6) fully- integrated tested Wearable ALTAR prototypes, with enhanced functions. |

| Task 14 | **TESTING & EVAL & FINAL DOCUMENTATION** | **Duration:** 3 Months |
|---|---|---|
| | **Main Deliverables:** Six (6) fully integrated, updated Wearable ALTAR prototypes; Three (3) Area ALTAR prototypes. | |
| | **Objective:** Update six (6) Wearable and three (3) Area detector prototypes based on the results of task 12, Prototype Update and Testing Loop #2.<br>**Approach:** Contractor personnel will travel to T&E location, which is to be determined, and equipment and materials necessary to participate the event. Contractor will also update and produce the **final** version of the following documents:<br>• User Operating Manual<br>• Final Phase II Field Assessment Technical Report<br>• Prototype Property Report<br>• Updated Commercialization Plan<br><br>**Exit criteria:** Delivery of three (3) fully- integrated and tested Aerial ALTAR Prototype and six (6) fully- integrated tested Wearable ALTAR prototypes, with enhanced functions. Successful completion of Testing & Evaluation event.<br><br>**Note:** The final Technical Report must include detailed information on all relevant activities, findings, and modifications made throughout the project. Specifically, the report will cover:<br>• Documentation of design decisions, technical details, test data, and trade-offs made during implementation.<br>• Data deliverables that reflect a systematic and objective assessment of the prototypes' capabilities and performance.<br>• Integration of First Responder feedback and the resulting system adjustments and modifications. | |

### 2.4.3 First Responder Field Assessment Deliverables

| Item | Task Title | Deliverable | Due By |
|---|---|---|---|
| Task 1 | Project Management | • Monthly Status Reports | Two (2) business days prior to Monthly Progress meeting |
| | | • Monthly Progress Meetings (Teleconference) | Monthly, coordinate date with Government |
| Task 2 | Department Assessment Plan | • Feedback on First Responder Assessment Plan | As requested |

| Item | Task Title | Deliverable | Due By |
|---|---|---|---|
| Task 3 | Review and Incorporate OFA I Feedback | Report of briefing detailing feedback incorporated | NLT Field Assessment (FA) Month One (1) |
| Task 4 | Design Review I | Design Review I - Briefing and Report | NLT End of FA Month Two (2) |
| Task 5 | Prototype Update & Testing Loop #1 | Verified Completion of One (1) fully-integrated and tested Aerial ALTAR Prototype and One (1) fully- integrated tested Wearable ALTAR prototype, with enhanced functions. | NLT End of FA Month 6 |
| | Technology Readiness Assessment (TRA) Documentation I | Provide updated design and testing data and/or reports to facilitate updating the TRA completed during the Base Contract | Two (2) weeks after task Prototype Update and Testing Loop #1 is completed |
| Task 6 | Produce Prototypes for Field Assessments | • Six (6) additional ALTAR Wearable Prototypes and Six (6) additional ALTAR Area Prototypes<br>• Updated User Operating Manual and Training Material | NLT End of FA Month 6 |
| Task 7 | Prototype Distribution and Training | • End User Training to five Department Collaborators<br>• Distribution Report | NLT End of FA Month 7 |
| Task 8 | Department Field Assessment Coordination | • Technical Assistance Report | Every four (4) weeks during assessment period; and at completion of the assessment period |
| Task 9 | Post Field Assessment Workshop | • Participate in Post Field Assessment Workshop | When scheduled, but NLT FA Month 9 |
| Task 10 | Review & Incorporate Assessment Feedback | • Report or briefing detailing feedback incorporated | Two (2) weeks after the conclusion of the Post Field Assessment Workshop |
| Task 11 | Design Review II | • Design Review II Briefing Report | 30 Days after First Responder Field Assessment Workshop |
| Task 12 | Prototype Update and Testing Loop #2 | • Internal Report & briefing detailing the status of the updates made to the prototypes and testing results<br>• Updated TRA Documentation, as necessary | Two (2) weeks after task Prototype Update and Testing Loop #2 is completed |
| Task 13 | Produce updated Prototypes for Test & Evaluation (T&E) Assessment | • Deliver Six (6) Wearable and three (3) Area prototypes<br>• Updated User Operating Manual and | 30 Days after Prototype Update and Testing Loop #2 |

| Item | Task Title | Deliverable | Due By |
|---|---|---|---|
| | | Training Material | |
| Task 14 | T&E Coordination | • Participation in T&E event | NLT FA Month 12 |
| | Final Documentation | Documentation to be delivered:<br>• User Operating Manual<br>• Final Field Assessment Technical Report<br>• Prototype Property Report<br>• Commercialization Plan | NLT FA Month 12 |

### 2.4.4 First Responder Field Assessment Schedule

| Base Month # | | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Field assessment month # | | | | | | | | | | | | | |
| Task # | Task Title | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| T1 | Monthly Progress Reports | | | | | | | | | | | | |
| T2 | Department Assessment Plan | | | | | | | | | | | | |
| T3 | Incorporate OFA Feedback | | | | | | | | | | | | |
| T4 | Critical Design Review (CDR1) | | | | | | | | | | | | |
| T5 | Prototype Update and Testing Loop #1 | | | | | | | | | | | | |
| | Technology Readiness Assessment (TRA) Documentation #1 | | | | | | | | | | | | |
| T6 | Produce Prototypes for Field Assessments | | | | | | | | | | | | |
| T7 | Department Field Assessment Roadshow | | | | | | | | | | | | |
| T8 | Department Field Assessment Coordination | | | | | | | | | | | | |
| T9 | Post Field Assessment Workshop | | | | | | | | | | | | |
| T10 | Incorporate Assessment Feedback | | | | | | | | | | | | |
| T11 | Critical Design Review (CDR2) | | | | | | | | | | | | |

| Base Month # | | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Field assessment month # | | | | | | | | | | | | | |
| Task # | Task Title | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| T12 | Prototype Update and Testing Loop #2 | | | | | | | | | | | | |
| | Technology Readiness Assessment (TRA) Documentation #2 | | | | | | | | | | | | |
| T13 | Produce updated Prototypes for Test & Evaluation (T&E) Assessment | | | | | | | | | | | | |
| T14 | T&E Coordination | | | | | | | | | | | | |
| T15 | Documentation | | | | | | | | | | | | |

*Figure 4: Phase II -National Field Assessment Schedule*

**Technology Readiness Assessments**

**Summary/Overview**

To effectively manage risk (technical and programmatic) and effectively transition suitable solutions to achieve DHS outcomes, DHS policy requires programs to assess the technical maturity of potential solutions during the systems design and development phases. Technology Readiness Assessments (TRA) are a systematic, evidence-based process used to evaluate the maturity of hardware and software technologies that are critical to either the performance of the system or the fulfillment of key objectives of the acquisition program.

TRAs are intended to assess the technical maturity of Critical Technology Elements (CTEs) within a specific application and within a specific environment. Therefore, it is possible for a CTE to be assessed at a high technology maturity in one application, but to be assessed at a low technology maturity in another application. It is important to emphasize that the TRA is an assessment of the CTEs and not an assessment of the overall system concept.

TRAs measure a technology's maturity using Technology Readiness Levels (TRLs), a maturity scale from 1-9 that is ordered according to the characteristics of both (a) the demonstration or testing environment; and (b) levels of fidelity in terms of technology form and integration with other elements of a system.

**Documentation Needed**

The TRA will be conducted by DHS S&T Systems Engineering and Standards Division (SESD) team. For the SESD team to conduct a comprehensive TRA, the vendor is required to provide documentation including but not limited to the following:

- Detailed system design documentation containing information regarding all components/sub-components and systems/sub-systems.
- Interface control documentation providing detailed information on all interfaces between components/ sub-components and systems/sub-systems.
- Requirements document showing high-level system design requirements and their corresponding decomposition to lower-level requirements.
- Hardware and software design documentation.
- System and critical component testing plans and test results.

**Data Rights**

Where the contractor has limited data rights of specific CTE(s), there are two options in handling TRA documentation needs. 1. The contractor can supply the qualifying data with limited rights or restricted rights. This option is supported by both federal employees and contractors having Non-Disclosure Agreements (NDA) in place, or 2. The contractor can provide form, fit, and function data with unlimited rights.

**Bypass Option**

The government reserves the option to bypass performing a Technology Readiness Assessment. If the government does exercise this option, then the specific documents required to perform the assessment do not need to be delivered. 2.3 Schedule.

## 3.0 CONTRACTOR PERSONNEL

### 3.1 QUALIFIED Personnel

The Contractor shall provide qualified personnel to perform all requirements specified in this SOW.

### 3.2 Continuity of Support

The Contractor shall ensure that the contractually required level of support for this requirement is maintained at all times. The Contractor shall 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 Contracting Officer's Representative (COR) prior to employee absence. Otherwise, the Contractor shall provide a fully qualified replacement.

### 3.3 Key Personnel

Before replacing any individual designated as *Key* by the Government, the Contractor shall notify the Contracting Officer no less than 15 business days in advance, submit written justification for replacement, and provide the name and qualifications of any proposed

substitute(s). All proposed substitutes shall possess qualifications equal to or superior to those of the *Key* person being replaced, unless otherwise approved by the Contracting Officer. The Contractor shall not replace *Key* Contractor personnel without approval from the Contracting Officer. The following Contractor personnel are designated as Key for this requirement. Note: The Government may designate additional Contractor personnel as *Key* at the time of award.

Key Personnel: Principle Investigator/Program Manager.

**3.3.1 Contractor:** *Key* personnel shall not be assigned by the Contractor to more than one key position for this requirement.

### 3.4 Employee Identification

Contractor employees visiting Government facilities shall wear an identification badge that, at a minimum, displays the Contractor name, the employee's photo, name, clearance-level, and badge expiration date. Visiting Contractor employees shall comply with all Government escort rules and requirements. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist at all times.

### 3.5 Employee Conduct

Contractor's 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, and possession of weapons) when visiting or working at Government facilities. The Contractor shall ensure Contractor employees present a professional appearance at all times and that their conduct shall not reflect discredit on the United States or the Department of Homeland Security. The Project Manager shall ensure Contractor employees understand and abide by Department of Homeland Security established rules, regulations and policies concerning safety and security.

### 3.6 Removing Employees for Misconduct or Security Reasons

The Government may, at its sole discretion (via the Contracting Officer and/or COR), direct the Contractor to remove any Contractor employee from DHS facilities for misconduct or security reasons. Removal does not relieve the Contractor of the responsibility to continue providing the services required under the contract. The Contracting Officer will provide the Contractor with a written explanation to support any request to remove an employee.

## 4.0 OTHER APPLICABLE CONDITIONS

### 4.0.1 Technical Direction

Performance of work under this contract shall be subject to the technical direction of the COR. The term "Technical Direction" is defined to include, without limitation, the following: (a) Directions to the contractor which redirect the contract effort, shift work emphasis between work

areas of tasks, require pursuit of certain lines of inquiry, fill in details or otherwise serve to accomplish contractual ~~statement of work~~ SOW. (b) Provision of information to the contractor that assists in the interpretation of drawings, specifications, or technical portions of the work description. (c) Review and, where required by the contract, approval of technical reports, drawings, specifications, and technical information to be delivered by the contractor to the Government under the contract. Technical direction must be within the general scope of work stated in the contract. The COR does not have authority to and may not issue any technical direction which (i) constitutes an assignment of additional work outside the general scope of the contract; (ii) constitutes a change as defined in the contract clause entitled "Changes" (FAR 52.243-1); (iii) in any manner cause an increase or decrease in the total contract cost or price, the fixed fee or the time required for contract performance; or (iv) changes any of the expressed terms, conditions, or specifications of the contract. All technical direction shall be issued in writing by the COR or shall be confirmed in writing within five (5) working days after issuance. The contractor shall proceed promptly with the performance of technical directions duly issued by the COR in the manner prescribed by this article. If, in the opinion of the contractor, any instruction or direction issued by the COR is within one of the categories and defined in (i) through (iv) above, the contractor shall not proceed but shall notify the CO in writing within five (5) working days after the receipt of any instruction or direction and shall request the CO to modify the contract accordingly.

Upon receiving such notification from the contractor, the CO shall issue an appropriate contract modification or advise the contractor in writing that, in his/her opinion, the technical direction is within the scope of the contract. The contractor shall thereupon proceed immediately with the direction given. A failure of the parties to agree upon the nature of the instruction or direction or upon the contract action to be taken with respect thereto shall be subject to the provisions of the contract clause titled, "Disputes" (FAR 52.233-1.).

### 4.0.2 Public Health Security and Bioterrorism Preparedness Response Act Requirements

All contractor personnel working under the task order shall be subject to certain sections of the Public Health Security and Bioterrorism Preparedness Response Act of 2002. Specifically, as part of the suitability check process each contractor employee must complete a Federal Bureau of Investigation background check information form (OMB No. 1110-0039). Each contractor employee will be required to complete a training covering his or her responsibilities under the Act.

### 4.0.3 Environment, Safety and Health, and Energy

If the contractor works with hazardous materials the contractor must comply with all applicable regulations as referenced in the sources listed below. GSA defines hazardous materials as: "Hazardous Material is commonly referred to as HAZMAT or Dangerous Goods by industry and the U.S. Government. Occupational Safety & Health Administration (OSHA) in 29 CFR 1910.1200, and GSA in FED-STD-313 define Hazardous Material as:

Any item or chemical which is a "health hazard" or "physical hazard", including the following:

- Chemicals that are carcinogens, toxic or highly toxic agents, reproductive toxins, irritants, corrosives, hepatotoxins, nephrotoxins, neurotoxins, agents that act on the hematopoietic system, and agents that damage the lungs, skin, eyes, or mucous membranes;
- Chemicals that are combustible liquids, compressed gases, explosives, flammable liquids, flammable solids, organic peroxides, oxidizers, pyrophoric, unstable (reactive) or water-reactive; and
- Chemicals that, in the course of normal handling, use or storage, may produce or release dusts, gases, fumes, vapors, mists or smoke having any of the above characteristics.

Any item or chemical which, when being transported or moved, is a risk to public safety or is an environmental hazard, and is regulated as such by one or more of the following:

- DOT-Department of Transportation; Hazardous Materials Regulations (49 CFR 100-180);
- EPA- Environmental Protection Agency (40 CFR);
- IMO-International Maritime Organization; International Maritime Dangerous Goods (IMDG) Code;
- IATA-International Air Transport Association; Dangerous Goods Regulations;
- ICAO-International Civil Aviation Organization; Technical Instructions; and
- AF-Air Force "INTERSERVICE" Manual, Preparing Hazmat for Military Air Shipments (AFMAN 24-204).

HAZMAT also includes any item or chemical which is reportable or potentially reportable or noticeable as inventory under the reporting requirements of the Hazardous Chemical Reporting (40 CFR Part 302), or as an environmental release under the reporting requirements of the Toxic Chemical Release Reporting: Community Right To Know (40 CFR Part 372).

These include chemicals with special characteristics which, in the opinion of the manufacturer, can cause harm to people, plants, or animals when released by spilling, leaking, pumping, pouring, emitting, emptying, discharging, injecting, escaping, leaching, dumping, or disposing of in the environment (including the abandonment or discarding of barrels, containers, and other receptacles). Also, HAZMAT includes an item or chemical if it is a special nuclear source or by-product material as defined in 10 CFR, or is regulated or referred to as radioactive."

Depending on the type of hazardous material, the following FAR clauses will apply:

- 52.223-1 Biobased Product Certification.
- 52.223-2 Affirmative Procurement of Biobased Products Under Service and
- Construction Contracts.
- 52.223-3 Hazardous Material Identification and Material Safety Data.
- 52.223-4 Recovered Material Certification.
- 52.223-5 Pollution Prevention and Right-to-Know Information.
- 52.223-6 Drug-Free Workplace.
- 52.223-7 Notice of Radioactive Materials.
- 52.223-9 Estimate of Percentage of Recovered Material Content for EPA-Designated Items.
- 52.223-10 Waste Reduction Program.
- 52.223-11 Ozone-Depleting Substances and High Global Warming Potential

Hydrofluorocarbons.
- 52.223-12 Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners.
- 52.223-13 Acquisition of EPEAT®–Registered Imaging Equipment.
- 52.223-14 Acquisition of EPEAT®-Registered Televisions.
- 52.223-15 Energy Efficiency in Energy-Consuming Products.
- 52.223-16 Acquisition of EPEAT®-Registered Personal Computer Products.
- 52.223-17 Affirmative Procurement of EPA-designated Items in Service and Construction Contracts.
- 52.223-18 Encouraging Contractor Policies to Ban Text Messaging While Driving.
- 52.223-19 Compliance with Environmental Management Systems.
- 52.223-20 Aerosols.
- 52.223-21 Foams.
- 52.223-22 Public Disclosure of Greenhouse Gas Emissions and Reduction Goals-Representation.

Federal Standard: Material Safety Data, Transportation Data and Disposal Data for Hazardous Materials Furnished to Government Activities (FED-STD-313, latest version).

## 4.1 SECURITY

### 4.1.1 Special Security Requirements

Contractor Pre-screening contractors requiring recurring access to Government facilities or access to sensitive but unclassified (SBU) information and/or logical access to Information Technology (IT) resources shall verify minimal fitness requirements for all persons/candidates designated for employment under any Department of Homeland Security (DHS) contract by prescreening the person/candidate prior to submitting their name for consideration to work on the contract. Pre- screening the candidate ensures that minimum fitness requirements are considered and mitigates the burden of DHS having to conduct background investigations on objectionable candidates. The Contractor shall submit only those candidates that have not had a. felony conviction within the past 36 months, illegal drug use within the past 12 months, or misconduct such as criminal activity on the job relating to fraud or theft within the past 12 months from the date of submission of their name as a candidate to perform work under this contract. Contractors are required to flow this requirement down to subcontractors. Pre-screening involves contractors and subcontractors reviewing. Felony convictions within the past 36 months. An acceptable means of obtaining information on felony convictions is from public records, free of charge, or from the National Crime Information Center (NCIC). Illegal drug use within the past J 2 months. An acceptable means of obtaining information related to drug use is through employee self-certification, by public records check; or if the contractor or subcontractor already has drug testing in place. There is no requirement for contractors and/or subcontractors to initiate a drug testing program if they do not have one already in place.

Misconduct such as criminal activity on the job relating to fraud or theft within the past 12 months. An acceptable means of obtaining information related to misconduct is through employee self- certification, by public records check, or other reference checks conducted in the

normal course of business. Pre-screening shall be conducted within 15 business days after contract award. This requirement shall be placed in all subcontracts if the subcontractor requires routine physical access, access to sensitive but unclassified.

### 4.1.2 Access to DHS Facilities and Resources

DHS may exercise full control over granting, denying, withholding, or terminating unescorted access to DHS facilities, DHS systems, and/or sensitive DHS information for government/contract employees. Access will be based upon the results of a DHS fitness/suitability investigation. DHS may, as appropriate, make favorable entry of duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the government/ contract employee 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 DHS fitness/ suitability authorization will follow. The granting of a favorable EOD decision or a full DHS 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 contract/task order. No employee of the government/contractor shall be allowed unescorted access to a DHS facility, access to any sensitive DHS information, or access to DHS Systems without a favorable EOD decision or DHS fitness/suitability determination by the DHS HQ Office of Security. Government/contract employees assigned to the contract/task order not needing access to sensitive DHS information, DHS systems, or access to DHS facilities will not be subject to DHS fitness/suitability screening. Government/contract employees waiting on an EOD decision may not begin work on the task order. Limited access to DHS facilities is allowable prior to the EOD decision if the government/contract employee is escorted by an approved DHS employee. This limited access is to allow government/contract employees to attend briefings, nonrecurring meetings, and begin transition work. During one's limited access the government/ contract employee will not have access to sensitive or classified DHS 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 government/contract employee 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 government/ contract employee is required to have access to classified information at another Government Facility, it shall abide by the requirements set forth by the agency.

### 4.1.3 Additional Guidance

Contractor access to classified information is not currently required under this SOW.

## 4.2 SAFEGUARDING OF SENSITIVE INFORMATION.

### 4.2.1 Applicability

This clause applies to the Teledyne Scientific & Imaging, LLC 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.

### 4.2.2 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.

### 4.2.3 Authorities

The Contractor shall follow all current versions of Government policies and guidance accessible at https://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 https://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 https://csrc.nist.gov/publications/PubsSPs.html; and
(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at https://csrc.nist.gov/publications/PubsSPs.html.

### 4.2.4 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.

### 4.2.5 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 9.1, July 24, 2012), 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 https://www.dhs.gov/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.

### 4.2.6 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.

### 4.2.7 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 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.

### 4.2.8 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.

### 4.2.9 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.

### 4.2.10 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.

## 4.3 PERIOD OF PERFORMANCE

The period of performance for this contract, as modified, is 45 months from the date of award, expiring 06/30/2026.

## 4.4 PLACE OF PERFORMANCE

The primary place of performance will be the Contractor's facilities with occasional visits to the Department of Homeland Security 301 7th St SW, Washington, DC 20407 facilities.

Location of the Operational Field Assessment (OFA) will be determined during the planning phase of the OFA.

## 4.5 TRAVEL

Contractor travel may be required to support this requirement. All travel required by the Government outside the local commuting area(s) will be reimbursed to the Contractor in accordance with the Federal Travel Regulations. The Contractor shall be responsible for obtaining COR approval (electronic mail is acceptable) for all reimbursable travel in advance of each travel event. The Contractor is not authorized for travel reimbursement unless there is prior COR approval for the travel event and estimated costs.

## 4.6 POST AWARD CONFERENCE

The Contractor shall attend a Post Award Conference with the Contracting Officer and the COR no later than 30 business days after the date of award. The purpose of the Post Award Conference, which will be chaired by the Contracting Officer, is to discuss technical and contracting objectives of this contract and review the Contractor's draft project plan. The Post Award Conference will be held at the Government's facility, located at 301 7th St SW, Washington, DC 20407, or via teleconference.

## 4.7 PROJECT PLAN

The Contractor shall provide a draft Project Plan at the Post Award Conference for Government review and comment. The Contractor shall provide a final Project Plan to the COR not later than 15 business days after the Post Award Conference.

## 4.8 BUSINESS CONTINUITY PLAN

The Contractor shall prepare and submit a Business Continuity Plan (BCP) to the Government. The BCP Plan shall be due 30 business days after the date of award, and will be updated on an annual basis. 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 description of the Contractor's emergency management procedures and policy
- A description of how the Contractor will account for their employees during an emergency
- How the Contractor will communicate with the Government during emergencies
- A list of primary and alternate Contractor points of contact, each with primary and alternate:
  - Telephone numbers
  - E-mail addresses

**4.8.1** Individual BCPs shall be activated immediately after determining that an emergency has occurred, shall be operational within 24 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 Project 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 Project Manager and the COR shall promptly open an effective means of communication and verify:

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

**4.8.2** The Government and Contractor Project Manager shall make use of the resources and tools available to continue contracted functions to the maximum extent possible under emergency circumstances. Contractors shall obtain approval from the Contracting Officer prior to incurring costs over and above those allowed for under the terms of this contract. Regardless of contract type, and of work location, Contractors performing work in support of authorized tasks within the scope of their contract shall charge those hours accurately in accordance with the terms of this contract.

## 4.9 PROGRESS REPORTS

The Contractor shall provide a monthly progress report to the Contracting Officer and COR via electronic mail. 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.

## 4.10 PROGRESS MEETINGS

Contractor shall participate in meetings and discussions with Project representatives and provide documentation or demonstrations sufficient for Project representatives to evaluate the system elements of the Contractor's solution. Documents or demonstrations may include test results, design documentation, and systems analysis.

The Contractor shall meet with the Program Manager and COR on a monthly basis to discuss progress, exchange information and resolve emergent technical problems and issues. These meetings shall take place at Government's facility located at 1120 Vermont Ave NW, Washington, DC, 20005, or 301 7th St SW, Washington, DC 20407, or via teleconference.

## 4.11 GENERAL REPORT REQUIREMENTS

The Contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with DHS workstations (Windows XP and Microsoft Office Applications).

## 4.12 PROTECTION OF INFORMATION

Contractor access to information protected under the Privacy Act is required under this SOW.

Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with the law and Government policy and regulation.

Contractor will have access to PII (a category of controlled unclassified information) in the form of business contact information for the purpose of supporting the OFA that will be conducted in connection with this project. Contractor will not have access to DHS information systems nor recurring access to government facilities. Contractor will not be required to retain CUI on behalf of the government.

The following Homeland Security Acquisition Regulation (HSAR) Class Deviation 15-01 apply to this contract:

- HSAR 3052.204-70, Security Requirements for Unclassified Information Technology Resources (JUN 2006);
- Safeguarding of Sensitive Information (MAR 2015); and
- Information Technology Security and Privacy Training (MAR 2015).

## 4.13 RESERVED

Note: In the previous version of this SOW, there was no section 4.13. For the sake of continuity of numbering, 4.13 is now labeled "Reserved" as a placeholder.

## 4.14 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 https://www.section508.gov.

### 1. Section 508 Requirements

Section 508 of the Rehabilitation Act (classified to 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Appendixes A, C & D, and available at:

https://www.ecfr.gov/cgi-bin/textidx?SID=e1c6735e25593339a9db63534259d8ec&mc=true&node=pt36.3.1194&rgn=div5 .

In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards. ICT includes IT and other equipment.

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated November 12, 2018 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated November 20, 2018, or any successor publication.

1.1 Section 508 Requirements for Technology Products (include in the SOW, PWS, or SOO) Section 508 applicability to Information and Communications Technology (ICT): Laser Detection Equipment

Applicable Exception: N/A.

Authorization #: N/A Applicable Functional Performance Criteria: Does not apply.

Applicable 508 requirements for electronic content features and components (including but not limited to Electronic emergency notifications): All requirements in E205 apply, including all WCAG 2.0 Level A and AA Success Criteria apply as specified in E205, except 2.4.1 Bypass Blocks, 2.4.5 Multiple Ways, 3.2.3 Consistent Navigation, and 3.2.4 Consistent Identification.

Applicable 508 requirements for software features and components: Does not apply.

Applicable 508 requirements for hardware features and components: Does not apply.

Applicable 508 requirements for support services and documentation: All requirements in Chapter 6 apply.

1.2 Section 508 Deliverables

Section 508 Accessibility Conformance Reports: For each ICT item offered through this contract (including commercially available products, and solutions consisting of ICT that are developed or modified pursuant to this contract), the Offeror shall provide an Accessibility Conformance Report (ACR) to document conformance claims against the applicable Section 508 standards. The ACR shall be based on the Voluntary Product Accessibility Template Version 2.0 508 (or successor versions). The template can be found at https://www.itic.org/policy/accessibility/vpat. Each ACR shall be completed by following all of the instructions provided in the template, including an explanation of the validation method used as a basis for the conformance claims in the report.

## 5.0 GOVERNMENT TERMS & DEFINITIONS

5.1 CO - -Contracting Officer
5.2 COR - Contracting Officer's Representative
5.3 DHS - Department of Homeland Security
5.4 S&T - Science & Technology
5.5 PM - Program Manager
5.6 PI - Principal Investigator
5.7 OFA - Operational Field Assessment
5.8 ACA - After Contract Award
5.9 ICT - Information and Communications Technology

## 6.0 PROPERTY

## 6.1 PROPERTY DEFINITIONS

**6.1.1** Accountable Personal Property. An asset that meets one or more of the following criteria:

a. Has an expected useful life of 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.

Current accountable personal property information may be obtained through the Personal Property Management Office at ST_Personal_Property@hq.dhs.gov or through the applicable Office Accountable Property Officer (APO).

**6.1.2** Capitalized Personal Property: Non-expendable personal property with an acquisition cost over an established threshold and a normal life expectancy of two years or more. Capitalization Threshold information may be obtained through the Personal Property Management Office at ST_Personal_Property@hq.dhs.gov or through the applicable Office Accountable Property Officer (APO).

**6.1.3** Consumable Assets: 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.

**6.1.4** Contract Property: 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.

**6.1.5** Leased Property: 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).

**6.1.6** Sensitive Asset: 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. 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 Personal Property Management Office at ST_Personal_Property@hq.dhs.gov or through the applicable Office Accountable Property Officer (APO) , Program Manager (PM), or Contracting Officer (CO).

## 6.2 PROPERTY ACCOUNTABILITY

**6.2.1** When contractors are furnished with GFP, DHS barcodes will not be removed. In all GFP cases, the Government retains title to the property.

**6.2.2** 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.

**6.2.3** 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.

## 6.3 PHYSICAL INVENTORY

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

**6.3.1** The Contractor, jointly with the Personal Property Management Office at ST_Personal_Property@hq.dhs.gov or through the applicable Office Accountable Property Officer (APO) on a quarterly basis, shall perform, record, and disclose physical inventory results of CAP and GFP.

**6.3.2** 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 Personal Property Management Office at ST_Personal_Property@hq.dhs.gov or through the applicable Office Accountable Property Officer (APO) 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.

**6.3.3** As requested, inventory results will be completed, certified, and submitted in the timeframe defined at the time of the request, to the Personal Property Management Office at ST_Personal_Property@hq.dhs.gov or through the applicable Office Accountable Property Officer (APO) 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.

## 6.4 PROPERTY DISPOSAL

**6.4.1** 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 Personal Property Management Office at ST_Personal_Property@hq.dhs.gov or through the applicable Office Accountable Property Officer (APO) for all excess property prior to taking any action.

**6.4.2** 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.

## 6.5 LOST, STOLEN, DAMAGED OR DESTROYED (LDD) PROPERTY

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

**6.5.1** 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.

**6.5.2** 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 Personal Property Management Office at ST_Personal_Property@hq.dhs.gov or through the applicable Office Accountable Property Officer (APO).

**6.5.3** 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.

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

**6.5.5** The COR must submit the completed package to the Personal Property Management Office at ST_Personal_Property@hq.dhs.gov or through the applicable Office Accountable Property Officer (APO) within 5 business days of receipt from the Contractor.

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

## 6.6 GOVERNMENT FURNISHED RESOURCES

The Government will not furnish any resources to the Contractor in support of this contract.

## 7.0 CONTRACTOR FURNISHED PROPERTY

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 SOW 2.0 and SOW 6.0.

## 8.0 GOVERNMENT ACCEPTANCE PERIOD

The COR will review deliverables prior to acceptance and provide the contractor with an e-mail that provides documented reasons for non-acceptance. If the deliverable is acceptable, the COR will send an e-mail to the Contractor notifying it that the deliverable has been accepted.

**8.1** The COR will have 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.

**8.2** The COR will have 7 business days to review deliverables and make comments. The Contractor shall have 7 business days to make corrections and redeliver.

**8.3** All other review times and schedules for deliverables shall be agreed upon by the parties based on the final approved 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.

**END OF SOW UPDATED FOR MODIFICATION P00008**