PART B: Interagency Agreement (IA) Between DHS Science and Technology Directorate (S&T) and the United States Air Force, IAA# HSHQPM-16-X-00174/P00001, Under the Economy Act

Statement of Work (SOW)

**MIT/LL Project Number: 10302**

**I. Introduction**

**1. Purpose**

This Statement of Work (SOW) provides specific information regarding the requirements of the Department of Homeland Security, Science and Technology Directorate, Requesting Agency, hereinafter referred to as DHS S&T, sufficient to enable the U.S. Air Force-Massachusetts Institute of Technology/Lincoln Laboratory (AF-MIT/LL), Servicing Agency, hereinafter referred to as the AF-MIT/LL, to perform services under an interagency agreement.

**2. Authority**

DHS’s authority to enter into this IA is 31 U.S.C. 1535-1536 as implemented in subpart 17.5 of the Federal Acquisition Regulations (FAR).

**3. General Terms & Conditions**

Activities undertaken pursuant to this document are subject to the general Terms and Conditions hereby attached between the DHS S&T and the AF-MIT/LL.

**4. Project Title**

“Aviation Security Technology and Methods”, on behalf of the DHS S&T Homeland Security Advanced Research Projects Agency, Explosives Division, as part of the Apex Screening at Speed (SaS) program***.***

**5. Description of Products or Services / Bona Fide Need**

DHS S&T has a need for the AF-MIT/LL to provide research and development services for the Apex Screening at Speed (SaS) program, described in Section II. The AF-MIT/LL, in its capacity as a Department of Defense Federally Funded Research and Development Center, possesses the expertise and the professional scientific resources to perform key research and development activities in support of Apex SaS, as outlined in Section III. The AF-MIT/LL has substantial experience working with technologies relevant to today’s aviation security challenges. In particular, AF-MIT/LL has performed previous research on RF antenna array sensor design employing millimeter wavelengths, chemical trace vapor sensing, automatic image and video processing algorithms, biometrics, data fusion and risk assessment methods, and human-in-the-loop testing of security technologies.

The purpose of this action is to establish a new interagency agreement (IAA) with the AF-MIT/LL for the tasking described in Section III of this Statement of Work (SOW). Massachusetts Institute of Technology/Lincoln Laboratory is a Federally Funded Research and Development Center (FFRDC) under Air Force (AF) Prime Contract No. FA8702-15-D-0001. The AF contract is the vehicle by which sponsors fund R&D at MIT LL and is managed by the Enterprise Acquisition Division ESC/CAA, at Hanscom Air Force Base.

Work performed under this SOW should be considered severable.

II. Background

Protecting aviation facilities and aircraft against malicious attacks and other criminal activity, while ensuring high-throughput passenger access to such facilities, is a challenging problem for both the Transportation Security Administration (TSA) and airport security personnel. One challenge is the complexity of the threat space, which includes explosives, weaponry, and other safety related items, and which may be concealed in checked luggage, carry-on items, or underneath clothing. Another challenge is the (currently) limited opportunities to collect observations relating to potential threats, primarily at staff-constrained TSA checkpoints. Finally, any new screening capabilities designed to enhance threat detection must be conducted without introducing additional latencies in the screening process, in order to minimize wait times.

DHS S&T initiated the Apex SaS program to address current and future challenges to aviation security. The Apex SaS Program is pursuing transformative R&D activities that support a future vision for increasing security effectiveness while dramatically reducing wait times and improving the passenger experience. Innovative solutions will be developed to support a curb-to-gate screening architecture, and may include investment in areas such as identity verification, risk-based methodologies, training and human performance, surveillance and video analytics, and improved screening systems for passengers and carry-on baggage.

By design, the Apex SaS program will:

* Develop technologies for both primary and secondary screening of people and carry-on baggage
* Invest in innovative technology exploration with the goal to inspire industry to develop new approaches to the screening process and reduce the per-unit cost to TSA
* Continuously look for new approaches and technologies through market research, collaboration with other Government agencies, and alternative R&D processes

The end goal of Apex SaS is the development of solutions that detect threats at a significantly reduced threat mass, while screening 300+ people and their carry-on items per hour with minimal or very limited divestiture. It will strive to eliminate current restrictions on liquids, aerosols, and gels (LAG) and allow passengers to keep personal electronics in carry-on bags, significantly improving the passenger experience.

To successfully achieve this end state, Apex SaS will pursue the following objectives:

* More accurate threat detection, especially at small volumes or in non-traditional forms
* Faster passenger or bag screening processes with less restrictive divestiture requirements
* Extension of threat detection beyond the checkpoint, to potentially include sensor cues collected within the unsecured (pre-checkpoint) and secured (post-checkpoint) areas of aviation facilities
* More comprehensive assessment of potential threats via combinations of threat cues from multiple sensors or data sources
* Adaptation of screening technologies to emerging or site-specific threat concerns

The purpose of this action is to amend this IA with the AF-MIT/LL to add and fund subtasks 1.3, 1.4, 2.3 and 2.4 and extend the period of performance end date to March 31, 2019. This will increase the total estimated cost from $2,365,750 to $4,806,441.89.

**III. Scope**

**Task 1: Improved Walk-By Threat Detection Accuracy**

Rapid near-range standoff active millimeter wave (MMW) scanners have the potential to capture high frame rate images of threat materials underneath passenger clothing or within carried bags, and are therefore relevant for walk-by/walk-through (or “screening at speed”) checkpoint concepts. For instance, AF-MIT/LL is developing a novel MMW scanner that can produce such imagery for subjects in motion at a range of a few meters at 5 – 10 frames per second. However, the likelihood of capturing useful observations in any single scan depends upon the view angle, the relative position of the threat material, and occlusion or clutter effects from the sensed environment. This task focuses on high-level data fusion methods from multiple looks that can achieve better detection accuracy than single scans, and can determine when enough data has been collected to “clear” a passenger with sufficient confidence during a walk-by action.

**Subtask 1.1: Multi-Look MMW/Optical Data Fusion Analysis**

AF-MIT/LL will develop and test an algorithm for processing joint imagery from active/passive MMW scanners and co-located video or RGBD sensing. The input to the algorithm will be a series of MMW scans over time and potentially from multiple sensors positioned to get different view angles of the subject, along with co-located optical sensing. The data fusion framework will consist of the following steps:

* Postulate a collection of person-borne threat hypotheses to be ruled out, such as “large mass of dielectric material on left leg” or “anomalous mass of metal on mid-section”;
* Parse each MMW scan and corresponding optical imagery to estimate subject pose, and therefore subject components to which the scanner has an unobstructed view;
* Analyze each MMW scan to attach feature-level evidence to each threat hypothesis based on view;
* Assess likelihood for each threat hypothesis based on aggregated evidence from all inputs;
* Determine that a passenger is “cleared” if the likelihood of all threat hypotheses based on cumulative evidence falls below some established threshold.

The third step (extraction of single-image features) will leverage existing funded work to recognize threat cues within individual MMW images.

The result of this task will be an initial implementation of the multi-look MMW/optical fusion algorithm, with some performance metrics based on laboratory-collected imagery or high-fidelity simulation data. AF-MIT/LL will make use of a combination of COTS sensors (e.g., Kinect) and custom sensors (e.g., AF-MIT/LL MMW scanner test components) to collect the test data to the extent possible. This task will also assess the effectiveness of directed passenger actions (e.g., turning or slowing down) during walk-by/walk-though.

**Subtask 1.2: Technology Maturation Plan and Analysis**

AF-MIT/LL shall develop a technology plan based on the Data Fusion Analysis. This plan shall include alternative technical approaches, development challenges, commercialization considerations, expected developmental milestones and maturation plan. This task will result in a report summarizing the technology maturation plan and analysis.

**Subtask 1.3: Real-time Processing Feasibility Assessment**

Of critical importance to a high-throughput walk-by passenger screening technology is the ability to process data and detect threats in real time, so that a nearly instantaneous recommendation can be made regarding the need for secondary screening. This is critical for achieving the throughput benefits of a screening-at-speed system. For this task, AF-MIT/LL will perform an analysis to understand and demonstrate the feasibility of real-time multi-look fusion, based on the most promising fusion algorithms identified during the initial development phase.

The fusion framework will be characterized in terms of computational complexity (operations per second, memory needed) and throughput (e.g., frames per second or people per hour) in order to identify hardware and software requirements necessary for real-time processing. For instance, it is likely that high performance hardware such as COTS GPUs will be necessary to handle the computational loads. Optimization techniques such as subsampling in time or space, or making changes to the underlying fusion algorithm will be explored as well. To the extent possible, prototype code will be converted to operational code to support a limited, in-lab demonstration of real-time threat detection from multiple look angles.

**Subtask 1.4: Expanded Image Collection and Performance Analysis**

This task will expand upon the algorithm development in Subtask 1.1 to enhance the data fusion framework with respect to new sensor data types, threat variations, and environmental conditions (e.g., divestiture, pose).

New experiments will be designed to explore the following:

* Robustness to new sensor configurations or sensor types. This may require the acquisition of data from collaborating partners (e.g., PNNL, TSA/TSL) in addition to data collected using AF-MIT/LL technology.
* Multi-view detection performance over a variety of threat types, sizes and placements on the body.
* Effect of level of divestiture (e.g., coats, belts, wallets, phones) on multi-view detection and fusion performance.
* Effect of directed passenger actions (position, pose, walking speed) on multi-view detection and fusion performance.

In addition to test imagery, high-fidelity simulations may be used to support the analysis. The result of this task will be a performance evaluation of the multi-look fusion algorithm under an expanded set of conditions, with recommendations regarding sensor placement/combinations, directed passenger actions, and required levels of divestiture.

**Task 2: Passenger Tracking and Identity Verification**

A “curb-to-gate” aviation security approach is advantageous because it uses observations collected during passenger traversal through the airport (not just at the checkpoint) to make a more comprehensive assessment of potential risk level. Such an approach may also consider historical travel patterns of a passenger as useful contextual information. However, this type of security approach does require a mechanism for correlating spatially and temporally distributed observations about the same passenger. This task examines techniques that may be applied to make these associations more accurately.

**Subtask 2.1: Passenger Tracking / Re-Identification**

AF-MIT/LL will investigate candidate sensor deployments and data processing methods to automatically track the progression of each passenger through an airport facility. It is assumed that the data used to perform the tracking would be derived from a combination of general video surveillance infrastructure and specialized camera placements at key locations such as terminal entrances and checkpoints. The data processing algorithm will place an emphasis on accurate person re-identification (i.e., matching across camera views), with short-term tracking methods used to fill in the gaps. MIT LL will leverage its expertise in multi-camera path reconstruction from previous DHS-funded work, but with the new objective of achieving more automated forms of appearance-based person re-identification.

AF-MIT/LL will run experiments on offline video data to assess the feasibility of automatic passenger tracking using emerging computer vision techniques such as deep convolutional neural networks to achieve better accuracy. The data needed to perform such experiments is already available at AF-MIT/LL, which has access to sample video from distributed camera systems at airports and other large transportation facilities. This analysis may also consider the use of reference imagery of a passenger collected at multiple view angles in order to develop a high-fidelity model of appearance that can be used during the re-identification process. The use of specialized reference imagery would require either data collection at AF-MIT/LL or the deployment of new camera systems at a test site. AF-MIT/LL will also assess the computational load of applying these techniques in a few possible deployment scenarios (e.g., attempt to track every passenger, focus processing only on passengers with some initial indication of risk, etc).

**Subtask 2.2: Passenger Identity Verification and Baggage Correlation**

Current airport screening protocols rely on identification cards such as driver’s licenses to perform identity verification at TSA checkpoints. In the future, ensuring identity could be even more important if a substantial fraction of the flying public goes through an expedited screening protocol based on information (e.g., travel patterns) associated with passenger identity. In addition, more adaptive security protocols, in which checked or carry-on baggage screening protocols are closely linked to passenger risk, would require mechanisms for high-confidence association between passengers and their bags.

In this task, AF-MIT/LL will conduct a study of existing and feasible near-term identity verification and correlation methods in order to assess advantages and projected vulnerabilities with respect to potential “screening at speed” checkpoint protocols. Components that will be considered include credential authentication technologies, standoff biometrics, scan-able unique identifiers, and the underlying software architecture and databases required to manage identity-related information. AF-MIT/LL will perform limited implementation to support the analysis; for instance, evaluation of low-fidelity face matching to verify identity across multiple passenger visits to the same airport may require some testing with actual face images extracted from surveillance video at a range of resolutions. The output of this task will be a set of recommendations for the use of identity verification and correlation mechanisms, and an identification of near-term development efforts required to fill capability gaps.

**Subtask 2.3: Passenger Tracking Limited Pilot Demonstration**

AF-MIT/LL will develop a limited system-level prototype for multi-camera passenger tracking based on the findings from the initial technology assessment in Subtask 2.1. The goal of the prototype will be to provide a new level of automation for airport operators to track passengers from curb-to-gate via automated analysis of surveillance videos. The initial design will be based on the outcome of the sensor placement and system architecture analysis for tracking and re-identification, as well as performance testing of various algorithms for passenger tracking against pre-recorded data from Logan airport and other relevant data sources.

Once implemented, the prototype will be deployed to an airport test site for demonstration on operational video feeds. The test site partner will be jointly selected with DHS S&T after consideration of the relative advantages of different sites (such as video infrastructure) and is likely to include consideration of Logan Airport in Boston, among other options. Although AF-MIT/LL will design the system to scale with the number of cameras involved, this prototype will be limited in terms of its hardware footprint and in the number of cameras with which it will integrate. Subsequent scaling (in future phases) of the limited system to work with more cameras will incur less risks after the technology has been proven in an operational environment of the partner airport.

The system-level prototype will be an end-to-end system that integrates natively with the video manager system (VMS) at the partner facility. It will include backend video data processing software and hardware, as well as desktop client applications. AF-MIT/LL will work with the airport partner to understand their specific needs and operational requirements to come up with the final software design, especially the client user interface (UI) component. Based on trade-off analysis of performance vs. speed, specific algorithms will be adapted or implemented, and optimized to meet the real-time operational requirements. AF-MIT/LL may leverage software initially developed for other DHS programs if appropriate in order to reduce overall development cost within the proposed timeline.

**Subtask 2.4: Passenger Identity Verification Experimental Validation**

The Passenger Identity Verification analysis subtask (2.2) is focused in part on developing promising concepts to enhance the traditional identity verification process at aviation security checkpoints. The initial analysis has identified four key “threat vectors” to be addressed: falsified credentials, borrowed credentials, credentials obtained with stolen identity, and credentials obtained with synthetic identity. Existing technologies that are close to adoption at checkpoints (e.g., Credential Authentication Technologies (CAT)) provide a useful countermeasure for some but not all of these threat vectors (e.g., falsified credentials), but not all of them. Therefore, subtask 2.2 addresses a broader set of supplemental countermeasures, including opportunistic biometric checks and outside database checks.

The analysis efforts have included development of a general simulation framework that relates assumed threats and technology capabilities to overall performance statistics characterizing detection probability and average latency. A central concept being explored is the combination of component checks into a unified “risk score” based on the available information such as CAT results, algorithmic results comparing biometric images, and selective database checks.

This subtask is directed at the next step in development and demonstration: a more direct experimental validation of some of the most promising countermeasures identified in the initial analysis. Although the exact scope and the technology/methods to be explored will be determined based on the initial study results, it is clear that additional investigation in several general areas will be valuable. In particular, this subtask will include the following activities:

* Collection of critical performance data from operational entities. AF-MIT/LL will work with TSIF, TSL, or the TSA Innovation Task force to collect more accurate statistics of threat presentations and operational performance of component technologies, for the purpose of refining simulation models. This may involve working with partner entities on a protocol for acquiring this information (e.g., analysis of existing records, or collection of new data over time). Emphasis will be placed on data relating to the most critical components identified by the initial evaluation phase.
* Selected novel methods or combinations of technology components will be prototyped and tested in a laboratory setting for practicality and to collect basic statistics on performance. For example, facial recognition algorithms could be selected, adapted to the problem of comparing a checkpoint image to a record image and/or opportunistic surveillance images, and used to test the approach and collect basic performance statistics.

**Task 3: Adaptive Threat Detection**

The goal of automatic threat detection algorithms, whether applied to optical, MMW, or X-ray imagery, is to maximize discrimination between actual threats and nuisance or clutter objects. However, accurate discrimination can be difficult to achieve, especially when (1) new threat types emerge as security concerns or (2) the detection algorithm encounters new clutter sources that were not anticipated during algorithm design or training. This task will focus on adaptive threat detection algorithms to address these problems.

**Subtask 3.1: Offline Prototype Development and Testing**

AF-MIT/LL will prototype a feedback-adaptive framework for threat detection, which uses aggregated binary feedback from users to suppress false positives while maintaining probability of detection. This prototype will leverage pre-existing project work at AF-MIT/LL (referred to as “Customizable Pattern Analytics”) that re-engineers both the derived features and the classifier that underlies the detection process to optimize performance in the operational environment. It may also be possible to update the threat detection algorithm based on evolving threat concerns, if exemplars of the new threat are collected and merged with the site-specific feedback. The algorithm will be evaluated using either laboratory-collected or vendor-provided imagery combined with annotations that emulate the process of feedback over time. The scope of available imagery will depend upon which imaging modalities are selected for experimentation (e.g., a study on MMW imagery would depend on internal collection efforts, but a study on X-ray imagery might require collaboration with vendors and/or the Transportation Security Laboratory).

IV. Key Milestones and Deliverables

*Table 1*

| **Task/Subtask Number and Name**  **(F) Funded**  **(P) Partially Funded**  **(U) Unfunded** | **Milestones / Deliverables** | **Due Date or Completion Date** | **Budget** |
| --- | --- | --- | --- |
| **Aviation Security Technology and Methods** | | | |
| **Task 1: Improved Walk-By Threat Detection Accuracy** | | | |
| Subtask 1.1: Multi-Look MMW/Optical Data Fusion Analysis (F) | * Status update briefing on walk-by imaging algorithm development (F) | 31 Mar 2017 | $750,000 |
| * Walk-by image processing test results (F) | 31 Dec 2017 |
| Subtask 1.2: Technology Maturation Plan (F) | * Maturation Plan and Analysis Report and briefing | 30 June 2018 |
| Subtask 1.3: Real-time Processing Feasibility Assessment (F) | * Real-time fusion algorithm implementation and assessment | 30 Sep 2018 | $450,000 |
| Subtask 1.4: Expanded Image Collection and Performance Analysis (F) | * Expanded test results and recommendations for multi-view screening protocols | 31 Dec 2018 | $375,000 |
| **Task 2: Passenger Tracking and Identity Verification** | | | |
| Subtask 2.1: Passenger Tracking and Re-Identification (F) | * Sensor placement and system architecture analysis for tracking and re-identification | 31 Mar 2017 | $700,000 |
| * Performance testing of passenger tracking against offline data set | 30 Sep 2017 |
| Subtask 2.2: Passenger Identity Verification and Baggage Correlation (F) | * Feasibility study of passenger identity correlation | 30 Sep 2017 | $365,000 |
| Subtask 2.3: Passenger Tracking Limited Pilot Demonstration (F) | * Demonstration of initial pilot system at test site | 31 Dec 2018 | $1,205,391.89 |
| * Assessment of operator feedback and plan for further development | 31 Mar 2019 |
| Subtask 2.4: Passenger Identity Verification Experimental Validation (F) | * Validation of promising novel identity verification concepts using experimental data | 31 Dec 2018 | $410,000 |
| **Task 3: Adaptive Threat Detection** | | | |
| Subtask 3.1: Offline Prototype Development and Testing (F) | * Performance testing of adaptive threat detection algorithms | 30 June 2017 | $550,000 |

1. Project Timeline

Table 2

|  | **Indicate Month Deliverable is due after Award or Services are to be completed** | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 3 | 6 | 9 | 12 | 15 | 18 | 21 | 24 | 27 | 30 | 33 | 36 |
| **Task 1: Improved Walk-By Threat Detection Accuracy** |  |  |  |  |  | X |  |  |  |  |  |  |
| Status update briefing on walk-by imaging algorithm development |  |  | X |  |  |  |  |  |  |  |  | X |
| Walk-by image processing test results |  |  |  |  |  | X |  |  |  |  |  |  |
| Technology Maturation Report |  |  |  |  |  |  |  | X |  |  |  |  |
| Real-time Fusion Algorithm Assessment |  |  |  |  |  |  |  |  | X |  |  |  |
| Image Collection and Performance Analysis Test Results |  |  |  |  |  |  |  |  |  | X |  |  |
| **Task 2: Passenger Tracking and Identity Verification** |  |  |  |  | X |  |  |  |  |  |  | X |
| Sensor placement and system architecture analysis for tracking and re-identification |  |  | X |  |  |  |  |  |  |  |  |  |
| Performance testing of passenger tracking against offline data set |  |  |  |  | X |  |  |  |  |  |  |  |
| Feasibility study of passenger identity correlation |  |  |  |  | X |  |  |  |  |  |  |  |
| Passenger tracking demonstration |  |  |  |  |  |  |  |  |  | X |  |  |
| Passenger tracking demonstration operator feedback |  |  |  |  |  |  |  |  |  |  | X |  |
| Passenger identity verification and validation report |  |  |  |  |  |  |  |  |  | X |  |  |
| **Task 3: Adaptive Threat Detection** |  |  |  | X |  |  |  |  |  |  |  |  |
| Performance testing of adaptive threat detection algorithms |  |  |  | X |  |  |  |  |  |  |  |  |

1. Other IA Details
2. Period of Performance. The period of performance (POP) for this SOW is from the effective date of the IA through 31 March 2019.
3. Travel. Travel will be required in the performance of the duties listed herein. If travel is required, it is anticipated that travel will be limited to CONUS.
4. **DHS-Furnished** **Information and Property** DHS furnished property, if any, shall be provided in a numbered attachment to this SOW and listed in Section VII, Applicable Documents.
5. Upon completion of this IAA, the property will be disposed of consistent with the guidance provided by, or advice of, the DHS Contracting Officer.
6. **Place(s) of Performance**. The AF-MIT/LL will perform the work under this SOW at Massachusetts Institute of Technology Lincoln Laboratory (MIT/LL) and at other sites as determined by the DHS S&T Technical Representative.
7. **Program Status Report.** The AF-MIT/LL will provide program status reports to the DHS consistent with direction provided in the SOW within 15 days of the end of each month. Reports should be provided to the DHS S&T Technical Representative, and contain metrics pertaining to financial, schedule, and performance information, risk information, a summary of expected deliverables and milestones for the effort, and an assessment of performance of all work performed under the IA.
8. **Deliverables**. The AF-MIT/LL will provide all deliverables identified in this SOW, in accordance with Section IV of this SOW, to the DHS S&T Technical Representative.
9. **Invoices.** The AF-MIT/LL *w*ill deliver a monthly invoice to ST.Invoicing@hq.dhs.gov by the 15th day of each month.
10. **Security** **Requirements**. All work performed under this SOW is unclassified unless otherwise noted below:

If provided DHS “sensitive” information (e.g., items marked with FOUO or other appropriate marking), the Servicing Agency agrees it shall safeguard such information by not providing access of this marked information to any non-federal personnel unless advance approval is obtained from the DHS/S&T Technical Representative.  In turn, the DHS/S&T Technical Representative must ensure any applicable DHS security and/or suitability requirements are satisfied by its servicing DHS Security office and that a DHS NDA Form 11000-6s are signed by the non-federal personnel before access to DHS “sensitive” information is given to them.  The DHS/S&T Technical Representative must further obtain copies of the executed, signed DHS Form 11000-6s, to be provided to the DHS Contracting Officer (for inclusion in the official DHS/OPO inter-agency agreement file).

AF-MIT/LL will potentially need access to Secret information. This information will be related to threat detection requirements and threat information. DHS will provide this information to AF MIT/LL for their use and storage for the duration of the project. Upon completion of the project, all classified materials will be returned or destroyed.

1. **Funding Requirements**. DHS will provide funding to the AF-MIT/LL in accordance with DHS’s appropriations and available funds.
2. Points of Contact

The AF-MIT/LL Points of Contact (POCs) are as follows:

* **Contractual POC**

Gary Tutungian

Administrative Contracting Officer

ESC/PKE, Enterprise Acquisition Division

Phone: 781-981-2331

Email: [tutungian@ll.mit.edu](mailto:tutungian@ll.mit.edu)

* **Financial POC**

Patrick Hanley

Air Force Life-Cycle Management Center (AFLCMC/PZE)

20 Schilling Circle, Bldg. 1305, 3rd Floor

Hanscom Air Force Base, MA 01731

E-mail: [AFLCMC.PZE.MIT.LL@hanscom.af.mil](mailto:AFLCMC.PZE.MIT.LL@hanscom.af.mil)

Fax: (781) 225- 2141

Phone: (781) 225-1248 or email; [Patrick.Hanley.ctr@hanscom.af.mil](mailto:Patrick.Hanley.ctr@hanscom.af.mil)

* **Technical POC(s):**

Dr. Tim Dasey

244 Wood Street

Lexington, MA, 02420

Phone: 781-981-7451

Email: [timd@ll.mit.edu](mailto:timd@ll.mit.edu)

Dr. Jason Thornton  
244 Wood Street

Lexington, MA 02420  
781-981-5784  
Email: [jason.thornton@ll.mit.edu](mailto:jason.thornton@ll.mit.edu)

* **Laboratory Financial POC(s):**

Kim Saxonis

244 Wood St

Lexington, MA 02420-9108

Phone: 781-981-5891

Email: [kim.saxonis@ll.mit.edu](mailto:kim.saxonis@ll.mit.edu)

The DHS POCs are as follows:

* **DHS S&T Technical POC:**

Dr. John Fortune

Department of Homeland Security

245 Murray Lane

Washington, DC 20528

Email: john.fortune@dhs.gov

Tel: (202) 254-6622

* **DHS S&T Financial Analyst**

Mingming Yu

Financial Analyst

Department of Homeland Security

Science and Technology Directorate/Finance & Budget Division (FBD)

S&T SPB MS#0214

245 Murray Lane

Washington, DC 20528-0214

[Mingming.Yu@hq.dhs.gov](mailto:Mingming.Yu@hq.dhs.gov)

202-254-5309

* **DHS S&T Invoicing**

Attn: S&T Invoice

Dallas Payment Center Address:

1605 LBJ FWY

Suite 300

Farmers Branch, TX  75234

[ST.Invoicing@hq.dhs.gov](mailto:ST.Invoicing@hq.dhs.gov)

1. **Applicable Documents**

Part A of this Interagency Agreement (General Terms and Conditions) is incorporated by reference into this Statement of Work.

1. **Changes to this SOW**

Changes to this SOW shall be made in accordance with the section of the General Terms and Conditions of this IA entitled “Amendments”.