

**Broad Agency Announcement (BAA)**  
**Call Solicitation 70RSAT20RB0000003**  
**Call under BAA HSHQDC-16-R-B0004**  
**Project: Advanced Checked Baggage Screening Systems**

## **1. Introduction**

- 1.1.** This BAA Call solicitation (70RSAT20RB0000003) is a Call issued against the Department of Homeland Security (DHS), Science & Technology Directorate (S&T), 5-Year Broad Agency Announcement (BAA), HSHQDC-16-R-B0004 “Apex Screening at Speed Program (Apex SaS).” All terms and conditions of the DHS S&T BAA HSHQDC-16-R-B0004 apply to this solicitation unless otherwise noted herein.
- 1.2.** The potential use of improvised explosive threats with homemade explosives (HME) by terrorists poses many challenges to the Transportation Security Administration (TSA) in conducting aviation security passenger screening. This problem is made increasingly difficult by the considerable complexity of contemporary items and materials found in checked and carry-on baggage screened at major airports in the United States. Maintaining a high threat detection posture in this operating environment can require screening operations to tolerate significant incidence of false alarms. Substantial Transportation Security Officer (TSO) resources must be used to adjudicate the false alarms in order to maintain normal checked baggage screening operations.
- 1.3.** The screening of passenger baggage using traditional Explosives Detection Systems (EDS) for checked baggage and advanced technology (AT) X-ray systems for carry-on baggage has faced many challenges in developing a broadly applicable detection capability for explosive threats that addresses commercial, military and HME explosives threats. Established primary checked and carry-on baggage explosives detection technologies evolved from medical X-ray systems. These conventional transmission X-ray methods utilize two derived discriminating signatures: effective atomic number and density of screened objects. These discriminators perform well for identifying materials where variations in the chemical composition are minimal, such as commercial and military explosives. HMEs are usually formulated using numerous household ingredients; lacking tight quality control in their preparation, and they have high variations in their chemical composition. The detection of HMEs using these two discriminators requires expansion of the system detection windows, which can result in ambiguities with many common stream-of-commerce items (other items that may be found in checked and carry-on baggage). This leads to significantly higher primary screening false alarm rates generating a greater demand for TSO secondary screening to resolve false alarms. The net effect is increased TSO manpower requirements and reduced screening throughput, which results in higher screening costs to TSA and significant passenger inconvenience due to long screening delays.
- 1.4.** Improvements to current checked and carry-on baggage screening system operating characteristics are needed that will provide an acceptable level of detection on all threats but also significantly reduce primary screening false alarms and improve overall

screening throughput. Enhancing the ability to reduce/resolve aviation security screening alarms is identified in the TSA Strategy Plan (2018-2026) and by the Aviation Security Integrated Product Team as a priority capability gap. The TSA's Electronic Baggage Screening Program has established an operational performance objective to require checked baggage primary automated screening performance to demonstrate a net false alarm rate of less than 10%. In addition, the TSA's Passenger Screening Program (PSP) has identified the need for increasing checkpoint passenger screening throughput with the goal of 300 passengers per lane per hour. This will require primary checkpoint baggage screening systems to screen carry-on baggage in a similar manner as checked baggage, maintaining the checkpoint level of security without the need for divestiture, in order to increase passenger throughput at the checkpoint.

- 1.5.** DHS S&T has a need to identify advanced technologies that could increase the measurement or mathematical discrimination between HMEs and stream-of-commerce clutter in checked baggage and carry-on items. Previous research and development (R&D) investments (such as Explosives Division (EXD) BAA13-05 "Advanced X-ray Material Discrimination") initiated efforts to explore additional signature methodologies to discriminate between HMEs and stream-of-commerce clutter, improve screening system detection capability, and reduce false alarm rates. In these R&D acquisition efforts, S&T made investments to prove the feasibility and effectiveness of many discriminating x-ray signature approaches within the context of the TSA Concepts of Operations (CONOPS) through development and testing of robust test bed hardware and software prototypes.

This R&D Acquisition will continue the development of advanced X-ray material discrimination methodologies proven out in previous work and mature testbed prototype technologies into full up Advanced X-ray System prototypes addressing these technical challenges. The efforts under this Call seek to enable technology developments from early TRL levels into technologies ready for maturation into deployable solutions. This BAA will focus on five specific topic areas:

- Advanced X-ray Systems Development – Development and testing of full-up system engineering design models (EDMs) (Technology Readiness Level (TRL) 3-5 level of maturity)
- Advanced Algorithms and System Integration – Development/maturation of threat detection and false alarm reduction algorithms, integration into operational/prototype systems and demonstration of real time operation.
- Supporting Component Technology Development – Development/maturation of system components and subsystems (such as X-ray Sources and Detectors) necessary to evolve laboratory and experimental prototypes into full up X-ray system designs able to meet the Advanced X-ray Systems requirements.
- Supporting Baggage Movement Technology – Development of information-based methods to include new methods of baggage classification, screening, and transport in the checked baggage domain to enable multiple parallel screening tiers to

adjudicate bag safety outside of X-ray technologies.

- Developing In-Line Checked Baggage Screening Training Applications - Development of both Threat Image Projection Software (TIPS) integrated with current EDS deployments as well as the development of best practices for training and data collection with TIPS programs.

## 2. Project Description/Scope

- 2.1. BAA Call solicitation 70RSAT20RB0000003 will advance aviation security and improvised explosive threat detection by maturing enabling technologies and technology prototypes. With this Call, S&T is interested in investing in technologies around TRL level 3-5 which can be developed to support checked and checkpoint baggage screening EDMs. The EDMs developed will be demonstrated and tested at a Government test facility under operationally realistic Stream of Commerce (SOC) screening conditions.

The primary technical focus is demonstrating full-up system capabilities that significantly enhance the capability to robustly detect improvised explosive threats, reduce primary baggage screening false alarm rates on all explosive threat classes, and increase passenger baggage screening throughput. This BAA Call is predominantly seeking responses offering *significant* enhancements to current baggage screening system detection and false alarm capabilities. Minor improvements to existing capabilities are not of interest for this BAA Call. Incremental improvements to existing system capabilities are of interest under this BAA Call and will be evaluated in relation to the level of performance enhancement and/or significant cost savings that are anticipated. For incremental improvements to existing system capabilities the proposer must provide detailed analysis to substantiate the level of performance enhancement and/or cost savings claims.

The majority of efforts under this BAA Call are anticipated to be Type II efforts, 24 months in duration, as defined by BAA HSHQDC-16-R-B0004 paragraph 2.2. The timelines and dollar values included in HSHQDC-16-R-B0004 and referenced in this document are the anticipated maximum award amounts and timelines, but the Government may exceed these amounts at its discretion. A transition of technology to TSA is anticipated to be in a period of 2-3 years. However, S&T also has interest in Type III technology efforts as defined in BAA HSHQDC-16-R-B0004 (period of performance 12 months or less) that may offer nearer term retrofit capability into currently deployed EDS and AT platforms.

- 2.2. Achieving significant enhancements in passenger baggage screening for explosive threat detection requires mature systems using next generation techniques for distinguishing the complex stream-of-commerce bag clutter from explosive threats. This BAA Call solicits responses to the following five technical topic areas (TTAs):

- Advanced X-ray Systems Development
- Advanced Algorithms and System Integration

- Supporting Component Technology Development
- Supporting Baggage Movement Technology
- Developing In-Line Checked Baggage Screening Training Applications

DHS S&T anticipates multiple awards under this BAA Call pending the quality of proposals received and the availability of funds. S&T reserves the right to make none, one, or multiple awards from this BAA Call.

- 2.3.** Central to this R&D acquisition will be the use of collaborative, multi-faceted research and development teams to achieve the desired end goals for the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) and the Transportation Security Administration (TSA). Candidate team members may consist of, but are not limited to, original equipment manufacturers (OEMs), university researchers, national laboratories, third party innovators of algorithms, and component manufacturers in the supply chain. The formation of strong systems development teams combining practical industry engineering experience with fundamental and applied research capabilities in multi-disciplinary fields including mathematics, x-ray physics, explosive/materials chemistry, and information science provides the greatest potential for developing and transitioning enhanced EDS and/or AT system capabilities to TSA for deployment in aviation security environments.

Each TTA is discussed in detail below and specific objectives for each TTA are also provided. Of particular note, it is anticipated that both metrics and analysis techniques to measure the development progress will evolve during the project.

### **3. Technical Topic Areas**

#### **3.1. TTA #1 Advanced X-ray Systems Development**

The focus of this TTA is to continue to mature advanced technologies for X-ray baggage screening systems. This effort will primarily be focused on maturing enabling technologies and technology prototypes into checked baggage explosive detection systems. These efforts are envisioned to be Type II efforts as defined in Section 2.2 of BAA HSHQDC-16-R-B0004 with a 24-month period of performance. The goal of this TTA is to achieve a significantly enhanced capability to robustly detect explosive threats, reduce primary baggage screening false alarm rates on all explosive threat classes, and increase passenger baggage screening throughput under real life operating conditions. The systems developed under this TTA will be demonstrated and tested at a government test facility (such as the TSL) under operationally realistic Stream of Commerce (SOC) screening conditions. All parties that have advanced X-ray system concepts meeting the maturity level of this TTA are encouraged to propose.

The advanced technologies listed below are representative only of technologies in which DHS S&T has made investments in the past:

- Multi-Energy Transmission X-ray Imaging

- Coded Aperture X-ray Imaging
- X-ray Diffraction Imaging
- Compton Scatter Imaging
- Phase Contrast Imaging

The above technologies are provided to help interested offerors understand potential program technical areas but are not meant to be inclusive for this BAA Call. S&T will also consider non-X-ray based screening capabilities and solutions which may or may not complement existing solutions.

A secondary goal is to support integration of third-party software components, such as those discussed in TTA #2, into OEM equipment with greater ease. Technology developed within this TTA will need to support an open architecture that will allow technology partners (including those that may be performing under TTA #2) access to the raw measurement data and the data processing resource environment for the purpose of algorithm development, software integration and testing initiatives. The goal is to facilitate opportunities for innovation, especially for third party algorithms, and increase the ability for OEMs to better deliver needed capability through such partnerships. Recognizing the significant research and development under this TTA, the goal will be to provide a preliminary Interface Control Document (ICD) describing the data, metadata formats, and a CONOP document on how to interface to the system. Such a document should allow technology partners (including those that may be performing under TTA #2) to access required measurement data and processing resources for the purpose of algorithm integration and testing. Computerized Tomography (CT) solutions as well as other technologies are welcomed, but solutions must include a significant unit cost reduction or capability improvement (lower probability of false alarm, higher probability of detection, greater scan rate) from current CT-based solutions. In addition to the requirements for explosives threat detection, enhanced detection capabilities for weapons, contraband and other prohibited items are of interest. The EDMs developed under this effort should be ready for developmental testing at the TSL within 24 months and ready for operational testing at the TSA Transportation Security Integration Facility (TSIF) within 30 months. The development efforts under this TTA shall have formal design reviews such as System Concept Review (SCR), Preliminary Design Review (PDR), Critical Design Review (CDR), as well as test readiness and test results reviews. These reviews will act as key go-/no-go decision points and will be further defined if a request for full proposal is made by the Government. Offerors should include a process for incorporating human factors and human performance design principles throughout the development of the equipment. SCR, PDR, and CDR should contain subject matter expert design inputs for Human Factors (HF) or Human Systems Integration (HSI). An initial project management plan will be due fifteen (15) days after award. Offerors must include personnel, test facilities & capabilities, and initial project timelines in the plan. Section 4.1 below identifies key deliverables for efforts under this TTA.

### **3.2. TTA #2 Advanced Algorithms and System Integration**

Under BAA-13-05 and BAA 17-03 several advanced reconstruction and automated threat recognition (ATR) algorithm methodologies were explored and assessed for their

feasibility and effectiveness to enhance the detection of explosives threats in checked and carry-on baggage screening. In this TTA, S&T is seeking to continue exploration and development of advanced reconstruction and ATR algorithm technologies for checked and carry-on baggage. A primary interest is in enhancing detection capabilities to cover a broader range of threat detection classes, significantly reduce primary screening false alarms and detect threats at TSA Tier levels higher than 2. This includes explosive and prohibited items that are listed for checked baggage. The efforts proposed under this TTA section must demonstrate that the technique can rapidly reach TRL 6 maturity to enhance explosive threat detection capabilities in passenger baggage screening X-ray equipment within the Type II 24-month time frame. Algorithms should be developed with the capability to adjust parameters affecting probability of false alarm, probability of detection, and screening speed in order to optimize the screening capability to passenger risk and the general threat environment.

Traditionally, OEMs have developed their own in-house detection algorithm methodologies. Since both third party (non-OEM developed) and OEM developed advanced ATR algorithms can be viable on an OEM platform, this TTA strongly encourages collaborative third party (non-OEM) and OEM algorithm development teams. These efforts are envisioned to be predominantly Type II efforts as defined in Section 2.2 of BAA HSHQDC-16-R-B0004 with a maximum 24-month period of performance.

Also of interest within the scope of this TTA are Type III efforts, as defined in Section 2.2 of BAA HSHQDC-16-R-B0004 (12 months or less), that focus on developing and transitioning advanced explosives detection algorithms to enhance the detection of improvised explosive threats and reduce the false alarm rates in deployed TSA EDS systems. These efforts should provide a threshold false alarm rate reduction by at least a factor of 2 while maintaining improvised explosive threat detection capabilities. OEMs are encouraged to work with academia and small business partners to develop feasible and effective algorithms to address the root causes of false alarms in deployed EDS. These efforts should provide algorithms that can be deployed with minimal field changeable modifications (for example, adding a processing sidecar) to the existing deployed EDS equipment. Efforts proposed under the Type III section of this TTA must demonstrate that the methodology can rapidly reach TRL 6-7 maturity to enhance explosive threat detection capabilities of passenger baggage screening X-ray equipment within the Type III 12-month time frame.

The advanced reconstruction and automated threat recognition (ATR) algorithm technologies developed under this TTA will be required to be integrated into an operationally viable X-ray platform such as a TTA #1 EDM or an existing OEM X-ray platform and to be demonstrated, tested and evaluated at a government test facility (such as the TSL) under operationally realistic Stream of Commerce (SOC) screening conditions.

In keeping with S&T's interest in maintaining open architecture standards for new development efforts, the efforts in this TTA shall define and specify an application programming interface (API) that will be used for integrating the enhanced ATR algorithms into the EDM or existing OEM X-ray platform. The API specifications will be

delivered to S&T to reflect the “to be built” state and updated with the “as built” and “delivered” states. Offerors should also use a process for incorporating human factors and human performance design principles, as necessary, throughout the development of the algorithm, the API, and the performance specifications.

The development efforts under this TTA shall have formal design reviews such as SCR, PDR, and CDR, as well as test readiness and test results reviews. These reviews will act as key go-/no-go decision points and will be further defined if a request for full proposal is made by the Government. Offerors should include a process for incorporating human factors and human performance design principles throughout the development of the equipment. SCR, PDR, and CDR should include subject matter experts in design for Human Factors (HF) or Human Systems Integration (HSI). An initial project management plan will be due fifteen (15) days after award. Offerors must include personnel, test facilities & capabilities, and initial project timelines in the plan. Section 4.2 below identifies key deliverables for efforts under this TTA.

### **3.3. TTA #3 Component Technology Development**

Baggage screening X-ray equipment system performance is highly dependent upon the availability of mature X-ray component technologies (such as X-ray sources and detectors) used to acquire X-ray information from the stream-of-commerce objects. This TTA is focused on the development/maturation of X-ray system components that are necessary to evolve laboratory and experimental prototypes into full-up X-ray system designs able to meet the Advanced X-ray Systems requirements. In previous advanced material discrimination R&D efforts many compromises were required in the feasibility and effectiveness evaluation of advanced techniques due to the lack of adequately mature components to support the design concepts. A prime example was assessing the utility of multi-energy imaging in improving detection and reducing false alarms in EDS and Advanced Technology (AT) 2 systems. While multi-energy detector arrays for small scale laboratory use were available, the maturity of arrays with sizes and form factors, resolution, linearity, dynamic range, uniformity, photon counting rate, and sensitivity to support many of the advance material discrimination design concepts were not available.

This TTA seeks to address these issues by focusing efforts to mature non-Commercial Off the Shelf (COTS) “long- lead” device technology, whose performance and enhanced characteristics are necessary to enable development of advanced X-ray baggage screening systems, such as those under TTA #1, to a TRL 6-7 maturity of systems development. These efforts are envisioned to be predominantly Type II efforts as defined in Section 2.2 of BAA HSHQDC-16-R-B0004 with a maximum 24-month period of performance.

DHS S&T will also consider development of near COTS devices that have clear immediate benefit to X-ray screening systems that are supportable by strong technical

analytical rationale with an accompanying business case. These efforts are envisioned to be Type III, as defined in Section 2.2 of BAA HSHQDC-16-R-B0004 with a maximum 12 months period of performance.

Proposers under this TTA will be required to develop detailed component specifications and provide them to DHS S&T and its stakeholders (such as BAA 13-05, 17-03, and TTA #1 performers and/or EDS/AT equipment manufacturers) as part of the SCR, PDR and CDR material packages for review and comment. The component specification level of maturity shall be commensurate with the design level of maturity at the corresponding review, (i.e. Functional level of detail at SCR, Preliminary detailed design specifications at PDR, Final detailed design specifications at CDR). The performer will design, build, and test the components developed under this TTA, integrate the component with an operationally viable X-ray baggage screening platform such as a TTA #1 EDM or an existing OEM platform, and evaluate and demonstrate that the component specification requirements have been achieved.

Performers under this TTA will also develop and provide a commercialization plan that will fully describe a manufacturing plan, a quality assurance plan, and sales plan in order to assess the performer's ability to successfully bring the component into the market place. The commercialization plan shall provide an anticipated product cost structure with estimated volume assumptions and end user pricing.

The development efforts under this TTA shall have formal design reviews such as SCR, PDR, and CDR, as well as test, test readiness, and test results reviews. These reviews will act as key go-/no-go decision points and will be further defined if a request for full proposal is made by the Government. An initial project management plan will be due fifteen (15) days after award. Offerors must include personnel, test facilities & capabilities, and initial project timelines in the plan. Section 4.3 below identifies key deliverables for efforts under this TTA.

### **3.4. TTA #4 Baggage Movement Technology Development**

The Baggage Handling System (BHS) currently exists under the purview of airport authority and is mostly limited to within-airport infrastructure. Responsibility for aspects of the BHS are shared between airports, TSA, and airlines. TSA has expressed interest in developing new methods of moving bags through airports by using logic-based decisions to either extend or reduce baggage time in system depending on extenuating factors. The result of this process would be one in which routing of bags could be changed due to expediency, detected threat level, or other environmental factors that may affect how a bag is treated in the BHS.

The focus of this TTA is to develop information-based methods to adjudicate bag safety outside of X-ray technologies. The effort will primarily be focused on developing novel methods of baggage classification, screening, and transport in the checked baggage domain to enable multiple parallel screening tiers. The goal is to achieve future architectures that take advantage of and expand upon airport baggage infrastructure and airport security infrastructure like networked sensors to reduce the need to physically search bags with false alarms and allow TSOs more time to search viable threats. The result should improve overall throughput while reducing pfa at a systemic level while allowing for more robust pd at the individual level. The methods developed under this TTA will be simulated and tested in a modelling environment.

Proposers under this TTA will be required to develop detailed specifications and provide them to DHS S&T and its stakeholders as part of the SCR, PDR and CDR material packages for review and comment. The specification level of maturity shall be commensurate with the design level of maturity at the corresponding review, (i.e. Functional level of detail at SCR, Preliminary detailed design specifications at PDR, Final detailed design specifications at CDR). The performer will design, model, and demonstrate the method/component/system developed under this TTA to validate specification requirements have been achieved. These efforts are envisioned to be predominantly Type II efforts as defined in Section 2.2 of BAA HSHQDC-16-R-B0004 with a maximum 24-month period of performance.

Performers under this TTA will also develop and provide a commercialization plan that will fully describe a manufacturing plan, a quality assurance plan, and sales plan in order to assess the performer's ability to successfully bring the component into the market place. The commercialization plan shall provide an anticipated product cost structure with estimated volume assumptions and end user pricing.

The development efforts under this TTA shall have formal design reviews such as SCR, PDR, and CDR. These reviews will act as key go-/no-go decision points and will be further defined if a request for full proposal is made by the Government. An initial project management plan will be due fifteen (15) days after award. Offerors must include personnel, facilities & capabilities, and initial project timelines in the plan. Section 4.4 below identifies key deliverables for efforts under this TTA.

### **3.5. TTA #5 In-Line Checked Baggage Screening Training Application Development.**

Baggage Screening relies not only on the EDS and associated software, but also on the training and actions of TSOs. Ensuring that TSOs are properly trained, maintain certifications, and perform well in the field can be a costly and time-consuming process for TSA. This TTA is focused on the development of a quality Threat Image Projection

System (TIPS) with combined or fictitious threat image capability for current and future EDS systems. The developed application/method should fulfill training needs and help determine levels of performance of TSOs.

A TIPS capability shall aid in reinforcing the TSO Technology Team through use of the TSOs expertise. The EDS associated software shall provide onsite training for the Officer assessing images as well as improving the Human Performance Systems Engineering and user interface. It shall address scoring as it relates to officer evaluation. EDS and On-Screen Alarm Resolution Protocol certified officers shall have the ability to focus on both the threat and the entire bag environment. Management shall be able to determine officer performance levels through data determined areas of concern for future training deployment.

This TTA seeks to address these issues by focusing efforts on the development of both TIP software integrated with current EDS deployments as well as the development of best practices for training and data collection with TIPS. The solution developed by a vendor should be all encompassing, including both a higher level of functional TIP performance like library management (to include multiple vectors for image creation/addition such as the user, OEM, and other third parties to be identified) and management of time-spacing for training inclusion, as well as collection and assessment of performance based data like overall airport testing results, assessments of individual screener performance, provision of feedback to screeners, and design of testing in a global sense and with respect to individual performances by individual screeners. Tests should be customizable per screener and per airport while also including guidance to achieve higher pd and lower pfa on a per screener and total airport basis. The methods developed under this TTA should have a path to be integrated into current or future OEM systems or currently fielded or future baggage handling systems. Any solution must comply with DHS/TSA IT security requirements.

DHS S&T will consider development of near COTS systems that have clear immediate benefits that are supportable by strong technical analytical rationale with an accompanying business case. These efforts are envisioned to be Type III, as defined in Section 2.2 of BAA HSHQDC-16-R-B0004 with a maximum 12 months period of performance. However, exceptions may be considered if advantageous to DHS S&T.

Proposers under this TTA will be required to develop detailed system specifications and provide them to DHS S&T and its stakeholders as part of the SCR, PDR and CDR material packages for review and comment. The component specification level of maturity shall be commensurate with the design level of maturity at the corresponding review, (i.e. Functional level of detail at SCR, Preliminary detailed design specifications at PDR, Final detailed design specifications at CDR). The performer will design and test the components developed under this TTA, integrate the component with an operationally viable X-ray baggage screening platform such as a TTA #1 EDM or an existing OEM platform, and evaluate and demonstrate that the component specification requirements have been achieved.

Performers under this TTA will also develop and provide a commercialization plan that will fully describe a manufacturing plan, a quality assurance plan, and sales plan in order

to assess the performer’s ability to successfully bring the component into the market place. The commercialization plan shall provide an anticipated product cost structure with estimated volume assumptions and end user pricing.

The development efforts under this TTA shall have formal design reviews such as SCR, PDR, and CDR, as well as test, test readiness, and test results reviews. These reviews will act as key go-/no-go decision points and will be further defined if a request for full proposal is made by the Government. An initial project management plan will be due fifteen (15) days after award. Offerors must include personnel, test facilities & capabilities, and initial project timelines in the plan. Section 4.5 below identifies key deliverables for efforts under this TTA.

## 4. Project Structure

This Call is structured into five distinct TTAs that aim to 1) develop and demonstrate Advanced X-ray Systems for screening checked baggage, 2) provide Advanced Algorithms and System Integration to enhance improvised explosive threat detection and reduce false alarms, 3) develop and mature component technologies necessary to develop TTA #1 Advanced X-ray Systems to TRL 6-7 maturity, 4) develop baggage movement technologies, and 5) develop complementary operational applications to facilitate TSO training and performance management.

### 4.1 TTA #1 Key Deliverables

The key deliverables required for TTA #1 are:

<b>DELIVERABLES</b>	<b>DUE DATE</b>
Project Management Plan	15 days after award
Monthly Status Reports	Due monthly until end of project
System Performance and Design Specifications	At major milestones
Major milestone reviews and materials (SCR, PDR, CDR Test Readiness Reviews (TRR) and Quarterly Status Reviews (QSR), etc.)	Read ahead due 5 day prior to review Final Due at Review meeting
Data Collection and Test Plans	Due 90 days prior to Test start
Data Collection and Test Reports	Due 15 days after Test Event end
Preliminary Interface Control Document (ICD) and a CONOP document	Not more than 12 months after award for Type II
Project Final Report – Including all analysis and raw data	Not more than 24 months after award for Type II and Not more than 12 months after award for Type III
EDM System Delivery	Not more than 24 months after award for Type II and Not more than 12 months after award for Type III

#### 4.2 TTA #2 Key Deliverables

The key deliverables required for TTA #2 are:

<b>DELIVERABLES</b>	<b>DUE DATE</b>
Project Management Plan	15 days after award
Monthly Status Reports	Due monthly until end of project
Major milestone reviews and materials (SCR, PDR, CDR Test Readiness Reviews (TRR) and Quarterly Status Reviews (QSR), etc.)	Read ahead due 5 day prior to review. Final Due at Review meeting
Data Collection and Test Plans	Due 90 days prior to Test start
Data Collection and Test Reports	Due 15 days after Test end
Project Final Report – Including all analysis and raw data	24 months after award for Type II and 12 months after award for Type III
API Definition Document	Final due at CDR
Advanced Detection Software Algorithm Data Package	Not more than 24 months after award for Type II and Not more than 12 months after award for Type III

#### 4.3 TTA #3 Key Deliverables

The key deliverables required for TTA #3 are:

<b>DELIVERABLES</b>	<b>DUE DATE</b>
Project Management Plan	15 days after award
Monthly Status Reports	Due monthly until end of project
Major milestone reviews and materials (SCR, PDR, CDR Test Readiness Reviews (TRR) and Quarterly Status Reviews (QSR), etc.)	Read ahead due 5 day prior to review Final Due at Review meeting
Test Reports	Due 15 days after Test end
Project Final Report – Including all analysis, raw data, and commercialization plan	Not more than 24 months after award for Type II and Not more than 12 months after award for Type III
Component Hardware Delivery	Not more than 24 months after award for Type II and Not more than 12 months after award for Type III

#### 4.4 TTA #4 Key Deliverables

The key deliverables required for TTA #4 are:

<b>DELIVERABLES</b>	<b>DUE DATE</b>
---------------------	-----------------

Project Management Plan	15 days after award
Monthly Status Reports	Due monthly until end of project
Major milestone reviews and materials (SCR, PDR, CDR Test Readiness Reviews (TRR) and Quarterly Status Reviews (QSR), etc.)	Read ahead due 5 day prior to review Final Due at Review meeting
Test Reports	Due 15 days after Test end
Project Final Report – Including all analysis, raw data, and commercialization plan	Not more than 24 months after award for Type II and Not more than 12 months after award for Type III
Software And/or Model Data Package	Not more than 24 months after award for Type II and Not more than 12 months after award for Type III

#### 4.5 TTA #5 Key Deliverables

The key deliverables required for TTA #5 are:

<b>DELIVERABLES</b>	<b>DUE DATE</b>
Project Management Plan	15 days after award
Monthly Status Reports	Due monthly until end of project
Major milestone reviews and materials (SCR, PDR, CDR Test Readiness Reviews (TRR) and Quarterly Status Reviews (QSR), etc.)	Read ahead due 5 day prior to review Final Due at Review meeting
Test Reports	Due 15 days after Test end
Project Final Report – Including all analysis, raw data, and commercialization plan	Not more than 24 months after award for Type II and Not more than 12 months after award for Type III
Software Data Package	Not more than 24 months after award for Type II and Not more than 12 months after award for Type III

## 5. Special Instructions/Notifications

### 5.1 Response Dates

<b>Event</b>	<b>Time Due</b>	<b>Date or Date Due</b>
Questions Due	2:00 PM Eastern Time	7/9/2020
Answers Posted		7/13/2020
White Papers Due	5:00 PM Eastern Time	7/20/2020
Notification of White Paper Evaluation Results		8/3/2020

Proposals Due	2:00 PM Eastern Time	8/19/2020
Notification of Proposal Evaluation Results		Sept./Oct. 2020

## 5.2 Contractual or Technical Inquiries

All contractual or technical questions regarding this BAA Call solicitation must be emailed to CBT20call@hq.dhs.gov no later than 2:00 PM Eastern Time June 30, 2020. Emails submitting questions are to include “Questions for 70RSAT20RB0000003” in the subject line. All questions and responses will be posted as an amendment to this solicitation on Contract Opportunities on beta.Sam.gov. Questions will only be accepted and answered electronically. **Offerors should be aware that contractor support personnel have access to this mailbox and that proprietary information should not be emailed to this inbox unless and until your organization has a signed company to company agreement with Noblis.** See section 5.5 for additional information.

## 5.3 General Instructions and Information

This BAA Call solicitation (70RSAT20RB0000003) is only seeking the submission of white papers at this time, subject to the date identified in the “Response Dates” table in Section 5.1 above. Full proposals are not being requested at this time. Invitations to submit full proposals will be extended based on white paper evaluation results in accordance with the date identified in the “Response Dates” table above. Full proposals must be received by the due date identified in the “Response Dates” table above. This Call is open to all responsible sources and is considered full and open competition.

Procedures for submission to the DHS S&T Portal are provided in Section 7 below and in Section 8 of BAA HSHQDC-16-R-B0004. Each submission must clearly state which TTA is being addressed. Note that offerors must complete the company/organization portal registration PRIOR to submitting a white paper for the first time. Ensure adequate time to complete the company/organization registration as delays in this process will not be authorization for late submissions of white papers. Company/organization registration information is in Section 7 below. In addition, each subsequent white paper requires registration in the portal. Information regarding white paper registration is in Section 7 below.

To be considered for award, offerors MUST submit white papers and Company to Company Agreements with Noblis, Inc. (discussed in Section 5.5 below) compliant with the response dates listed in Section 5.1, in accordance with the requirements in DHS BAA HSHQDC-16-R-B0004. Submissions not in compliance with BAA HSHQDC-16-R-B0004 may be rejected (note: the cover page created by the DHS S&T BAA Portal must be included but does not count against the page count). White papers will only be accepted via the portal. No emailed white paper submissions will be accepted for review. No classified white papers will be accepted.

White papers will be evaluated and Offerors will either be encouraged or not encouraged to submit a full proposal. Offerors who are not encouraged to submit a full proposal are still permitted to do so.

Procedures for submission of full proposals can be found in Section 9 of BAA HSHQDC-16-R-B0004. Invitations to submit full proposals will be extended based on white paper evaluation results in accordance with the date identified in the “Response Dates” table above. Full proposals must be received by the due date identified in the “Response Dates” table above.

DHS has a strong preference for open source licensing of software for all software developed and delivered, and the licenses for all proposed software deliverables will have to be identified in all submitted full proposals. However, as an alternative to open source release, offerors may also offer a strong technical transition plan for deployment of the technologies developed. All software developed and delivered is subject to security auditing; therefore, the offeror’s technical approach must identify how security auditing will occur. DHS expects offerors to follow industry best practices on software design

#### **5.4 Evaluation**

DHS S&T reserves the right to select for award and to fund all, some, or none of the proposals received in response to this BAA Call solicitation. The Evaluation Criteria in BAA HSHQDC-16-R-B0004, Section 11 “EVALUATION OF WHITE PAPERS AND PROPOSALS” apply to this Call.

Proposals received as a result of the BAA shall be evaluated in accordance with evaluation criteria specified therein through a peer or scientific review process. Written evaluation reports on individual proposals will be necessary but proposals need not be evaluated against each other since they are not submitted in accordance with a common work statement.

DHS S&T intends to use the following ratings to evaluate white papers and full proposals:

##### *Criterion I and Criterion II*

Excellent (E) - A very convincing demonstration that the BAA requirements are met by the Offeror’s display of the highest levels of innovation, technical competence, and managerial ability. The white paper/proposal fully and completely meets the expectations of the BAA and sets forth plans, approaches, and analyses that show a high probability of meeting DHS requirements.

Very Good (VG) - Analyses, approaches, and planning considerations demonstrate that the Offeror is able to interpret goals and project them into plans, analyses, etc., in a clear, concise manner. By this analysis, the offeror demonstrates an acute awareness of the subtle interactions influencing system design; technical and planning efforts show strong promise of meeting DHS requirements.

Good (G) - Plans, approaches, and analyses are provided to the extent requested, and the key or pivotal points raised by the applicable factors have been satisfactorily covered in the white paper. The offeror has presented an orderly plan to meet the stated goals, but the white paper/full proposal does not necessarily demonstrate any exceptional features, innovations, analysis, or originality. The technical

analyses satisfactorily meet requirements and are technically sound.

Fair (F) - The white paper/full proposal indicates minimal understanding of the problem. The technical analyses meet the goals and are technically sound, but the offeror fails to demonstrate a reasonable probability of successfully achieving the desired outcome of the topic area.

Unacceptable (U) - The white paper does not meet the BAA's criterion.

### *Criterion III*

Reasonable (R) – White paper/full proposal cost information appears reasonable based on the proposed time/level of effort and materials needed to successfully complete tasks associated with this effort. The Government has few, if any questions on costs.

Likely Reasonable with Questions (Q) – White paper/full proposal cost information may be reasonable after the Government receives additional information to evaluate costs.

Not Reasonable (N) – White paper/full proposal cost information does not appear reasonable. Costs are not adequately tied to technical approach or are not logical.

## **5.5 Company to Company Agreements**

White papers must comply with the information in BAA HSHQDC-16-R-B0004 paragraph 11.4 regarding Company to Company Agreements.

**Important Note: DHS intends to use Noblis, Inc. for routine administrative support during the evaluation process of both white papers and full proposals. All Offerors, Prime Contractors only (this applies to all offerors, whether or not the offeror is a company), must submit an executed Company to Company Agreement with Noblis, Inc., found in Appendix A, along with their white paper submission. Company to Company Agreements must be dated this year (2020). The Agreement found in Appendix A shall not be altered. Submissions that do not include an executed Agreement will be considered non-responsive and will not be considered. To get the Noblis, Inc. Point of Contact information, Offerors are to send an email to CBT20call@hq.dhs.gov and indicate “NDA” in the Subject line. Offerors are encouraged to allow sufficient time to permit agreement execution.**

## **5.6 Type Classification Ceilings**

BAA HSHQDC-16-R-B0004, describes the Type Classifications for proposals. Specific to this Call, the ceiling values for each type are as follows:

Type I – Type I awards are limited to a total contract value not to exceed \$2,000,000.00, not including operational evaluation, pilot, and/or transition options.

Type II – Type II awards are limited to a total contract value not to exceed \$3,500,000.00,

not including operational evaluation, pilot, and/or transition options.

Type III – Type III awards are limited to a total contract value not to exceed \$4,500,00.00, not including operational evaluation, pilot, and/or transition options.

The timelines and dollar values included in HSHQDC-16-R-B0004 and referenced in this document for types of awards are the anticipated award amounts and timelines, but the Government may exceed these amounts at its discretion. However, contractors are highly encouraged to stay within the parameters identified above.

## **5.7 Foreign Participation**

Offerors are reminded that foreign participation may occur as defined in BAA HSHQDC-16-R-B0004, Section 1.3. Offerors, including those located outside the continental United States, should provide full costs (delivery costs included) for any deliverables not anticipated for delivery in a softcopy format. All materials submitted in response to this solicitation shall be in the English language. White papers, and later proposals, received in other than English shall be rejected. Offerors invited to submit proposals shall do so only in terms of U.S. dollars. Proposals received in other than U.S. dollars shall be rejected.

## **5.8 Export Control Requirements**

Offerors are reminded of the export control markings required by BAA HSHQDC-16-R-B0004, Section 12.5

## **5.9 Travel**

For purposes of estimating costs for full proposals, offerors should anticipate travel to three (3) project meetings per year at DHS S&T Headquarters in Washington DC. Travel will be reimbursed in accordance with the limitations set forth in FAR 31.205-46, Travel Costs, and the Federal Travel Regulation. Local travel within a 50-mile radius from the Contractor's facility or the Contractor's assigned duty station will not be reimbursed. This includes travel, subsistence, and associated labor charges for travel time. Travel performed for personal convenience or daily travel to and from work at the Contractor's facility or local Government facility (i.e., designated work site) shall not be reimbursed hereunder. The Contractor shall not be reimbursed for moving or relocation expenses for the Contractor or Contractor employees, and/or subcontractors.

## **5.10 Order of Precedence**

If any of the terms and conditions contained in this solicitation conflict with terms and conditions included in BAA HSHQDC-16-R-B0004, the terms and conditions in this Call shall take precedence.

## **6. Sensitive Information; Privacy and Security Compliance**

DHS has and will exercise full control over granting, denying, withholding, or terminating

unescorted Government facility, Government systems and/or sensitive Government information access for Contractor employees, based upon the results of a DHS fitness (suitability) investigation. DHS may, as it deems appropriate, authorize and make a favorable entry of duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the contractor to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment contractor fitness (suitability) authorization will follow as a result thereof. The granting of a favorable EOD decision or a full contractor fitness (suitability) authorization determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by DHS, at any time during the term of the task order. No employee of the contractor shall be allowed unescorted access to a Government facility, access to any sensitive information or access to DHS Systems without a favorable EOD decision or contractor fitness (suitability) determination by the DHS Office of Security. Contract employees assigned to the task order not needing access to sensitive DHS information, DHS systems or access to DHS facilities will not be subject to security contractor fitness (suitability) screening. Contract employees awaiting an EOD decision may not begin work on the task order. Limited access to Government buildings is allowable prior to the EOD decision if the contractor is escorted by a Government employee. This limited access is to allow contractors to attend briefings, nonrecurring meetings, and begin transition work. Classified information is Government information which requires protection in accordance with Executive Order 13526, National Security Information (NSI) as amended and supplemental directives. If the contractor has access to classified information at a DHS owned or leased facility, it shall comply with the security requirements of DHS and the facility. If the contractor is required to have access to classified information at another Government Facility, it shall abide by the requirements set forth by the agency.

Depending on an offeror's specific proposal and the TTA proposed under, offerors may have access to sensitive information in awards under this BAA Call. DHS S&T will comply with the requirements of HSAR Class Deviation 15-01 and the HSAM Appendix G Sensitive Information Checklist for individual awards under this BAA. Accordingly the clauses below may apply to individual awards under this BAA.

#### Safeguarding of Sensitive Information (MAR 2015)

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

(b) Definitions. As used in this clause—

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or

identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

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

“Sensitive Information” is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

- (1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);
- (2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, “Policies and Procedures of Safeguarding and Control of SSI,” as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);
- (3) Information designated as “For Official Use Only,” which is unclassified information of a sensitive nature and the unauthorized

disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

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

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

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

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

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

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

- (1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
- (2) DHS Sensitive Systems Policy Directive 4300A
- (3) DHS 4300A Sensitive Systems Handbook and Attachments
- (4) DHS Security Authorization Process Guide

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

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

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

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

(3) All Contractor employees with access to sensitive information shall execute DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA), as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide

copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

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

(1) Complete the Security Authorization process. The SA process shall proceed according to the DHS Sensitive Systems Policy Directive 4300A (Version 11.0, April 30, 2014), or any successor publication, DHS 4300A Sensitive Systems Handbook (Version 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 <http://www.dhs.gov/privacy-compliance>.

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

(3) Security Review. The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

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

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

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

Plan, or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) Sensitive Information Incident Reporting Requirements.

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with 4300A Sensitive Systems Handbook Incident Response and Reporting requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use FIPS 140-2 Security Requirements for Cryptographic Modules compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

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

- (i) Data Universal Numbering System (DUNS);
- (ii) Contract numbers affected unless all contracts by the company are affected;
- (iii) Facility CAGE code if the location of the event is different than the prime contractor location;
- (iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
- (v) Contracting Officer POC (address, telephone, email);
- (vi) Contract clearance level;
- (vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
- (xiii) Government programs, platforms or systems involved;
- (ix) Location(s) of incident;
- (x) Date and time the incident was discovered;

- (xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
- (xii) Description of the Government PII and/or SPII contained within the system;
- (xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
- (xiv) Any additional information relevant to the incident.

(g) Sensitive Information Incident Response Requirements.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- (i) A dedicated telephone number to contact customer service within a fixed period;
- (ii) Information necessary for registrants/enrollees to access credit reports and credit scores;

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

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

#### Information Technology Security and Privacy Training [March 2015]

- (a) **Applicability.** This clause applies to the Contractor and its contractors, its subcontractors, and their employees (hereafter referred to collectively as “Contractor”). The Contractor shall insert the substance of this clause in all subcontracts.
- (b) **Security Training Requirements.**

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

training has been completed for all Contractor and subcontractor employees.

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

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

## **7. Procedures for Submitting White Papers and Proposals in DHS S&T BAA Portal**

### **7.1 Company/Organization Registration.**

**IMPORTANT:** Before submitting a white paper or proposal for the first time, you must first register your company/organization in the system. Note, this registration takes some time; therefore, it is prudent to ensure company registration is completed well before the closing time for either white paper or proposals submissions. It is recommended that the Business Official or an authorized representative designated by the Business Official be the first person to register for your company. Your company's Taxpayer Identification Number (TIN) is required during registration. (If your company is registered, other new users may register and associate their information with the company's existing record.) When registration is completed, users can submit and manage their white papers and proposals.

- After the company/organization is registered, new users must register by associating their information with the company/organization's existing record.
- When registration is complete, users can submit and manage white papers and proposals.
- To access the log in/registration page of the DHS S&T BAA Portal:
  - Go to the DHS S&T BAA Portal at <https://baa2.st.dhs.gov/>;
  - On the home page, click on the *Portal Login* link, located at top-right corner of the page.
  - To begin the registration process, click either the *Register* link at the top of the page or the *Not Registered?* link at the bottom of the page.
- For additional step-by-step information regarding registration and submission of white papers and proposals, on the DHS S&T BAA Portal home page (<https://baa2.st.dhs.gov/>), in the navigation menu on the far right, click on *Resources*. Once on the Resources page, click on the link to the Portal Registration and Submissions Training Guide.

## **7.2 White Paper and Proposal Registration.**

- Each white paper, if requested, and proposal to be uploaded in the DHS S&T BAA Portal will be assigned a white paper and proposal registration number in the portal.
- To upload a white paper or proposal, after logging into the portal at (<https://baa2.st.dhs.gov/>), see Section 4.2 of the Portal Registration and Submissions Training Guide (access information provided in paragraph 7.1 above.)

## **7.3 DHS S&T BAA Portal Help Desk.**

For additional assistance with the DHS S&T BAA Portal, you can contact the DHS S&T BAA Portal Help Desk at [dhsbaa@reisystems.com](mailto:dhsbaa@reisystems.com) or by phone at (703) 480-7676. This contact information is provided in the "Help Desk" portion of the bottom of the screen of any page in the portal.

Appendix A. Company to Company Agreement

**COMPANY TO COMPANY AGREEMENT**

COMPANY TO COMPANY AGREEMENT: DHS BROAD AGENCY ANNOUNCEMENT (BAA) HSHQDC-16-R-B0004 (Calls 70RSAT20RB00000002 and 70RSAT20RB00000003)

The Parties to the subject Agreement agree that Noblis, Inc. (2002 Edmund Halley Drive, Reston VA 20191) may have access to proprietary information contained within the technical and cost proposals that were submitted on behalf of your company/facility solely for the purpose of performing technical advisory and/or administrative support services for the Government, in evaluating proposals submitted in response to this BAA Call.

The Parties agree to protect the proprietary information from unauthorized use or disclosure for a period of 10 years, or less if the disclosed information ceases to remain proprietary, and to refrain from using the information for any purpose other than that for which it was furnished.

---

Offeror's Company Name

---

Name of Offeror's Company Official (Printed)

---

Signed / Dated

---

Name of Noblis Company Official (Printed)

---

Signed / Dated