Department of Homeland Security
Science and Technology (S&T) Directorate

OFFICE OF MISSION AND CAPABILITY SUPPORT

OPEN BROAD AGENCY ANNOUNCEMENT (BAA)

Screening at Speed Program (SaS)

70RSAT22RB00000001 P00001

Table of Contents

1. GENERAL INFORMATION 5

1.1 Introduction. 5

1.2 Program Mission and Objectives. 5

1.3 Foreign Government Participation. 6

1.4 Agency Name. 7

1.5 Research Opportunity Title. 7

1.6 Program Name. 7

1.7 Research Opportunity Number. 7

1.8 Response Dates. 7

1.9 Government Representatives. 7

1.10 Inquiries. 8

2. RESEARCH OPPORTUNITY DESCRIPTION 8

2.1 Anticipated Topic Areas (TAs). 8

2.2. Type Classifications. 9

3. TESTING AND EVALUATION FACILITIES. 10

4. AWARD INFORMATION 10

4.1 Anticipated Funding for the Program. 10

4.2 Anticipated Number of Awards. 10

4.3 Anticipated Award Types. 10

4.4 Expected Amount of Individual Awards. 11

4.5 Anticipated Period of Performance for Individual Awards. 11

5. ELIGIBILITY INFORMATION 11

6. DOWNLOAD OF THIS BAA 11

7. REGISTRATION IN DHS S&T BAA PORTAL (Must be completed prior to uploading any submissions.) 12

8. PHASE I SUBMISSION REQUIREMENTS 12

8.1 White Paper Submission Requirements 12

8.2 Other Phase I Procedures 13

9. PHASE II PROPOSAL SUBMISSION REQUIREMENTS 13

9.1 Submission Requirements. 14

9.2 Submission Dates and Times. 14

9.3 No Classified Documents. 14

9.4 Multiple Proposals. 14
9.5 Proposal Format....14
Assertions Table....14
9.6 Non-compliant Proposals. 18
10. PROCEDURES FOR SUBMITTING WHITE PAPERS AND PROPOSALS IN DHS S&T BAA PORTAL 18
10.1 Company/Organization Registration. 18
10.2 White Paper and Proposal Registration....19
10.3 DHS S&T BAA Portal Help Desk....19
11. EVALUATION OF WHITE PAPERS AND PROPOSALS....19
11.1 General. 19
11.2 Evaluation Criteria. 19
11.3 Basis for Phase I and Phase II Selection. 20
11.4 Evaluation Panel....20
11.5 Notification to Offerors of Evaluation Findings....22
12. OTHER TERMS AND CONDITIONS 22
12.1 NAICS. 22
12.2 System for Award Management (SAM)....22
12.3 Information for Respondents. 22
12.4 Organizational Conflict of Interest....23
12.5 Export Control....23
12.6 Intellectual Property. 24
12.7 Publication of Research Results and Award Information....24
12.8 Adequate Accounting System for Cost Reimbursement Type Contracts. 25
12.9 Certificate of Current Cost or Pricing Data. 25
12.10 Applicable Provisions and Contract Clauses....26
12.11 Government Property, Government Furnished Equipment (GFE) and Facilities. 43
12.12 SAFETY Act. 43
12.13 Security Classification....43
12.14 Subcontracting Plan....44
12.15 Additional Deliverables....44
12.16 Types of Changes That May Occur to Awards Under This BAA. 44
12.17 Reporting....44

Appendix A. Company to Company Agreement 45

1. GENERAL INFORMATION

1.1 Introduction.

This solicitation is a Broad Agency Announcement (BAA) as contemplated in Federal Acquisition Regulations (FAR) 6.102(d)(2) and 35.016. A formal Request for Proposal (RFP) will not be issued in this matter. This announcement does not request any proposals at this time. Solicitations (or Calls) requesting white papers or proposals will be accomplished via amendments to this BAA. This BAA is issued in support of Department of Homeland Security (DHS) Science and Technology Directorate (S&T) targeted research and development (R&D) projects.

This Screening at Speed (SaS) BAA will be open for five years from the date publicized on the Government's Point of Entry (GPE), SAM.gov website (SAM). The strategy for a five-year BAA with the ability to make Calls throughout the life of the BAA will allow for quick and efficient delivery of practical R&D services to generate potential solutions for each Topic Area.

Periodically during the five years, individual Calls for white papers or proposals responding to the specified SaS program capability need will be solicited on SAM against this BAA. Each Call will (1) identify specific details regarding the Call Topic Area, (2) identify submission instructions in addition to those outlined in this BAA, and (3) contain a common cutoff date for submissions. The Call details will be such that interested and capable contractors can tailor a response and provide a submission in response to the Call.

1.2 Program Mission and Objectives.

Evolving threats have created a need for technological improvements to securely screen the growing number of people who pass through security checkpoints each year. The aviation security threat environment is constantly evolving and the DHS and Transportation Security Administration (TSA) must work diligently to overcome novel threats. To meet this challenge, DHS and TSA must invest in emerging technologies with the potential to transform the airport security landscape. The SaS program was developed by DHS S&T to investigate, develop, and efficiently deploy transformational technologies to bolster aviation security while creating a more seamless passenger experience. SaS is developing traditional security checkpoints into a "system of systems" to enable a more efficient and secure holistic threat assessment of passengers and property. This applies to many law enforcement and security agencies at the federal, state, local, tribal and territorial level. As an example, before 9/11, the average aviation checkpoint processed 350 passengers per hour. Today, increased security measures have reduced that number below 150. Limitations in current technology require people to divest, and later collect, some categories of their accessible property (references to carry-on items, personal electronics, and carry-on baggage, here after referred to as "accessible property") prior to transiting the checkpoint. The divestiture and collection process can take significant time (35 seconds and 40 seconds per passenger, respectively), heavily burden TSA resources, and pose a major inconvenience to the traveling public. The Federal Aviation Administration (FAA) forecasts a steady annual increase in passenger volume over the next 20 years, indicating that technology must quickly become more efficient as it becomes more secure.

System limitations also lead to false alarms, requiring additional time and resources to resolve. As

the threat environment continues to evolve, current technology and procedures are limited in their ability to adapt rapidly. Advanced threats have compelled TSA to institute regulations (*e.g.,* '3-1-1' quantity restrictions on liquids/aerosols/gels (LAGs), shoe removal, electronics divestiture) which force people to surrender benign items (such as drinks and cosmetics) and increase the number of discrete items that must be screened. Finally, the Automated Target Recognition (ATR) capability of currently deployed screening systems requires the development of state-of-the-art Machine Learning (ML) algorithms capable of handling high threat levels (lower masses, different form factors, etc.). This is an opportunity for the TSA to leverage an emerging transformational technology to significantly enhance passenger and accessible property screening capabilities.

The primary DHS Component driving requirements for SaS is TSA. However, S&T will work closely with other DHS operational organizations such as United States Secret Service (USSS) and Federal Protective Service (FPS) to identify and incorporate their requirements as funding and time allows. SaS also hopes to develop dual-use technologies that can meet multiple Component requirements as a single capability or a family of related capabilities.

The end goal of the SaS is to develop and demonstrate faster and more robust passenger and personal item / accessible property screening technologies. For the TSA example, technologies are expected to have the following capabilities:

- Detect threats at TSA's highest standards
- Screen 300+ people per lane per hour as well as their accessible property by:
    - Screening people without the divestiture of outerwear, shoes, belts, or headwear
    - Screening LAGs and Powders without removal from accessible property
    - Lifting restrictions on the quantity and size of LAGs and Powders in accessible property
    - Screening personal electronics without removal from accessible property
    - Significantly reducing false alarms
- Integrate future third-party capability upgrades as they become available
- Intuitive operations enabling positive Transportation Security Officer (TSO) and passenger experiences

Other DHS stakeholders' requirements will be similarly centered on throughput of people per hour, characteristics of threats to be detected and systems with which to be integrated. Additional target items that are not directly in the TSA mission space (e.g., narcotics) may also be considered under this BAA.

1.3 Foreign Government Participation.

Security is a global concern and DHS has collaborative activities with several countries. As a result, this BAA intends to have foreign government participation, to include access to white papers and proposal submissions for determining joint-funding, as well as joint participation in overseeing projects throughout the contract period of performance. Foreign government participation will be determined by Topic Area for each Call based on DHS collaboration and may include any of the following international partners: (a) the United Kingdom of Great Britain and Northern Ireland; (b) the Government of Australia; (c) the Government of Canada;

(d) the Kingdom of the Netherlands; (e) the European Union; (f) the Government of Germany; (g) the Government of Israel; (h) the Kingdom of Sweden; (i) the Government of New Zealand; and (j) the Government of Singapore.

In addition, foreign government personnel from any one of the aforementioned countries may participate in the evaluation process as technical reviewers of submitted white papers and/or proposals if their respective nation has been identified in the individual Call made under this BAA. Should foreign government personnel participate in the evaluation process, DHS will share white papers and proposals subject to the provisions for handling both "Controlled Unclassified Information" and "Business Confidential Information," as stated in each country's international agreement with the DHS or the U.S. Government. In addition, foreign government personnel are not permitted to release any information to third parties, including others in their organization. By the act of submitting any material in response to this BAA, offerors are therewith consenting to allowing access to financial, confidential, proprietary, and/or trade secret marked information, and any other material contained therein to foreign government personnel.

Intellectual Property Implications: Offerors should note that, in individual Calls where a foreign government is a participant, the technical annex or other governing document may require that the foreign government acquire the same rights as the United States.

1.4 Agency Name.

Department of Homeland Security
Science & Technology Directorate
Washington, DC 20528

1.5 Research Opportunity Title.

Screening at Speed Research and Development.

1.6 Program Name.

Screening at Speed.

1.7 Research Opportunity Number.

The number on the cover page of this BAA.

1.8 Response Dates.

This announcement does not request any white papers or proposals at this time. Individual Calls will be made against this BAA via solicitations posted on SAM at http://www.sam.gov/. Each individual Call will identify submission requirements for white papers or proposals.

1.9 Government Representatives.

Program Office:

John Fortune
Screening at Speed Program Manager
Office of Mission Capability and Support DHS Science & Technology
245 Murray Lane, #0200
Washington DC, 20528

Business:

Jennifer K. Koons
Contracting Officer
Department of Homeland Security
Office of Procurement Operations
Science & Technology Acquisitions Division, Mailstop 0115
Washington, DC 20528-0115

1.10 Inquiries.

All contractual or technical inquiries to this BAA must be submitted to the BAA Contracting Officer and Contract Specialist. The program and technical staff will not acknowledge, forward, or respond to any inquiries received in any other manner concerning this BAA or Calls issued against this BAA. Contractual questions and answers will be posted periodically in www.sam.gov under the announcement for this BAA. All inquiries must be in writing and will not be answered verbally.

For inquiries regarding use of the DHS S&T Office of Industry Partnerships (OIP) portal, refer to paragraph 10.3 below for information on contacting the portal Help Desk.

2. RESEARCH OPPORTUNITY DESCRIPTION

2.1 Anticipated Topic Areas (TAs).

The following TAs are representative only**.**

- Passenger Analysis
  - Video Analytics
  - Integrated Sensing / Data Fusion
  - Risk-Based Security
  - Identity Verification / Credential Authentication
- Passenger Screening
  - Millimeter Wave (Active or Passive)
  - Terahertz Wave
  - Enhanced Metal Detection
  - Automatic Threat Recognition
  - Radio Frequency (RF) Material Characterization
- Property Screening
  - Computed Tomography (CT) X-ray
  - Phase Contrast Imaging
  - X-ray Diffraction

    - CT Reconstruction
    - Prohibited Items Detection Algorithms
    - Explosive Detection Algorithms
    - Non-X-ray Sensors (e.g., Neutron Imaging)
- System Architecture and Integration
    - Open Interfaces and Algorithms
    - Curb-to-gate Sensing
    - Network Interconnects and Data Topology
    - Data Storage and Curation
    - Data Fusion Algorithms
    - Seamless Concepts of Operations, Passenger Self-Screening
    - Image Processing and Human Systems
- Enabling Capabilities
    - Trace Explosives Detection (Contact or Non-Contact)
    - Bulk Explosives Detection
    - User Interfaces Including Augmented/Virtual Reality
    - Synthetic Data Generation
    - Rapid Response / Emerging Threat Mitigation
    - Process Optimization and Officer Evaluation
- Test & Evaluation
    - Explainable Artificial Intelligence / Machine Learning
    - Automated Testbeds

The above TAs are provided to help interested offerors understand the potential SaS program technical areas. Specific TAs will be identified in each Call.

2.2. Type Classifications.

Calls may include Type Classifications which may specify more specific requirements for a proposed solution under a Call. Type Classifications will depend on the specific program objectives at the Call level. In general, requirements under this BAA may include one or more of the development strategies depending on the maturity of solutions available, end-user requirements, transition strategies and available funding. Offerors submitting responses will be required to identify which of the Type Classifications, as defined in the Call, align with their submission. DHS S&T may use a phased or stepped approach on Calls, as needed, for various technology levels. Some development strategy examples include:

Development Strategy	TRL (Start)	TRL (Finish)

Novel Major Requirements	3	7
Technology Adaptation	5	7
Core R&D	3	6
Transition R&D	4	6
Novel Concept Maturation	3	5

Technology Readiness Levels (TRLs) for this BAA roughly correspond to the NASA TRL Definitions: https://www.nasa.gov/pdf/458490main_TRL_Definitions.pdf

3. TESTING AND EVALUATION FACILITIES.

Performers for SaS will be required to test and evaluate their technologies with respect to project goals. DHS uses test results from several different venues to assess program capability and maturity:

- Vendor in-house testing to determine status of development and risk mitigation
- Transportation Security Laboratory (TSL) for three levels of Developmental Test and Evaluation (DT&E) for most explosive and threat types
- Tyndall Reactive Materials Group (TRMG) for DT&E of certain explosive types/quantities
- TSA Systems Integration Facility (TSIF) for integration testing, concept of operations development, and Operational Test and Evaluation (OT&E)

Offerors should consider the specific test and evaluation requirements of the proposed technical solutions, identify in the proposal the primary test environment to be used to conduct testing and evaluation, and include a description of the test and evaluation methodology appropriate for the proposal.

4. AWARD INFORMATION

4.1 Anticipated Funding for the Program.

Subject to official fiscal appropriations, it is anticipated that SaS will have a total of $99M over the next 5 years to support this BAA. The estimated value is not a promise of assured funding in that amount. Funding is uncertain and is subject to change. Government discretion may result in changes in funding availability.

Depending on interest in particular submissions, individual awards may be jointly funded from any of the foreign countries identified in paragraph 1.3 above.

4.2 Anticipated Number of Awards.

The total number of awards under this solicitation is unknown. However, one or more awards may be made from each Call issued during the 5-year open period of this BAA.

4.3 Anticipated Award Types.

It is anticipated that awards made for each Call issued against this BAA will be in the form of cost reimbursement type contracts. However, the Government reserves the right to award firm fixed price, time and materials, or labor hour contracts, cooperative agreements, Other

Transactions (OTs) (if authorized by law at time of award), Cooperative Research and Development Agreements (CRADAs), or interagency agreements to appropriate parties should the situation warrant.

In the event an offeror or subcontractor is a Federally Funded Research and Development Center (FFRDC), Department of Energy National Laboratory, or other Federally funded entity, DHS S&T will work with the appropriate sponsoring agency to issue an interagency agreement pursuant to the Economy Act (31 U.S.C. 1535) or other appropriate authority.

4.4 Expected Amount of Individual Awards.

Individual award amounts will vary per Call. Therefore, any specified award per Type Classification will be identified on a Call-by-Call basis.

4.5 Anticipated Period of Performance for Individual Awards.

Individual Calls will specify period of performance requirements. No individual award made under any Call may exceed five (5) years.

5. ELIGIBILITY INFORMATION

This BAA is open to ALL responsible sources, domestic or foreign. Foreign or foreign-owned offerors are advised that their participation is subject to the foreign disclosure review procedures, applicable export control laws, and other applicable federal laws, regulations, and policies pertaining to foreign entities. It is the intent of R&D contracting to obtain a broad base of the best contractor resources from the scientific and industrial community, to include small businesses. As a result, no portion of this BAA will be set aside pursuant to FAR Part 19.502-2. Offerors may include (but are not limited to):

- Single entities or teams from private-sector organizations;
- Government laboratories;
- FFRDCs, including Department of Energy National Laboratories and Centers, individually or as a team member of an eligible principal Offeror, so long as they are permitted under a sponsoring agreement between the Government and the specific FFRDC.
- Historically Black Colleges and Universities (HBCUs);
- Minority Institutions (MIs);
- Small & Small Disadvantaged Business concerns, including Women-Owned Small Business concerns, Veteran-Owned Small Business concerns, Service-Disabled Veteran-Owned Small Business concerns, and Historically Underutilized Business Zone (HUBZone) Small Business concerns; and

  Any academic institutions or non-profit organizations not included in the above categories.

6. DOWNLOAD OF THIS BAA

This BAA should be read in its entirety by any entity considering a submission in response to any Call issued against this BAA. This BAA can be downloaded in its entirety from the SAM

website at **http://www.sam.gov**. The BAA will also be available on the DHS S&T Office of Industry Partnerships (OIP) Portal.

7. REGISTRATION IN DHS S&T OIP PORTAL (Must be completed prior to uploading any submissions.)

Registration in an S&T electronic interface may be required prior to submission. Instructions for such registration will be provided on the individual Calls.

8. PHASE I SUBMISSION REQUIREMENTS

The Government may choose to utilize a multi-step evaluation process which may include one or more phases. Submission instructions and the evaluation process will be determined by individual Calls. The first phase of a Call may include White Papers or another evaluation process. General information on White Paper submissions, if used, is included below.

8.1 White Paper Submission Requirements

8.1.1 Calls May Request White Papers.

Calls issued against this BAA may request the submission of white papers. Submission requirements for white papers, when requested, shall be in accordance with this announcement, unless otherwise amended in the individual Call. Offerors should be alert for any amendments to individual Calls that may permit extensions to the submission date or modify the terms and conditions identified in that Call.

8.1.2 Submission Dates and Times.

Submission dates and times will be identified in each Call. White papers WILL NOT BE ACCEPTED after the established due date. There will be no exceptions to the time and date on which responses are due, unless otherwise determined by the Government.

8.1.3 No Classified Documents.

No classified white papers will be accepted.

8.1.4 No Proposal Submission Authorized Without White Paper Submission.

If a Call requests a white paper submission, offerors must submit an evaluable white paper to be considered for participation in proposal submissions. Offerors are not eligible to submit a proposal for any white paper rejected as non-compliant. For more information regarding non-compliant white paper submissions, refer to Section 8.1.8 below.

8.1.5 Multiple White Papers.

Multiple white papers per Call may be submitted. Each submitted white paper must comply with

the terms outlined herein.

8.1.6 White Paper Format.

White paper format will be specified in the individual Calls. White papers may include narrative, pictures, figures, tables, and charts in a legible size, and must be accompanied by a one-page quad chart.

8.1.7 Company to Company Agreement with Noblis, Inc (or successor Systems Engineering and Technical Assistance (SETA) contractor).

This Agreement shall be included in accordance with paragraph 11.4 and does not count against the white paper page count.

8.1.8 Non-compliant White Papers.

White papers submitted that do not comply with the white paper submission requirements outlined in this BAA, as well as any additional submission requirements outlined in the respective Call under which the white paper is being submitted, may result in the white paper being determined non-compliant and rejected without evaluation. Examples of non-compliant white papers include, but are not limited to:

- Total contract value proposed in the white paper is greater than the boundaries identified in the respective Call;
- Total number of pages submitted does not comply with the page count limitations identified in the respective Call; or
- Pages within the white paper do not comply with the requirements for font sizes and margins identified in the respective Call; or
- Submission requirements are not met, such as the one-page limitation for the cover page and the quad chart (as required by 8.1.6 above) is exceeded, etc., or the Company to Company Agreement is not submitted.

8.2 Other Phase I Procedures

8.2.1 The Government may identify other Phase I procedures for a multi-step evaluation process. These will be identified at the Call level and may include such procedures as:

- Technical demonstrations
- Oral/virtual presentations
- Written application
- Survey of past experience
- Written quad charts

9. PHASE II PROPOSAL SUBMISSION REQUIREMENTS

The Government anticipates full proposal submission to be a requirement for each individual Call, whether or not a multi-phased approach is used. However, the Government may use its discretion to use alternate submission requirements as determined by individual Calls.

9.1 Submission Requirements.

Submission requirements for proposals shall be in accordance with this announcement unless otherwise amended in the individual Call. Offerors should be alert for any amendments to individual Calls that may permit extensions to the submission date or modify terms and conditions identified in the Call.

9.2 Submission Dates and Times.

Submission dates and times will be identified in each Call. Proposals WILL NOT BE ACCEPTED after the established due date. There will be no exceptions to the time and date on which responses are due, unless otherwise determined by the Government.

9.3 No Classified Documents.

No classified proposals will be accepted.

9.4 Multiple Proposals.

If only proposals (no white papers) have been requested by the individual Call, then multiple proposals may be submitted. When white papers are requested by the individual Call, then offerors must submit a white paper to be considered for participation in the submission of proposals. Each submitted proposal must comply with the terms outlined herein.

9.5 Proposal Format.

Proposal submission formatting will be identified in the individual Calls.

- Assertion of Data Rights.
    - The Assertions Table completed in accordance with this section does not count against the page count for Volume 1 - Technical Proposals.
    - It is anticipated that the proposed Assertion of Data Rights will be incorporated in the resultant award instrument. To this end, proposals must include a severable Assertion of Data Rights (i.e., it will begin on a new page and the following section shall begin on a new page) without any proprietary restrictions, which can be removed from the proposal and attached to the contract or agreement award. After proposal submission, any changes to this information requested by an offeror may cause a proposal to be re-evaluated or deemed not selectable at the Government's discretion. The format for this section is as follows:

Assertions Table

Identify in the table below each deliverable included in the offeror's proposal. For each deliverable listed in the below table, identify any assertion of restriction on the Government's use, release or disclosure of technical data or computer software.

Deliverable	Technical Data or Computer Software to be Furnished With Restrictions*	Basis for Assertion**	Asserted Rights Category***	Name of Person Asserting Restrictions****

*For technical data (other than computer software documentation) pertaining to items, components, or processes developed at private expense, identify both the deliverable technical data and each such item, component, or process. For computer software or computer software documentation, identify the software or documentation.

**Generally, development at private expense, either exclusively or partially, is the only basis for asserting restrictions. For technical data, other than computer software documentation, development refers to development of the item, component, or process to which the data pertain. The Government's rights in computer software documentation generally may not be restricted. For computer software, development refers to the software. Indicate whether development was accomplished exclusively or partially at private expense. If development was not accomplished at private expense, enter the specific basis for asserting restrictions.

***Enter asserted rights category (e.g., government purpose rights, limited rights, restricted rights , or specially negotiated licenses).

****Corporation, individual, or other person, as appropriate, or enter "none" when all data or software will be submitted without restrictions.

Completed by:

_____ _____

Signature Date

Printed Name and Title

- Patents. All offerors must include documentation proving ownership or possession of appropriate licensing rights to all patented inventions to be used for the proposed project. If a patent application has been filed for an invention, but it includes proprietary information and is not publicly available, an offeror must provide documentation that includes: the patent number, inventor name(s), assignee names (if any), filing date, filing date of any related provisional application, and summary of the patent title, with either: (1) a representation of invention ownership, or (2) proof of possession of appropriate licensing rights in the invention (i.e., an agreement from the owner of the patent granting

license to the offeror).

- Company to Company Agreement with Noblis, Inc. (or successor SETA contractor). If white papers were not submitted for the Call, this Agreement shall be included in accordance with paragraph 11.4 and does not count against the proposal page count.

Price/Cost Proposal. Price/Cost Proposal will typically consist of a cover page and two parts, Part 1 and Part 2, and cover the following information:

- Cover Page. The words "Price/Cost Proposal" should appear on the cover page in addition to the following information:
    - Respective BAA Call number;
    - DHS S&T OIP Portal Assigned Proposal Number
    - Title of proposal;
    - Name of offeror's organization and offeror's administrative and technical points of contact, including name, address, telephone and facsimile numbers, and email addresses;
    - Whether offeror is U.S. or foreign owned entity;
    - Identity of prime offeror and complete list of subcontractors or consultants, if applicable, otherwise indicate that there are no subcontractors or consultants;
    - Duration of effort. Separately identify the base effort and any options;
    - In accordance with FAR 4.1201, prospective offerors for contracts and for OTs involving prototypes shall state the certifications in SAM database at https://www.sam.gov have been completed and shall provide the certification validity period; and
    - The signature and title of an authorized representative of the entity submitting the proposal.

- Part 1. As stated above in paragraph 4.5, submissions must propose periods of performance in line with the requirements of the BAA Call, not to exceed five (5) years in total. Therefore, Part 1 shall consist of a detailed breakdown of all costs by cost category identified by period of performance in which the costs are expected to occur (e.g., base period, option period 1, etc.). All contractor and subcontractor costs must be provided in United States Dollars (USD). Other currencies may be present in the cost proposal information, however conversion to USD must be included to show the rate of exchange. Cost categories include, at a minimum, the following:

- Direct Labor. Labor hours and ***unburdened*** direct labor rates for each person proposed.

- Indirect Costs Breakdown. Fringe Benefits, Overhead, General & Administrative (G&A), Cost of Money, etc.; ***must show amount and rate for each element.***

- Travel. Number of trips, destinations, durations, etc.

- Materials. Materials should be specifically itemized with costs or estimated costs. Where possible, indicate basis of estimate, (e.g., recent purchase of same or similar item, vendor quote, catalog price, engineering estimate, market survey, etc.).

- Other Directs Costs (ODCs). ODCs, particularly any proposed items of equipment or

facilities. Equipment and facilities generally must be furnished by the contractor/recipient. Justifications must be provided when Government funding for such items is sought.

Subcontract(s). A cost proposal ***<u>not less detailed than the Offeror's cost proposal</u>*** will be required to be submitted by the subcontractor. Costs should be clearly marked as "prime" or "subcontractor" costs. If the subcontractor costs cannot be included with the above detailed cost breakdown, then the prime contractor must stipulate on the detailed cost breakdown that the costs presented only represent those from the prime and the subcontractor's costs are provided separately as an attachment to an e-mail sent to *[location to be identified in each individual Call]*. The subject line of the email shall say "Separate Subcontractor Cost Submission – *[insert the white paper or proposal number assigned from the DHS S&T OIP Portal*." The body of the email shall contain the following:

- The prime entity's name which should be the same entity that is registered in the DHS S&T OIP Portal;
- A POC (name and phone number) from the prime entity; and
- For each subcontractor proposal attached, include:
  - The name of the subcontractor for the subcontractor proposal attached; and
  - A POC (name and phone number) from the subcontractor whose proposal is attached.
- The separate subcontractor cost proposal must be not less detailed than the offeror's cost proposal and must be received at the location designated in the individual Call no later than the closing date and time specified by the Call. Note that email transmission time may vary depending on the file size of the attachment(s) included in the email. Therefore, ensure there is adequate time for receipt of the email and any accompanying attachments of the subcontractor(s) cost proposal(s) by the required closing date and time. Acceptance of the email submission is dependent upon the actual date and time the e-mail and any accompanying attachment(s) is **RECEIVED** at the location designated in the Call. **NO SEPARATE SUBCONTRACTOR COST PROPOSALS RECEIVED WILL BE ACCEPTED IF RECEIVED AFTER THE CLOSING DATE AND TIME SPECIFIED IN EACH INDIVIDUAL CALL.**

- Consultant(s). Provide a consultant agreement or other document which verifies the proposed loaded daily/hourly rate.
- Fee/Profit. Identify amount and percentage of Fee/Profit, if proposed.

- <u>Part 2</u>. Part 2 shall consist of the cost breakdown by task/sub-task using the same task numbers in the Statement of Work (SOW). In addition, the task/sub-task breakdown must be identified by period of performance in which it is expected the costs/tasks/sub-tasks to occur (e.g., base period, option period 1, etc.).

9.6 Non-compliant Proposals.

Proposals submitted that do not comply with the proposal submission requirements outlined in this BAA and any additional submission requirements outlined in the Call the proposal is responding to may result in the proposal being determined non-compliant and rejected without evaluation. Examples of non-compliant proposals include, but are not limited to:

- Total contract value proposed in the proposal is greater than the boundaries identified in the respective Call;
- Total number of pages submitted does not comply with the page count limitations identified in the respective Call; or
- Pages within the proposal do not comply with the requirements for font sizes and margins identified in the respective Call; or
- Submission requirements are not met, such as the one-page limitation for the cover page, the transmittal letter, or the quad chart is exceeded, or no separate assertions table is provided, etc.

10. PROCEDURES FOR SUBMITTING WHITE PAPERS AND PROPOSALS IN THE DHS S&T Office of Industry Partnerships (OIP) Portal

10.1 Company/Organization Registration.

- **IMPORTANT**: Before submitting a white paper or proposal for the first time, you must first register your company/organization in the OIP Portal. 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), country and state it is registered in are 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 OIP Portal:
  - Go to the DHS S&T OIP Portal at https://oip.dhs.gov/
  - Click on the *Profile Login* icon in the top right corner of the OIP program portal landing page
  - To begin the registration process, check the box to agree to the Terms of Service and DHS Privacy Notice and then click *New User? Register as a public user here* icon at the top of the page.
- For additional step-by-step information regarding registration, on the OIP program home

page in the top navigation bar on the far right, click on *Resources*. On the next page, you can review FAQs or download a copy of the *Portal Registration and LRBAA Submission Guide* and review Section 2.

10.2 White Paper and Proposal Submissions.

- Each white paper, if requested, and proposal to be uploaded in the DHS S&T OIP Portal will be assigned a white paper and/or proposal number in the portal.
- To upload a white paper or proposal, after logging into the portal, click on the *Funding* menu in the navigation bar and select *Open Funding Opportunities*. On the following search page, click on the *TBAA* tab, locate the open topic of interest and click on *Apply*.

10.3 DHS S&T OIP Portal Technical Support.

For any technical assistance with the DHS S&T OIP Portal, you can contact the DHS S&T OIP Portal Technical Support at OIPPortalHelpDesk@hq.dhs.gov or by phone at (571) 446-4869. Support hours are Monday through Friday, 9:00AM to 5:00PM.

11. EVALUATION OF WHITE PAPERS AND PROPOSALS

11.1 General.

Any submitted white papers and proposals that do not comply with the requirements of this BAA and the individual Call issued under the BAA may be rejected as non-compliant.

The evaluation of all white papers and proposals received that are compliant with the requirements of this BAA and the respective Call issued under this BAA will be accomplished through a technical review panel using the evaluation criteria specified below.

11.2 Evaluation Criteria.

The evaluation criteria anticipated to be used for the technical review of both white papers and proposals received in response to each Call issued under this BAA are identified below in descending order of importance. These evaluation criteria will be used unless a Call modifies or changes them.

Criterion I: **Quality and Technical Merit:** Presentation of a sound technical and managerial approach to the proposed work that demonstrates a clear, reasonable, and responsive path to provide a solution to the problem presented by each Topic Area associated with the planned 5-year BAA. DHS will assess the soundness of the Offeror's technical and managerial approach to the proposed work and whether the approach demonstrated is reasonable and responsive to the program requirements; demonstrates an understanding of the problem; clearly identifies all risks and associated mitigation approaches; and presents a clear plan and schedule to provide a solution to the problem presented by each Topic Area associated with the planned 5-year BAA.

Criterion II: **Capabilities and Experience**: Demonstration of the qualifications, capabilities and experience needed to achieve the proposal objectives. DHS will assess the Offeror's qualifications, capabilities, and experience to determine if the proposed team has sufficient

expertise to perform the proposed work, manage the project cost, and complete the project within the proposed schedule to achieve the proposed objectives.

Criterion III: Cost Reasonableness[1]:

- White Papers. The cost evaluation factor for white papers, when requested, is as follows: "Cost. White papers will be evaluated on the reasonableness and affordability of proposed technical work."

  Proposals. Offerors must present accurate, well-founded estimates of all costs related to performance of the proposed effort. Costs of the proposal must be reasonable and provide a high value to the Government. The proposed costs are reasonable (i.e., reflect a sufficient understanding of the technical goals and objectives of the Topic Area, and are consistent with the Offeror's technical/management approach, to include the proposed SOW), and are based on reasonable assumptions. An assessment will be made of the offeror's proposed costs as to whether they are reasonable for the solution proposed.

11.3 Basis for Phase I and Phase II Selection.

- The primary basis for identifying Phase I submissions as encouraged to submit Phase II responses, and for selecting responses for award shall be the evaluation criteria listed in 11.2 and funding availability. Cost reasonableness and completeness shall also be considered to the extent appropriate.
- DHS S&T reserves the right to select for award and to fund all, some, or none of the proposals received in response to any Calls issued against this BAA.

11.4 Confidence Ratings.
Unless otherwise identified in a BAA Call, awards will be evaluated using the following confidence ratings:

Confidence Ratings	
Rating	Definition
High	The Government has high confidence that the Quoter understands the requirement, proposes a sound approach, and will be successful in performing the contract with little or no Government intervention.
Some	The Government has some confidence that the Quoter understands the requirement, proposes a sound approach, and will be successful in performing the contract with some Government intervention.
Low	The Government has low confidence that the Quoter understands the requirement, proposes a sound approach, and will be successful in performing the contract even with Government intervention.

[1] The Government will evaluate Cost Realism prior to making any cost type awards.

11.5 Evaluation Panel.

All properly submitted Phase I and Phase II submissions that conform to the BAA requirements will be evaluated by a review panel comprised of Government technical experts drawn from staff within DHS S&T and other federal agencies. All Government personnel are bound by public law to protect proprietary information.

Important Note: DHS intends to use Noblis, Inc. (or successor SETA contractor) for routine administrative and/or technical support during the evaluation process of both Phase I and Phase II. 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 Phase I submission (or with their proposal submission if white papers are not required). 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 the BAA Call Contracting Officer and Contract Specialist and indicate "NDA" in the Subject line. Offerors are encouraged to allow sufficient time to permit agreement execution.

- Offerors are advised that employees of Noblis, Inc. may serve as administrative and/or technical support to Source Selection Evaluation Board (SSEB) members in the source selection process. These individuals will be authorized access to only those portions of proposal data and discussions that are necessary to enable them to perform their respective duties. Noblis Inc. is expressly prohibited from competing on the subject acquisition and from scoring or rating white papers and proposals or recommending the selection of a proposal for funding. Contractor personnel will not provide subject matter expertise to the SSEB unless the OPO HCA signs a D&F allowing for this support.
- In accomplishing their duties related to the source selection process, Noblis, Inc. employees may require access to proprietary information contained in the offerors' white papers and proposals. Therefore, pursuant to FAR 9.505-4, Noblis, Inc. must execute an agreement with each offeror that states that they will (1) protect the offeror's information from unauthorized use or disclosure for as long as it remains proprietary, and (2) refrain from using the information for any purpose other than that for which it was furnished. To expedite the evaluation process, each offeror must contact Noblis, Inc. to effect execution of an Agreement prior to submission of white papers. Each offeror shall submit copies of the Agreement with its white paper.
- The Noblis, Inc. POC will only address questions relevant to the Company to Company Agreement.

Foreign Government Participation. As stated in paragraph 1.3 above, DHS S&T intends to have foreign government participation in the selection process as technical reviewers of submitted white papers and/or proposals, foreign government access to white papers and proposals for purposes of determining joint-funding, and joint participation (U.S. and foreign government) in overseeing projects throughout the contract period of performance. The following foreign government participation may include the following international partners: (a) the United Kingdom of Great Britain and Northern Ireland; (b) the Government of Australia; (c) the Government of Canada; (d) the Kingdom of the Netherlands; (e) the European Union; (f) the

Government of Germany; (g) the Government of Israel; (h) the Kingdom of Sweden; (i) the Government of New Zealand; and (j) the Government of Singapore.

11.6 Notification to Offerors of Evaluation Findings.

Once the Phase I technical review process is complete, offerors will be notified via e- mail or in writing, whether the offeror is "encouraged" or "not encouraged" to move to Phase II. Offerors not encouraged to move to Phase II are not prohibited from Phase II. All timely Phase II submissions received will be included in the technical review process.

11.6.1 Once the Phase II technical review process is complete, offerors will be notified via e-mail or in writing that its proposal has been selected, selected but not funded, or not selected for award.

For those proposals that are selected but are on hold for funding, offerors will be so advised and asked to confirm that their proposals remain valid for funding for a time specified in the notification letter.

11.6.2 Offerors Feedback. Offerors not selected for an award may request feedback regarding the technical review findings of submitted proposals. A written request to the Contracting Officer must be received within three calendar days of notification of non-selection. Feedback will not be provided on submitted white papers, or proposals that have been selected or selected but not funded for award.

12. OTHER TERMS AND CONDITIONS

12.1 NAICS.

The North American Industry Classification System (NAICS) code for this announcement and any Calls issued against this BAA is 541715, with a small business size standard of 1,000 employees.

12.2 System for Award Management (SAM).

Successful offerors not already registered in the SAM will be required to register in the SAM prior to award of any contract, cooperative agreement, or OT, if authorized by law at time of award. Information regarding SAM registration is available at https://www.sam.gov.

12.3 Information for Respondents.

This BAA is for planning purposes only. It will not be construed as an obligation on the part of the Government to acquire any products or services.

No entitlement to payment of direct or indirect costs or charges by the Government will arise as a result of submission of responses to any Calls issued against this BAA and the Government's use of such information. Respondents to any Calls issued against this BAA may be requested to provide additional information based on their submittals. Unnecessarily elaborate responses containing extensive marketing materials are not desired.

Technical and cost proposals, or any other material, submitted in response to any Calls issued against this BAA will not be returned.

12.4 Organizational Conflict of Interest.

Offerors who have existing or pending contract(s) to provide scientific, engineering, technical and/or administrative support directly to DHS S&T may be considered to have actual or potential conflict of interest, resulting in one or more offerors with the potential to attain an unfair competitive advantage.

If any such conflict of interest is found to exist, the Contracting Officer may (1) disqualify the offeror, or (2) determine that it is otherwise in the best interest of the United States to contract with the offeror and include the appropriate provisions to mitigate or avoid such conflict in the contract awarded. After discussion with the offeror, the Contracting Officer may determine that the actual conflict cannot be avoided, neutralized, mitigated, or otherwise resolved to the satisfaction of the Government, and the offeror may be found ineligible for award.

Disclosure. Each offeror will be required to represent, as part of its proposal and to the best of its knowledge that: (1) It is not aware of any facts which create any actual or potential organizational conflicts of interest relating to the award of this contract; or (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential organizational conflicts of interest, and has included the mitigation plan in accordance with the paragraph below, titled: Mitigation/Waiver.

Mitigation/Waiver. If an offeror with a potential or actual conflict of interest or unfair competitive advantage believes it can be mitigated, neutralized, or avoided, the offeror shall submit a mitigation plan to the Contracting Officer for review. Award of a contract where an actual or potential conflict of interest exists shall not occur before Government approval of the mitigation plan.

Other Relevant Information. In addition to the mitigation plan, the Contracting Officer may require further relevant information from the offeror. The Contracting Officer will use all information submitted by the offeror, and any other relevant information known to DHS, to determine whether an award to the offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.

Corporation Change. The successful offeror shall inform the Contracting Officer within 30 calendar days of the effective date of any corporate mergers, acquisitions, and/or divestures that may affect this clause.

Flow-down. The contractor shall insert the substance of this clause in each first-tier subcontract that exceeds the simplified acquisition threshold.

12.5 Export Control.

Offerors are advised that the export of any goods or technical information from the United States, and the disclosure of technical information to foreign nationals, may require some form of export authorization from the U.S. Government. Failure to obtain necessary export authorization may result in criminal liability of offerors under U.S. laws.

Offerors are responsible for ensuring compliance with the International Traffic in Arms Regulations administered by the U.S. Department of State (22 C.F.R. Parts 120 to 130), Export Administration Regulations administered by the U.S. Department of Commerce (15 C.F.R. Parts 730 to 774), and Foreign Assets Control Regulations administered by the U.S. Department of Treasury (31 C.F.R. Parts 501 to 598), as warranted, and compliance with all recordkeeping

requirements under U.S. export regulations. Offerors are responsible for compliance with any applicable export license, authorization, reporting, or other preapproval requirements by the U.S. Government. DHS neither represents that a license, authorization, or preapproval shall not be required nor that, if required, it shall be issued. Nothing granted herein to offerors provides any such export license or other preapproval.

Offerors shall identify any anticipated export compliance issues in their response to the Call. Specifically, offerors are advised to include information in their response regarding any known equipment, software or technical information that will be developed as a result of work to be performed that is subject to export control restrictions.

To the extent that export-controlled information may be provided to DHS by offerors in response to a Call, offerors are responsible for ensuring that such information is appropriately marked and are responsible for complying with all applicable export controls and regulations in the process of providing such information.

12.6 Intellectual Property.

It is desired that all noncommercial software (including source code), software documentation, hardware designs and documentation, and technical data generated under the project be provided as a deliverable with unlimited rights for the Government, or delivered with a mutually agreed to open source license. DHS intends to allow and encourage offerors the opportunity to transition their proposed technologies to the commercial marketplace or other Government entities. The reason for this position is that while DHS would prefer that an offeror commercialize or transition the technology they develop, DHS wants to ensure that it has the right to commercialize or otherwise leverage its technology investments should an offeror choose not to or not have success.

All references to "Unlimited Rights" are intended to refer to the definition set forth in the Federal Acquisition Regulation (FAR) 52.227-14, Rights in Data-General clause.

Specific Intellectual Property terms and conditions will be negotiated for each individual contract award.

12.7 Publication of Research Results and Award Information.

As noted in this BAA, resultant contract awards may involve joint, United States and foreign country (as identified in paragraph 1.3 above) funding, pursuant to each country's bilateral, international agreement. To ensure the rights of these international agreements are secured, the following terms and conditions regarding publication of research results will apply to each contract awarded, where DHS plans to apply foreign co-funding, as a result of this BAA:

- Limitation on Contractor's Use of Data. For the purposes of paragraphs (b) (2) (i) and (d) of the Rights in Data-General (FAR 52.227-14) clause of this contract, the Contractor shall not use, release to others, reproduce, distribute, or publish any data first produced or specifically used in the performance of this contract for private purposes (to include publications) without the prior, written approval of the Contracting Officer.
- Publication of Research Results.
    - For publication of materials based, in whole or part, on data first produced under this contract, the Contractor shall transmit a copy to the DHS Program Manager and Contracting Officer at least **60 days prior** to such desired publication for

review by DHS and any other foreign government co-funding the award. In all cases, the Contractor shall supply two copies of the final publications to DHS, in accordance with the requirements of the individual contract award.

- Any copy of material published under this clause shall contain acknowledgment of DHS's sponsorship of the research effort and a disclaimer stating that the published material represents the position of the author(s) and not necessarily that of DHS.
- Publication under the terms of this clause does not release the Contractor from the obligation of preparing and submitting to the Contracting Officer a final report containing the findings and results of research, as set forth in the schedule of the contract.

Once an Offeror has been notified that they have been selected for funding, all publication of information of that status, to include press releases and award announcements, are subject to the constraints and processes of HSAR 3052.205-70 Advertisements, Publicizing Awards, and Releases (Sept 2012).

12.8 Adequate Accounting System for Cost Reimbursement Type Contracts.

In order to qualify for the award of a cost reimbursement type contract, the offeror must have an adequate accounting system in accordance with FAR 16.301-3(a)(3). If a proposal is selected, the offeror will be required to provide evidence of an adequate accounting system before a cost reimbursement contract will be considered.

Evidence of an adequate accounting system would include a written opinion or other statement from the cognizant federal auditor (CFA) or the cognizant federal agency official (CFAO) that the system is approved or has been determined to be adequate. If available, the offeror will be requested to provide the audit report number and date associated with the accounting system review. If the offeror does not have a copy of the report, the offeror may furnish a copy of the audit report number.

If the offeror does not have an accounting system that has been determined adequate by the CFA or CFAO, but believes its accounting system is adequate, the offeror shall so state in its response to the Government's request for evidence of an adequate accounting system. As part of the pre-award evaluation process, the Government will obtain the necessary review by the CFA. The offeror will be required to allow the CFA to review the accounting system and correct (or have a timely action plan to correct) any issues identified as precluding the system from being adequate. The offeror will provide the CFA name, address and telephone number and the point of contact as part of its proposal.

Offers will be rejected if the offeror does not have an adequate accounting system, unless the Government determines that the Offeror‘s action plan for correcting the accounting system is timely and acceptable. However, no costs will be paid under the contract until the Contractor's system has been determined adequate.

12.9 Certificate of Current Cost or Pricing Data.

Successful contract proposals will require the submission of a Certificate of Current Cost or Pricing Data in accordance with FAR 15.403- 4(b)(2), prior to award.

12.10 Applicable Provisions and Contract Clauses.

At the time of any award resulting from any Call issued against this BAA, excluding cooperative agreements and OTs, all FAR and Homeland Security Acquisition Regulation (HSAR) provisions and clauses applicable to the resultant award will be included in the selected offeror's contract. DHS S&T will comply with the requirements of DHS's final rule on Safeguarding of Controlled Unclassified Information (CUI) and the HSAM Appendix G Controlled Unclassified Information Checklist for individual awards under this BAA. Accordingly, the clauses below may apply to individual Calls and awards under this BAA.

FAR 52.224-3 Privacy Training – Alternate I (DEVIATION) (July 2023)

(a) *Definition.* As used in this clause, personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) Circular A–130, Managing Federal Information as a Strategic Resource).

(b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who—

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or

(3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.1 and 39.105).

(c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract. Contractor employees shall satisfy this requirement by completing *Privacy at DHS: Protecting Personal Information* accessible at *http://www.dhs.gov/dhs-security-and-training-requirements-contractors*. Training shall be completed within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year.

(d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.

(e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.

(f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will—

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information; or

(3) Design, develop, maintain, or operate a system of records.

(End of clause)

HSAR 3052.204-71 CONTRACTOR EMPLOYEE ACCESS (JULY 2023)

(a) *Controlled Unclassified Information (CUI)* is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. This definition includes the following CUI categories and subcategories of information:

(1) Chemical-terrorism Vulnerability Information (CVI) as defined in 6 CFR part 27, "Chemical Facility Anti-Terrorism Standards," and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual "Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information" dated September 2008);

(2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through Pub. L. 116–283), PCII's implementing regulations (6 CFR part 29), the PCII Program Procedures Manual, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security, the PCII Program Manager, or a PCII Program Manager Designee;

(3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, "Protection of Sensitive Security Information," 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 designee), including Department of Homeland Security MD 11056.1, "Sensitive Security Information (SSI)" and, within the Transportation Security Administration, TSA MD 2810.1, "SSI Program";

(4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local, Tribal, territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing

consistent with the Cybersecurity Information Sharing Act of 2015;

(5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;

(6) International Agreement Information means information the Department of Homeland Security receives that is required to be protected by an information sharing agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization;

(7) Information Systems Vulnerability Information (ISVI) means:

(i) Department of Homeland Security information technology (IT) systems data revealing infrastructure used for servers, desktops, and networks; applications name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission or business use/need. Examples of ISVI are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526 will be classified as appropriate; and/or

(ii) Information regarding developing or current technology, the release of which could hinder the objectives of the Department, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system;

(8) Operations Security Information means Department of Homeland Security information that could be collected, analyzed, and exploited by a foreign adversary to identify intentions, capabilities, operations, and vulnerabilities that threaten operational security for the missions of the Department;

(9) Personnel Security Information means information that could result in physical risk to Department of Homeland Security personnel or other individuals whom the Department is responsible for protecting;

(10) Physical Security Information means reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of Federal buildings, grounds, or property. For example, threat assessments, system security plans, contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation;

(11) Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used

to distinguish or trace an individual's identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(ii) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(A) Truncated SSN (such as last 4 digits);
(B) Date of birth (month, day, and year);
(C) Citizenship or immigration status;
(D) Ethnic or religious affiliation;
(E) Sexual orientation;
(F) Criminal history;
(G) Medical information; and
(H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(iii) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

(b) *Information Resources* means information and related resources, such as personnel, equipment, funds, and information technology.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted or subject to other investigations as required. All Contractor employees requiring recurring access

to government facilities or access to CUI or information resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to CUI. The Contractor shall access and use CUI only for the purpose of furnishing advice or assistance directly to the Government in support of the Government's activities, and shall not disclose, orally or in writing, CUI for any other purpose to any person unless authorized in writing by the

Contracting Officer. For those Contractor employees authorized to access CUI, the Contractor shall ensure that these persons receive initial and refresher training concerning the protection and disclosure of CUI. Initial training shall be completed within 60 days of contract award and refresher training shall be completed every 2 years thereafter.

(f) The Contractor shall include this clause in all subcontracts at any tier where the subcontractor may have access to government facilities, CUI, or information resources.

(End of clause)

ALTERNATE I
(JULY 2023)

When the contract will require Contractor employees to have access to information resources, add the following paragraphs:

(g) Before receiving access to information resources under this contract, the individual must complete a security briefing; additional training for specific categories of CUI, if identified in the contract; and any nondisclosure agreement furnished by DHS. The Contracting Officer's Representative (COR) will arrange the security briefing and any additional training required for specific categories of CUI.

(h) The Contractor shall have access only to those areas of DHS information resources explicitly stated in this contract or approved by the COR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information resources not expressly authorized by the terms and conditions in this contract, or as approved in writing by the COR, are strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for DHS. It is not a right, a guarantee of access, a condition of the contract, or government-furnished equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The Contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management, or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) There must be a compelling reason for using this individual as opposed to a U.S. citizen; and

(2) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the Contracting Officer.

(End of clause)

ALTERNATE II
(JULY 2023)

When the Department has determined contract employee access to controlled unclassified information or Government facilities must be limited to U.S. citizens and lawful permanent residents, but the contract will not require access to information resources, add the following paragraphs:

(g) Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident Card (USCIS I-551). Any exceptions must be approved by the Department's Chief Security Officer or designee.

(h) Contractors shall identify in their proposals, the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

(End of clause)

HSAR 3052.204-72 SAFEGUARDING OF CONTROLLED UNCLASSIFIED INFORMATION (JULY 2023)

(a) *Definitions*. As used in this clause—

Adequate Security means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This

includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.

Controlled Unclassified Information (CUI) is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. This definition includes the following CUI categories and subcategories of information:

(1) Chemical-terrorism Vulnerability Information (CVI) as defined in 6 CFR part 27, "Chemical Facility Anti-Terrorism Standards," and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual "Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information" dated September 2008);
(2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through Pub. L. 116–283), PCII's implementing regulations (6 CFR part 29), the PCII Program Procedures Manual, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security, the PCII Program Manager, or a PCII Program Manager Designee;

(3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, "Protection of Sensitive Security Information," 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 designee), including Department of Homeland Security MD 11056.1, "Sensitive Security Information (SSI)" and, within the Transportation Security Administration, TSA MD 2810.1, "SSI Program";

(4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local, Tribal, territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015;

(5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;

(6) International Agreement Information means information the Department of Homeland Security receives that is required to be protected by an information sharing agreement or arrangement with a foreign government, an international organization of governments or any

element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization;

(7) Information Systems Vulnerability Information (ISVI) means:

(i) Department of Homeland Security information technology (IT) systems data revealing infrastructure used for servers, desktops, and networks; applications name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission or business use/need. Examples of ISVI are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526 will be classified as appropriate; and/or

(ii) Information regarding developing or current technology, the release of which could hinder the objectives of the Department, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system;

(8) Operations Security Information means Department of Homeland Security information that could be collected, analyzed, and exploited by a foreign adversary to identify intentions, capabilities, operations, and vulnerabilities that threaten operational security for the missions of the Department;

(9) Personnel Security Information means information that could result in physical risk to Department of Homeland Security personnel or other individuals whom the Department is responsible for protecting;

(10) Physical Security Information means reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of Federal buildings, grounds, or property. For example, threat assessments, system security plans, contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation;

(11) Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or trace an individual's identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, the DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security

numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(ii) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(A) Truncated SSN (such as last 4 digits);
(B) Date of birth (month, day, and year);
(C) Citizenship or immigration status;
(D) Ethnic or religious affiliation;
(E) Sexual orientation;
(F) Criminal history;
(G) Medical information; and
(H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(iii) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

Federal information means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

Federal information system means an information system used or operated by an agency or by a Contractor of an agency or by another organization on behalf of an agency.

Handling means any use of controlled unclassified information, including but not limited to marking, safeguarding, transporting, disseminating, re-using, storing, capturing, and disposing of the information.

Incident means an occurrence that—

(1) Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

(2) Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Information Resources means information and related resources, such as personnel, equipment, funds, and information technology.

Information Security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(1) Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

(2) Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(3) Availability, which means ensuring timely and reliable access to and use of information.

Information System means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

(b) *Handling of Controlled Unclassified Information.*

(1) Contractors and subcontractors must provide adequate security to protect CUI from unauthorized access and disclosure. Adequate security includes compliance with DHS policies and procedures in effect at the time of contract award. These policies and procedures are accessible at https://www.dhs.gov/dhs-security-and-training- requirements-contractors.

(2) The Contractor shall not use or redistribute any CUI handled, collected, processed, stored, or transmitted by the Contractor except as specified in the contract.

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

(4) Any government data provided, developed, or obtained under the contract, or otherwise under the control of the Contractor, shall not become part of the bankruptcy estate in the event a Contractor and/or subcontractor enters bankruptcy proceedings.

(c) *Incident Reporting Requirements.*

(1) Contractors and subcontractors shall report all known or suspected incidents to the Component Security Operations Center (SOC) in accordance with Attachment F, *Incident Response*, to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems*. If the Component SOC is not available, the Contractor shall report to the DHS Enterprise SOC. Contact information for the DHS Enterprise SOC is accessible at https://www.dhs.gov/dhs-security-and-training- requirements-contractors. Subcontractors are required to notify the prime Contractor that it has reported a known or suspected incident to the Department. Lower tier subcontractors are required to likewise notify their higher tier subcontractor, until the prime contractor is reached. The Contractor shall also notify the Contracting Officer and COR using the contact information identified in

the contract. If the report is made by phone, or the email address for the Contracting Officer or COR is not immediately available, the Contractor shall contact the Contracting Officer and COR immediately after reporting to the Component or DHS Enterprise SOC.

(2) All known or suspected incidents involving PII or SPII shall be reported within 1 hour of discovery. All other incidents shall be reported within 8 hours of discovery.

(3) CUI transmitted via email shall be protected by encryption or transmitted within secure communications systems. CUI shall be transmitted using a *FIPS 140-2/140-3 Security Requirements for Cryptographic Modules* validated cryptographic module identified on https://csrc.nist.gov/projects/cryptographic-module-validation- program/validated-modules. When this is impractical or unavailable, for Federal information systems only, CUI may be transmitted over regular email channels. When using regular email channels, Contractors and subcontractors shall not include any CUI in the subject or body of any email. The CUI shall be included as a password-protected attachment with the password provided under separate cover, including as a separate email. Recipients of CUI information will comply with any email restrictions imposed by the originator.

(4) An incident shall not, by itself, be interpreted as evidence that the Contractor or Subcontractor has failed to provide adequate information security safeguards for CUI or has otherwise failed to meet the requirements of the contract.

(5) If an incident involves PII or SPII, in addition to the incident reporting guidelines in Attachment F, *Incident Response*, to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems*, 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) Unique Entity Identifier (UEI);
(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, and email);
(v) Contracting Officer POC (address, telephone, and email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms, or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where CUI resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the government PII or SPII contained within the system; and
(xiii) Any additional information relevant to the incident.

(d) *Incident Response Requirements.*

(1) All determinations by the Department related to incidents, including response activities, will be made in writing by the Contracting 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 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;
(iv) Data analyses and processing; and
(v) Revocation of the Authority to Operate (ATO), if applicable.

(4) The Contractor shall immediately preserve and protect images of known affected information systems and all available monitoring/packet capture data. The monitoring/packet capture data shall be retained for at least 180 days from submission of the incident report to allow DHS to request the media or decline interest.

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

(e) *Certificate of Sanitization of Government and Government-Activity-Related Files and Information.* Upon the conclusion of the contract by expiration, termination, cancellation, or as otherwise indicated in the contract, the Contractor shall return all CUI to DHS and/or destroy it physically and/or logically as identified in the contract unless the contract states that return and/or destruction of CUI is not required. Destruction shall conform to the guidelines for media sanitization contained in NIST SP 800–88, *Guidelines for Media Sanitization*. The Contractor shall certify and confirm the sanitization of all government and government-activity related files and information. The

Contractor shall submit the certification to the COR and Contracting Officer following the template provided in NIST SP 800–88, *Guidelines for Media Sanitization*, Appendix G.

(f) *Other Reporting Requirements.* Incident reporting required by this clause in no way rescinds the Contractor's responsibility for other incident reporting pertaining to its unclassified information systems under other clauses that may apply to its contract(s), or as a result of other applicable statutory or regulatory requirements, or other U.S. Government requirements.

(g) *Subcontracts.* The Contractor shall insert this clause in all subcontracts and require subcontractors to include this clause in all lower tier subcontracts when subcontractor

employees will have access to CUI; CUI will be collected or maintained on behalf of the agency by a subcontractor; or a subcontractor information system(s) will be used to process, store, or transmit CUI.

(End of clause)

ALTERNATE I (JULY 2023)

When Federal information systems, which include Contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI, add the following paragraphs:

(h) *Authority to Operate*. The Contractor shall not collect, process, store, or transmit CUI within a Federal information system until an ATO has been granted by the Component or Headquarters CIO, or designee. Once the ATO has been granted by the Government, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. Unless otherwise specified in the ATO letter, the ATO is valid for 3 years. An ATO is granted at the sole discretion of the Government and can be revoked at any time. Contractor receipt of an ATO does not create any contractual right of access or entitlement. The Government's grant of an ATO does not alleviate the Contractor's responsibility to ensure the information system controls are implemented and operating effectively.

(1) *Complete the Security Authorization process.* The Security Authorization (SA) process shall proceed according to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems* (Version 13.3, February 13, 2023), or any successor publication; and the *Security Authorization Process Guide*, including templates. These policies and templates are accessible at https://www.dhs.gov/dhs-security-and-training-requirements-contractors.

(i) *Security Authorization Package*. The SA package shall be developed using the government-provided Security Requirements Traceability Matrix and SA templates. The SA package 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). The Contractor shall submit a signed copy of the SA package, validated by an independent third party, to the COR for review and approval by the Component or Headquarters CIO, or designee, at least 30 days prior to the date of operation of the information system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of modified documents.

(ii) *Independent Assessment*. Contractors shall have an independent third party validate the security and privacy controls in place for the information 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 SP 800–53, *Security and Privacy Controls for Information Systems and Organizations*, or successor publication, accessible at *https://csrc.nist.gov/publications/sp*. The Contractor shall address all deficiencies before submitting the SA package to the COR for review.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the Contractor shall renew the ATO every 3 years. The Contractor is required to update its SA package as part of the ATO renewal process for review and verification of security controls. Review and verification of security controls is independent of the system production date and may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place. The updated SA package shall be submitted for review and approval by the Component or Headquarters CIO, or designee, at least 90 days before the ATO expiration date. The Contractor shall update its SA package by one of the following methods:

(i) Updating the SA package in the DHS Information Assurance Compliance System; or
(ii) Submitting the updated SA package directly to the COR.

(3) *Security Review.* The Government may elect to conduct periodic reviews to ensure that the security requirements contained in the contract are being implemented and enforced. The Government, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in security review activities. The Contractor shall afford DHS, the Office of the Inspector General, other government organizations, and Contractors working in support of the Government access to the Contractor's facilities, installations, operations, documentation, databases, networks, systems, and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Component or Headquarters CIO, or designee, to coordinate and participate in review and inspection activity by government organizations external to DHS. Access shall be provided, to the extent necessary as determined by the Government (including providing all requested images), 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) *Federal Reporting and Continuous Monitoring Requirements.* Contractors operating information systems on behalf of the Government shall comply with Federal reporting and information system continuous monitoring requirements. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2015 DHS Information Security Performance Plan, or successor publication, accessible at https://www.dhs.gov/dhs-security-and-training- requirements-contractors. The plan is updated on an annual basis. Annual, quarterly, and monthly data collection will be coordinated by the Government. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for information systems. The Contractor shall provide the COR with requested information within 3 business days of receipt of the request. Unless otherwise specified in the contract, monthly continuous monitoring data shall be stored at the Contractor's location for a period not less than 1 year from the date the data are created. The Government may elect to perform information system continuous monitoring and IT security scanning of information systems from government tools and infrastructure.

(End of clause)

HSAR 3052.204-73 NOTIFICATION AND CREDIT MONITORING REQUIREMENTS FOR PERSONALLY IDENTIFIABLE INFORMATION INCIDENTS (JULY 2023)

(a) *Definitions.* Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or trace an individual's identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, the DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(1) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(2) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(i) Truncated SSN (such as last 4 digits);
(ii) Date of birth (month, day, and year);
(iii) Citizenship or immigration status;
(iv) Ethnic or religious affiliation;
(v) Sexual orientation;
(vi) Criminal history;
(vii) Medical information; and
(viii) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(3) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

(b) *PII and SPII Notification Requirements.*

(1) No later than 5 business days after being directed by the Contracting Officer, or as otherwise

required by applicable law, the Contractor shall notify any individual whose PII or SPII was either under the control of the Contractor or resided in an information system under control of the Contractor at the time the incident occurred. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by, the Contracting Officer. The Contractor shall not proceed with notification unless directed in writing by the Contracting Officer.

(2) All determinations by the Department related to notifications to affected individuals and/or Federal agencies and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer.

(3) Subject to government analysis of the incident and direction 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 or 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, mitigate the incident, and protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(c) *Credit Monitoring Requirements.* The Contracting Officer may direct the Contractor to:

(1) Provide notification to affected individuals as described in paragraph (b).

(2) Provide credit monitoring services to individuals whose PII or SPII was under the control of the Contractor or resided in the information system at the time of the 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.

(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 Frequently Asked Questions, approved in writing by the Contracting Officer in coordination with the Component or Headquarters Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(End of clause)

INFORMATION TECHNOLOGY SECURITY AWARENESS TRAINING (JULY 2023)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor 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.

(End of clause)

12.11 Government Property, Government Furnished Equipment (GFE) and Facilities.

The Government may provide government-furnished equipment (GFE), resources (GFR), information (GFI), or services (GFS) under the terms of each negotiated contract or agreement. GFE, GFR, GFI, or GFS requested by an offeror must be factored into the offeror's project cost. Each offeror must provide a very specific description of any equipment or hardware it needs to acquire to perform the work. This description should indicate whether or not each particular piece of equipment or hardware will be included as part of a deliverable item under the resulting award.

In addition, this description should identify the component, nomenclature, and configuration of the equipment or hardware that it proposes to purchase for this effort. The Government wants to have the contractor purchase the equipment or hardware for deliverable items under its contract. It will evaluate case-by-case the purchase, on a direct reimbursement basis, of special test equipment or other equipment, not included in a deliverable item. Maximum use of Government integration, test, and experiment facilities is encouraged in each of the Offeror's proposals.

Government research facilities may be available and should be considered as potential GFE. These facilities and resources are of high value, and some are in constant demand by multiple programs. The use of these facilities and resources will be negotiated as the program unfolds. Offerors should explain which of these facilities they recommend and why.

If any prototype, instrument or device is produced during the period of performance of a funded project, one or more samples shall be delivered to DHS S&T before the end of the period of performance for demonstration purposes. More specific information about the provision of a sample(s) will be incorporated in the SOW.

12.12 SAFETY Act.

As part of the Homeland Security Act of 2002, Congress enacted the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the "SAFETY Act"). The SAFETY Act puts limitations on the potential liability of firms that develop and provide qualified anti-terrorism technologies. DHS S&T, acting through its Office of SAFETY Act Implementation (OSAI), encourages the development and deployment of anti-terrorism technologies by making available the SAFETY Act's system of "risk management" and "liability management." Offerors submitting proposals in response to this BAA are encouraged to submit SAFETY Act applications for their existing technologies. They are invited to contact OSAI for more information, at 1-866-788-9318 or helpdesk@safetyact.gov. They also can visit OSAI's Web site at www.safetyact.gov.

12.13 Security Classification.

No classified documents will be accepted.

12.14 Subcontracting Plan.

Successful contract proposals that exceed $750,000.00, submitted by all but small business concerns, will be required to submit a Small Business Subcontracting Plan in accordance with FAR 52.219-9, prior to award. In the event an offeror required to submit a Small Business Subcontracting Plan determines there are no subcontracting possibilities, then the offeror must provide rationale as to why there are no subcontracting possibilities for any of the elements of costs identified in the offeror's proposal.

12.15 Additional Deliverables.

Performers should define additional program-specific deliverables as appropriate for the proposed approach. The Government may describe additional deliverables at the time proposals are requested.

12.16 Types of Changes That May Occur to Awards Under This BAA.

Types of changes that may occur to awards made under this BAA are:

Additional deliverables may be necessary once the Government develops the specific requirement based on the proposal received from the offeror. As a result, deliverables other than those identified by the offeror may be identified in the specific SOW included in the subsequent contract award.

During the performance of any contract, should the research result in the need to perform a different effort to achieve the solution due to the realization that the effort proposed will not provide the intended end result, the contract may be modified to reflect the necessary effort to achieve the goal of the contract. It is expected this modification will result in no change to the estimated cost of the contract. However, if additional costs are necessary, the Government will make a determination whether to proceed with the requirement or to terminate the contract due to insufficient funds to achieve the contract goal.

12.17 Reporting.

Specific reporting requirements will be included in each award. At a minimum, there will be three types of status reports: an annual report summarizing accomplishments and shortfalls throughout the year; a monthly financial report; and a monthly technical report providing detailed accomplishments and shortfalls throughout the previous month. These shall be required irrespective of award mechanism.

Appendix A. Company to Company Agreement

COMPANY TO COMPANY AGREEMENT

COMPANY TO COMPANY AGREEMENT: DHS BROAD AGENCY ANNOUNCEMENT (BAA) 70RSAT22RB00000001

The Parties to the subject Agreement agree that Noblis (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