

**Project: Public Safety and Violence Prevention
Broad Agency Announcement (BAA)
Call 0002
Under BAA 70RSAT21RB00000004**

1.Introduction

- 1.1. This BAA Call solicitation 0002 is a Call issued under Department of Homeland Security (DHS), Science & Technology Directorate (S&T), 5-Year Broad Agency Announcement (BAA) 70RSAT21RB00000004 “Public Safety and Violence Prevention (PSVP).” All terms and conditions of the DHS S&T 5-Year PSVP BAA 70RSAT21RB00000004 apply to this solicitation unless otherwise noted herein.
- 1.2. This Call has a two phased structure. Phase 1 is White Paper submission. Phase 2 is Full Proposal submission. Offerors must complete Phase 1 in order to participate in Phase 2. A separate Call will not be issued for Phase 2. The Government may award more than one contract for each Technical Topic Area. Alternately the Government may, at its discretion, make no awards in a Technical Topic Area.
- 1.3. The U.S. Department of Homeland Security (DHS), Science and Technology Directorate (S&T), PSVP project aims to conduct evidence-based research to better understand an evolving threat landscape in an effort to improve and/or build tools and techniques when it comes to enhancing public safety while preventing acts of violence from impacting our communities. While the program covers a broad set of requirements from across the homeland security enterprise, the focus of the PSVP project is to utilize the application of fundamental research in behavioral, social, economic, human factors and investigative sciences to assist in the development of knowledge, tools, and techniques to support efforts as we aim to mitigate and prevent acts that put an individual(s) and group(s) safety into question while identifying points of intervention for susceptible individual(s) and group(s) before they strike as we strengthen the preparedness and protection of the most vulnerable communities. Effective response requires a proactive, analytical, and qualitative approach to the prevention of, protection from, mitigation of, response to, and recovery from acts that impact our public safety.
- 1.4. This BAA Call seeks ideas to strengthen proactive approaches in enhancing public safety and violence prevention by collaborating with stakeholders to develop products that would:
 - Identify data through the development, analysis, reporting, and/or sharing of scientific data on the nature of threats, crimes, individuals, and organizations in an effort to better understand where, when and how to best intervene to prevent, protect, mitigate, respond and recover from these attacks to public safety.
 - Conduct evaluation research using standard social science research methods for evaluative purposes to determine what works, what doesn’t, and what’s promising in various Federal, state, local, tribal, and territorial (FSLTT) programs to strengthen preparedness and resilience for an individual(s) or group(s) within a community.

- Enhance capabilities by conducting experiments, simulations, and/or fundamental research by evaluating the value of policies, programs, training, and technologies in all aspects of national preparedness to improve the capabilities necessary to prevent, protect against, mitigate the effect of, respond to, and recover from those threats that pose the greatest risk to our public safety, both man-made and of natural causes.

2. Project Description/Scope

2.1 This BAA Call solicitation 0002 covers requirements identified in the National Strategy for Countering Domestic Terrorism (June 2021), and the DHS Strategic Framework for Countering Terrorism and Targeted Violence Implementation Plan (October 2020). Under this Call, S&T seeks to (1) produce at least four systematic reviews to help policymakers and practitioners take into account the least biased and most scientifically rigorous evidence in their decision-making; and (2) aim to make the reviews easily accessible to decision-makers, other researchers, and the general public.

Efforts under this BAA Call are anticipated to be Type IV efforts as defined in the 5-Year BAA 70RSAT21RB0000004 Section 2.2.

2.2 Findings from these research activities shall enable policy makers and operational end users with the evidence and meta-analysis needed to make informed decisions to divert vulnerable individuals, prevent potential offenders, mitigate vulnerabilities, and enhance community resiliency to improve targeted violence and terrorism prevention programming. This BAA Call solicits responses to the following Technical Topic Area (TTA):

- Targeted Violence and Terrorism Prevention Systematic Reviews

The TTA is discussed in detail below and specific objectives of the TTA are also provided in the Statement of Objectives (SOO). Of particular note, it is anticipated that both metrics and analysis techniques to measure the progress will evolve during the project. Depending on the TTA, there is a requirement to work with DHS S&T to address any privacy and human subject research requirements as necessary. Compliance with these requirements, which can include an internal review board (IRB), will be necessary for those activities that require human subjects research involvement.

3. Technical Topic Area

Targeted Violence and Terrorism Prevention Systematic Reviews

This effort seeks to produce systematic reviews to help policymakers and practitioners take into account the least biased and most scientifically rigorous evidence in their decision-making. The specific objective of this project is to conduct at least four systematic reviews per annum over a period up to three years. The contractor shall have research expertise in the field of targeted violence and terrorism prevention to support the development of the systematic reviews, including but not limited to identification of peer reviewers to the publishing of final systematic

reviews and plain language summaries.

4. Project Structure

This BAA Call is structured into one TTA that aims to develop at least four systematic reviews over a three-year period.

5. Project Schedule/Milestones

The deliverables and milestones below are anticipated under the TTA. Offerors should describe proposed deliverables similar to the ones in the relevant table below in their Technical Proposals.

Sample deliverables below:

Tasks & Deliverables			
Task #	Tasks/Deliverable	Description	Due Date
1.0	Project Management & Reporting		
1.1	Kick Off Meeting	A kick-off meeting with DHS stakeholders to initiate project.	Within 15 days of award
1.2	PMP	A project management plan that will accomplish the program's objectives as outlined in the SOW and proposal. The final version requires approval by the DHS Program Manager.	Within 30 days of award
1.3	Monthly Management Meetings and Reports	Monthly Management Meetings will be scheduled by the contractor and include written meeting minutes and action item tracking. The final version requires approval by the S&T Program Manager.	Initial meeting part of Kick Off (1.1) then monthly through the period of performance
2.0	Systematic Review Design & Approval		
2.1	Title Registration	Contractor reviews titles for deficiencies/overlap and conducts a title registration for each of the systematic reviews.	Within 2 months of award
2.2	Research Protocol	The contractor shall produce a protocol, which lays out a detailed strategy for conducting the research. Contractor shall develop a research protocol for each of the systematic reviews.	Within 4 months of award
3.0	Systematic Review		

3.1	Conduct Systematic Search for Studies	Contractor shall determine inclusion/exclusion criteria for studies and will search for, and code, all studies that satisfy the inclusion criteria. Upon completion of coding, contractor shall, where appropriate, apply meta-analytic methods to synthesize findings.	Initiate systematic reviews within 6 months of award
4.0	Dissemination of Findings		
4.1	Deliver Draft Systematic Reviews and Draft Plain Language Summary	Submit draft systematic reviews and draft 2-page plain language summaries for each systematic review for DHS review and comment.	Within 10 months of award
4.2	Publish Final Systematic Reviews and Plain Language Summary	Deliver and publish identified number of full systematic reviews to include the plain language summary for each systematic review.	Within 12 months of award
5.0	Close Out		
5.1	Close Out Meeting	Performer will coordinate a close-out meeting at the conclusion of the period of performance.	15 days before termination of period of performance.

6. Special Instructions/Notifications

6.1. Response Dates

Event	Time Due	Date or Date Due
BAA Call released	2:00 PM Eastern Time	March 23, 2023
Questions Due	12:00 PM Eastern Time	March 30, 2023
Answers Posted		April 6, 2023
White Papers Due (Phase 1)	12:00 PM Eastern Time	May 3, 2023
Notification of White Paper Evaluation Results		June 2, 2023
Proposals Due (Phase 2)	12:00 PM Eastern Time	June 30, 2023
Notification of Proposal Evaluation Results		July 28, 2023

6.2. Contractual or Technical Inquiries

All contractual or technical questions regarding this BAA Call solicitation must be emailed to PSVP@hq.dhs.gov, the Contracting Officer and Contract Specialist no later than 12:00 PM Eastern Time March 29, 2023. Emails submitting questions are to include “Questions for 70RSAT21RB00000004/0002” in the subject line. All questions and responses will be posted on the website Sam.gov. Questions will only be accepted and answered electronically. Offerors should be aware that contractor support personnel have access to this mailbox and that proprietary information should not be emailed to this mailbox unless and until your organization has a signed company to company agreement with [Noblis ESI] See the paragraph entitled “Company to Company Agreements” below for additional information.

Any questions concerning this Call must be submitted via email to PSVP@hq.dhs.gov, Contracting Officer: Jessica Wilson - Jessica.Wilson@hq.dhs.gov and Contract Specialist: Dorothy Woolfolk – Dorothy.Woolfolk@hq.dhs.gov not later than indicated in paragraph 6.1 above. Questions submitted shall follow this format:

Question #	Reference	Offeror’s Question
1	(Example) General – if no specific document is referenced	
2	(Example) BAA 70RSAT21RB00000004 Call 0002, page 2, Section 4, first sentence	

6.3. General Instructions and Information

This BAA Call 0002 is only seeking the submission of **Phase 1** White Papers at this time, subject to the date identified in paragraph 6.1 above. **Full Proposals (Phase 2) are not being requested at this time.** Invitations to submit Full Proposals will be extended based on white paper evaluation results in accordance with the date identified in paragraph 6.1 above. Full proposals must be received by the due date identified in paragraph 6.1 above. This BAA Call is open to all responsible sources and is considered to be full and open competition.

Basic procedures for submission of White Papers to the DHS S&T Portal are provided in Section 8 of BAA 70RSAT21RB00000004. These procedures are modified by this Call as described below. The following procedures and page limits apply to this BAA Call:

Phase 1 (White Papers): 10-page limit plus a one-page quad chart. White Papers may include narrative, pictures, figures, tables, and charts in a legible size. This submission should describe the Offeror’s technical and management approach as well as the Offeror’s relevant capabilities and experience. The White Paper shall include a cost estimate and a brief explanation of how the cost estimate was created. This submission must also include a signed Company to Company Agreement with Noblis (not included in page limit).

Phase 1 Quad Chart: The quad chart should follow the format described below and should not contain any font smaller than 10-point font.

BAA Number:		Offeror Name:	
Title: <i>(Brief/Short Title to Describe Offeror's Proposed Effort)</i>		Date:	
Photograph or artist's concept: <i>Provide a simple but sufficiently detailed graphic that will convey the main idea of the final capability/use/system prototype demonstration in an operational environment, and its technological methodology.</i>		Operational Capability: <ol style="list-style-type: none"> <i>Performance targets</i> <i>Quantify performance for key parameters</i> <i>Cost of ownership or licensing, if applicable.</i> <i>Address how the proposed development addresses the goals in the BAA call.</i> 	
Proposed Technical Approach: <ol style="list-style-type: none"> <i>Explain how it would meet the goals detailed in the BAA call.</i> <i>Describe tasks to be performed for base period.</i> <i>Describe current status of the proposed technology.</i> <i>Describe any actions done to date.</i> <i>Describe any related ongoing effort by the offeror.</i> 		Schedule, Cost, Deliverables, & Contact Info: <i>Provide any milestone decision points that will be required. Describe period of performance and total costs. Include the base performance period cost and length, and estimates of cost and lengths of possible option(s).</i> Deliverables: <i>Include all hardware, software and data deliverables.</i> Corporate Information: <i>You must include Offeror Name, POC full name, address, phone numbers and e-mail.</i>	

Phase 2 (Full Proposals): This submission includes both a Technical Proposal and a Cost Proposal. The Technical Proposal page limit is 40 pages. The Technical Proposal may include narrative, pictures, figures, tables, and charts in a legible size. Technical Proposals shall discuss in detail the Offeror's technical and management approach as well as the Offeror's relevant capabilities and experience. Technical proposals shall include the Offeror's proposed deliverables based on the sample deliverables in Section 5. This submission shall include the assertion of data rights described in Section 9.5 of 70RSAT21RB00000004. The Cost Proposal does not have a page limit but should not include technical information. Cost Proposals should specify the Offeror's preferred contract type (i.e., cost plus fixed fee, firm fixed price). Offerors should also specify the contract vehicle that they think is most appropriate for their proposed work (i.e., FAR-based contract, interagency agreement, other transaction). Cost proposals should include all applicable information specified under "Price/Cost Proposal" in Section 9.5 of 70RSAT21RB00000004.

Note that Offerors must complete the company/organization portal registration PRIOR to submitting a White Paper for the first time. Ensure adequate time to complete the company/organization registration as delays in this process will not be authorization for late

submissions of White Papers. Company/organization registration information is in Section 10.1 of BAA 70RSAT21RB00000004. In addition, each subsequent White Paper requires registration in the portal. Information regarding White Paper registration is in paragraph 10.2 of 70RSAT21RB00000004.

White Papers also must comply with the information in BAA 70RSAT21RB00000004

paragraph 11.4 regarding Company-to-Company Agreements. For the purposes of this Call, the Noblis, Inc. point of contact for agreements is Dr. Michelle Weinberger (Michelle.Weinberger@associates.hq.dhs.gov). Emails to Dr. Weinberger shall include the Contracting Officer and Contract Specialist on the cc line of the email.

To be considered for award, Offerors **MUST** submit White Papers and Company to Company Agreements with Noblis, Inc. compliant with the response dates listed in paragraph 6.1 above, in accordance with the requirements in DHS BAA 70RSAT21RB00000004. Submissions not in compliance with both BAA 70RSAT21RB00000004 and this BAA Call 00002 will be rejected (note: the cover page created by the DHS S&T BAA Portal must be included but does not count against the page count). White Papers will only be accepted via the portal. No emailed White Paper submissions will be accepted for review. No classified White Papers will be accepted.

White Papers will be evaluated and Offerors will either be encouraged or not encouraged to submit a Full Proposal. Offerors who are not encouraged to submit a Full Proposal are still permitted to do so. Offerors must submit a White Paper in order to be able to submit a Full Proposal. Feedback regarding the evaluation findings of submitted White Papers will not be provided.

Procedures for submission of Full Proposals can be found in Section 8 of BAA 70RSAT21RB00000004. Invitations to submit Full Proposals will be extended based on White Paper evaluation results in accordance with the date identified in paragraph 6.1 above. Full Proposals must be received by the due date identified in paragraph 6.1 above. **Full Proposals are not being requested at this time. In accordance with Section 8 of BAA 70RSAT21RB00000004, Offerors must submit a fully compliant White Paper to be considered for participation in the submission of proposals.**

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.

6.4 Evaluation

As stated in BAA 70RSAT21RB00000004, DHS S&T reserves the right to select for award and to fund all, some, or none of the proposals received in response to this BAA Call solicitation.

The Evaluation Criteria in Section 11 of 70RSAT21RB00000004 apply to this Call. The Evaluation Criteria will be used for both Phase 1 and Phase 2. The Government expects Phase 2 proposals to contain considerably more detail than Phase 1 and will evaluate based on this expectation.

DHS S&T intends to use the following ratings to evaluate White Papers and Full Proposals:

Criterion I and II

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

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

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

Fair (F) - The White Paper/Full Proposal indicates minimal understanding of the problem. The technical analyses meet the goals and are technically sound, but the Offeror fails to demonstrate a reasonable probability of successfully achieving the desired outcome of the topic area.

Unacceptable (U) - The White Paper/Full Proposal does not meet the BAA's requirements.

Criterion III

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

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

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

6.5 Company to Company Agreements

White Papers must comply with the information in BAA 70RSAT21RB0000004 paragraph 11.4

regarding Company-to-Company Agreements.

Important Note: DHS intends to use Noblis, Inc. for routine administrative support during the evaluation process of both White Papers and Full Proposals. All Offerors, Prime Contractors only (this applies to all Offerors, whether or not the Offeror is a company) must submit an executed Company to Company Agreement with Noblis, Inc., found in Appendix A, along with their White Paper submission. Company to Company Agreements must be dated this fiscal year (2023). 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. For the purpose of this Call, the Noblis point of contact is Dr. Michelle Weinberger (Michelle.Weinberger@associates.hq.dhs.gov). Offerors are encouraged to allow sufficient time to permit agreement execution.

6.6 Foreign Participation

Offerors are reminded that foreign participation may occur as defined in BAA 70RSAT21RB0000004, Section 1.3. Additionally, any foreign responses to this Call shall be in the English language. White papers, and later proposals, received in other than English shall be rejected. Offerors invited to submit proposals shall do so only in terms of U.S. dollars. Proposals received in other than U.S. dollars shall be rejected.

6.7 Export Control Requirements

Offerors are reminded of the export control markings required by BAA 70RSAT21RB0000004, Section 12.5.

6.8 Travel

For purposes of estimating costs for full proposals, Offerors should anticipate travel to two (2) project meetings per year. Travel will be reimbursed in accordance with the limitations set forth in FAR 31.205-46, Travel Costs, and the Federal Travel Regulation. Local travel within a 50-mile radius from the Contractor's facility or the Contractor's assigned duty station will not be reimbursed. This includes travel, subsistence, and associated labor charges for travel time. Travel performed for personal convenience or daily travel to and from work at the Contractor's facility or local Government facility (i.e., designated work site) shall not be reimbursed hereunder. The Contractor shall not be reimbursed for moving or relocation expenses for the Contractor or Contractor employees, and/or subcontractors.

6.9 Order of Precedence

In the event that any of the terms and conditions contained in this solicitation conflict with terms and conditions included in BAA 70RSAT21RB0000004, the terms and conditions in this BAA Call shall take precedence.

7. Sensitive Information

Depending on an Offeror's specific proposal and the TTA proposed under, Offerors may have access to sensitive information in awards under this BAA Call. DHS S&T will comply with the

requirements of HSAR Class Deviation 15-01 and the HSAM Appendix G Sensitive Information Checklist for individual awards under this BAA. Accordingly, the clauses below may apply to individual awards under this BAA. Awards under 70RSAT21RB0000004 are likely to require access to sensitive information. Accordingly, the clauses listed below will generally be included in awards under this Call.

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

HSAR 15-01 Safeguarding of Sensitive Information (MAR 2015)

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

(b) Definitions. As used in this clause—

“Personally Identifiable Information (PII)” means information that can be used to

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

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

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

- (1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, “Policies and Procedures of Safeguarding and Control of SSI,” as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as “For Official Use Only,” which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person’s privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

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

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

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

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

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

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

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

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

- (1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information describes how Contractors must handle sensitive but unclassified information. DHS uses the term “FOR OFFICIAL USE

ONLY” to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The DHS Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook provide the policies and procedures on security for Information Technology (IT) resources. The DHS Handbook for Safeguarding Sensitive Personally Identifiable Information provides guidelines to help safeguard SPII in both paper and electronic form. DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

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

(3) All Contractor employees with access to sensitive information shall execute DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA), as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer’s Representative (COR) no later than two (2) days after execution of the form.

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

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

(1) Complete the Security Authorization process. The SA process shall proceed according to the DHS Sensitive Systems Policy Directive 4300A

(Version 11.0, April 30, 2014), or any successor publication, DHS 4300A Sensitive Systems Handbook (Version 9.1, July 24, 2012), or any successor publication, and the Security Authorization Process Guide including templates.

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

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

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the

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

(2) Renewal of ATO. Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods:

(1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90-day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

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

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

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

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

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

defined in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) Sensitive Information Incident Reporting Requirements.

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

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

- (i) Data Universal Numbering System (DUNS);
- (ii) Contract numbers affected unless all contracts by the company are affected;
- (iii) Facility CAGE code if the location of the event is different than the prime contractor location;
- (iv) Point of contact (POC) if different than the POC recorded in the

- System for Award Management (address, position, telephone, email);
- (v) Contracting Officer POC (address, telephone, email);
 - (vi) Contract clearance level;
 - (vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
 - (xiii) Government programs, platforms or systems involved;
 - (ix) Location(s) of incident;
 - (x) Date and time the incident was discovered;
 - (xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
 - (xii) Description of the Government PII and/or SPII contained within the system;
 - (xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
 - (xiv) Any additional information relevant to the incident.

(g) Sensitive Information Incident Response Requirements.

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

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

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

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

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

response activities.

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

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

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

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

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

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

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

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

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

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

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

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

(b) Security Training Requirements.

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

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at

<http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

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

HSAR 3052.204-71 Contractor Employee Access (Sep 2012) Alt. II (Jun 2006)

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

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security

Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

- (2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);
 - (3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and
 - (4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.
- (b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.
 - (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 sensitive information or IT 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 sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

- (f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.
- (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-citizens proposed to work under the contract. Any additions or deletions of non-citizens after contract award shall also be reported to the contracting officer.