

Broad Agency Announcement Solicitation HSHQDC-14-R-B0014

Project: Data Privacy Technologies Research and Development

1. Introduction

1.1 This BAA solicitation is a call issued against Department of Homeland Security (DHS), Science & Technology (S&T), Cyber Security Division (CSD), 5-Year Broad Agency Announcement (BAA), HSHQDC-14-R-B0005, Amendment 00001. All terms and conditions of the DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00001, apply to this solicitation unless otherwise noted herein.

1.2 The Cyber Security Division (CSD) within the DHS S&T Directorate led the development of the Federal Cyber Security Research and Development (R&D) Strategic Plan (*Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*) that was issued by the White House in December 2011. The plan coordinates research and development (R&D) efforts across the Federal government and challenges Federal agencies to develop a targeted set of cybersecurity research priorities to “change the game” to ensure that cyberspace can become a safe, trustworthy, and prosperous environment.

1.3 This outcome rests as much on privacy as security; both are critical to achieving DHS mission objectives. The nature of DHS missions are such that they often involve the collection and use of considerable volumes of personally identifiable information (PII). While these activities include obvious ones like law enforcement and intelligence analysis, they also include activities like disaster relief, refugee processing, and providing health care to detainees. In contexts such as human trafficking, privacy directly supports the security of victims. In other contexts, privacy directly supports the security of DHS personnel as they perform their duties. In all these contexts, the need to support appropriate sharing and use of needed information constituting or implicating PII while preventing inappropriate sharing and use is central.

1.4 DHS S&T is funding a new research and development project related to these privacy protection requirements called Data Privacy Technologies. The goals of the research project within the CSD are:

1.4.1 To perform R&D aimed at improving privacy protection capabilities that also support usability and innovation advantages.

1.4.2 To develop innovative, easy-to-use, and cost-effective privacy-enhancing technologies ready for deployment.

1.4.3 To develop knowledge products and tools that facilitate trusted environments supporting users’ needs and expectations.

1.4.4 To facilitate the transfer of these technologies into the hands of government agencies, corporate enterprises, and developers as a matter of urgency.

1.5 To meet the increasing need for technologies that incorporate privacy by design (e.g., building privacy controls into systems that directly support a mission) through coordination early and often between developers, policy makers, and end users so as to produce innovative solutions that embed privacy controls while addressing mission requirements.

2. Project Description/Scope

2.1 Protecting PII is important to the overall mission of DHS and across the U.S. Government. Laws and regulations, such as the Privacy Act of 1974, the E-Government Act of 2002, the Children’s Online Privacy Protection Act (COPPA), the Fair Credit Reporting Act (FCRA), and the Health Insurance Portability and Accountability Act (HIPAA) specifically address protecting the privacy of populations that include not just U.S. citizens and legal permanent residents but often foreign nationals as well. In some cases, even though not legally required, DHS extends such protections to foreign nationals as a matter of policy.

2.2 By definition, any collection, use, or dissemination of PII entails risk, be it the risk of inadvertently failing to comply with applicable privacy laws, regulations and policies, risk of harm to individuals, including DHS personnel, or risk of compromising DHS missions. Privacy related breaches are increasing in frequency and impact. These breaches have effects that amount to multimillion-dollar impacts on federal, state, and local governments as well as on the private sector. In addition to lost or stolen PII, there have been an increasing number of privacy violations involving improper use of data. The effects of these privacy violations impose serious consequences on the public, our nation’s economic growth, and innovative developments.

2.3 At the same time, though, DHS missions often cannot be effectively executed without such data. Therefore, DHS seeks ways of mitigating these risks more effectively while still permitting it to carry out its missions. S&T, therefore, has a long-standing and broad interest in privacy-enhancing technologies (PETs). Much of the research in this area has focused on minimizing or preventing the collection of PII and S&T recognizes that, where this can be done consistent with operational efficiency and efficacy, such approaches offer significant potential for risk mitigation. In particular, to the extent that technologies can support the sharing of genuinely minimized information that nevertheless provides the necessary data, PETs offer very attractive possibilities. This BAA solicitation will build upon PETs and offeror’s should factor the following requirements into their technical approaches when responding to any of the Technical Topic Areas (TTAs):

2.3.1 Controls - Controls that support improved management of PII, including better accountability mechanisms, greater automation of protections, and functionality that enhances the ability of users to understand and control what is happening when interacting with a system.

2.3.2 Usability - Sophisticated controls will not have their intended effect if they cannot be easily understood and employed by those charged with implementing and using them. This imperative should not be interpreted as a restriction on the technical sophistication of PETs.

2.3.3 Scalability - S&T’s mission is to provide R&D support to the entire DHS enterprise as well as the broader homeland security enterprise across and beyond the federal government. Thus, the integration is as much a facet of scalability as the enterprise-scale capability. A need for substantial re-architecting or re-configuration of information and/or communications

infrastructure will significantly degrade the practical scalability of a technology. The broad use and scalability of PETs must be considered in response to this BAA solicitation.

3. Technical Topic Areas

The TTAs for Data Privacy Technologies Research and Development project are listed below, with a summary of the problem scope and related reference sources. In some cases, risk controls may be achievable through innovative integration of existing solutions. Other cases may require transforming largely theoretical concepts into workable technical implementations. Yet other cases may demand new concepts that can be readily translated into practical new approaches.

3.1 TTA #1: Homeland Security Enterprise Privacy Policy Compliance Tools

3.1.1 As part of daily operations, DHS component agencies regularly store and transmit personally identifiable information (PII) both inside and outside the enterprise. These transactions must comply with federal regulations and internal policies to properly protect sensitive information. DHS component agencies require innovative, cost effective tools and technologies that address policy compliance while minimizing business process overhead. Referencing the requirements for PETs above, two specific research areas of interest within privacy policy compliance are:

3.1.1.1 Automatic E-mail Encryption – DHS component agencies are concerned with the transmittal of PII both in the body of the e-mail and within attachments, especially the transmittal of such information to entities outside the DHS enterprise. Any proposed solution should meet federal encryption standards [1], be interoperable with existing e-mail systems, and be straightforward to implement and transparent to the user. Because e-mail may be sent to members of the public on an ad hoc basis, features such as flexibility as well as scalability and ease of use are of paramount importance. Proposed solutions may assume that the transmission of PII to the designated recipient is authorized and appropriate. Possible solutions includes, but are not limited to, data-level encryption.

3.1.1.2 OMB Data Extract Rule Compliance – OMB Memoranda 06-16 [2] and 07-16 [3] outline requirements that federal agencies ensure that data extracts containing PII are tracked, logged, and purged from recipient databases after a defined timeframe. Federal agencies are struggling with the ability to comply, especially for legacy systems; most are addressing the requirement using manual methods that are cumbersome and non-scalable. Technical approaches should focus on solutions to help automate compliance with OMB policy. Any proposed solution should be interoperable with Commercial-Off-The-Shelf (COTS) database management systems, be easy to use, record and track the necessary information, and support the 90-day extract timeframe rule. Possible solutions include, but are not limited to, data-level tagging and tracking, and data provenance.

3.1.2 The goal of this TTA is the development of cost-effective near-term solutions for DHS operational component agencies that address the two research areas above. Offerors should feel free to address one or both of the above research areas of interest, including synergistic solutions.

3.1.3 Technical approaches should include a discussion of how the tools and techniques developed would be transitioned to individual component agencies across the DHS enterprise, and across non-DHS agencies. Demonstrations or pilots with stakeholders to use the tools and techniques developed are encouraged and should be proposed as separate options.

3.2 TTA #2: Privacy-Preserving Federated Search

3.2.1 DHS component agencies currently employ segregated systems, many of which contain personally identifiable information (PII), that support specific mission purposes. Various restrictions and protections can make it difficult, if not impossible, to perform checks and analyses on this PII. For example, the PII of applicants for certain kinds of immigration status are subject to exceptional disclosure restrictions. At the same time, it is desirable to enable other agencies to identify applicants who have criminal or terrorist connections. Even in cases in which information may be shared for such purposes, the sensitivity of the PII represents significant risk which could be reduced if the information could be minimized. In other cases, the analysis of sensitive victim records could provide information regarding patterns of criminal activity, but disclosure restrictions render such sharing difficult. DHS requires the ability to perform federated searches across multiple data sources residing in multiple domains, organizations and jurisdictions that can return actionable results while continuing to appropriately protect PII consistent with applicable laws, regulations, and policies. DHS seeks technologies that can support such information sharing in a privacy-protective manner. Possible solutions include, but are not limited to, policy automation tools, data anonymization technology, encryption and frameworks.

3.2.2 Currently, disclosure control under certain circumstances consists of blocking any search results for records that cannot be shared. More nuanced and flexible mechanisms are needed. In some cases, owing to classification or privacy concerns, the agency or program conducting the search may need to protect the details of its query as well. This increases the difficulty of the problem, as information sharing is restricted in both directions. Further compounding the problem is the potential for inferences based on data aggregation. Federated search involves multiple databases with varying but overlapping fields. As a result, the information revealed by one database, even if unproblematic in and of itself, may indirectly reveal additional information when combined with information returned from other databases, compromising privacy and undermining compliance. In other words, the resultant information sharing will be more than what was actually intended or permitted. Possible solutions include access control, data anonymization and anonymity technology, and identity resolution tools.

3.2.3 Again, referencing the requirements for PETs above, research should focus on tools and techniques that can enable useful sharing of information based on PII while maintaining necessary protections [4] on the data being searched and, on an as needed basis, on the search data itself. This includes mechanisms for guarding against information leakage as a result of aggregated results from a federated search. Technologies of interest include, but are not limited to, anonymous matching, tokenization and privacy-preserving data mining. To the extent that achieving this goal requires defined research pertaining to federated search per se, irrespective of the privacy-protective aspects of the problem, technical approaches addressing this are also of interest. Issues of compatibility and interoperability with legacy systems should be explicitly

addressed, as should more general issues of scope and scaling. In addition, technical approaches should include a discussion of how the tools and techniques developed would be transitioned to individual component agencies, across the DHS enterprise, and across non-DHS agencies. Demonstrations or pilots with stakeholders to use the tools and techniques developed are encouraged and should be proposed as separate options.

3.3 TTA #3: Mobile Computing Privacy

3.3.1 Mobile device adoption and adaptation is on the rise in both the public and private sectors. As DHS component agencies incorporate these devices—including, but not limited to, smart phones and tablets—into the DHS workspace, new requirements are emerging that are specific to the mobile space. Not surprisingly, new risks to personally identifiable information (PII) have been identified in mobile environments. As mobile device use continues to increase, application security has come under closer scrutiny; adequate protection of user data that is stored on these devices is increasingly uncertain. Recent media attention surrounding user location tracking and unauthorized use of user data has provided greater motivation to adequately secure PII and location information on mobile devices. Technologies that improve mobile application security and privacy must also support a dynamic, user-driven mobile experience. Possible solution includes, but are not limited to, mobile software development kit.

3.3.2 Research of interest will avoid a *zero-sum game* where usability, functionality, innovation, or security is sacrificed to achieve privacy, with an emphasis on implementing the aforementioned PET requirements. There are a number of more specific privacy concerns related to mobile computing and supporting applications, including the following:

3.3.2.1 How can individual application user agreements be more succinct, understandable, and better highlight privacy concerns?

3.3.2.2 How can a user verify that an application performs according to stated/agreed terms and conditions?

3.3.2.3 How can the end user effectively control location-tracking preferences, including, but not limited to, ensuring that user data is not stored in an unprotected manner or shared with third-parties?

3.3.2.4 How can the small footprints of these devices accommodate data protection when competing with other necessary device features/functionality?

3.3.3 Protecting the privacy of mobile users requires context-aware, user-controlled mobile device functionality that addresses collection, use/reuse, and sharing of PII. Specifically, DHS component agencies seeking to use mobile technology require tools that will provide simplicity, ease of use, and adequate device protection, including automatic disabling of location-tracking features when used in sensitive environments and selective enabling of location tracking at variable granularities in disaster and other situations. Specific research of interest includes:

3.3.3.1 The development of automated, context-based controls (e.g., tools that automatically enable and disable sharing of location data, disclose with whom the information is being shared, and provide the capability to easily modify device actions).

3.3.3.2 Enforceable segregation of data on a single device so as to prevent cross-contamination and facilitate more granular data management, including mission and user (on devices with multiple users) separation and targeted secure deletion.

3.3.3.3 Mechanisms for ensuring individual awareness and choice when interacting with an enterprise from a mobile platform.

3.3.3.4 Indicators that inform users of inbound and outbound data flows—including, but not limited to, location information—and that can adjust controls on those flows automatically and contextually or enable easy user adjustment.

3.3.3.5 Indicators and user controls for mobile device cameras and/or microphones that cannot be circumvented, so as to prevent undesired capture of video and/or audio information.

3.3.4 DHS is seeking solutions that securely protect PII and offer granular yet simple control options, including solutions related to relative identifiability/anonymity. Offerors must choose mobile devices used by the Federal Government in its day to day business operations as target platforms for solutions. Technical approaches should include a discussion of how the tools and techniques developed will be transitioned to individual component agencies, across the DHS enterprise, and across non-DHS agencies. Demonstrations or pilots with stakeholders that would use the tools and techniques developed are encouraged and should be proposed as separate options.

4. Project Structure

The Data Privacy Technologies project will be structured as communities of interest around the TTAs above; as such, DHS, supports and encourages: collaborating with others in the research community and/or other developers and integrators; and forming collaborations, to provide joint deliverables to include whitepapers, proof-of-concept, and hardware/software products. Key deliverables for each TTA are below. Working prototype deliverables must include a full operating environment and developed software.

4.1 TTA #1: Key Deliverables

The following key deliverables for TTA #1 are required for each severable year of performance (note: for Type I and Type II awards, the version numbers will increase sequentially if options are exercised for out-year tasking):

DELIVERABLES	DUE DATE
Monthly Technical and Financial Status Reports	Due every month with Invoice
Design Document, Version 1	45 days after award
Transition Plan, Version 1	45 days after award
Target Capabilities Definition Document, Version 1	45 days after award
Design Document, Version 2	6 months after award
Target Capabilities Definition Document, Version 2	6 months after award
Working Prototype, Version 1	6 months after award
Developed Software for Working Prototype Version 1	6 months after award
User Manual for the Working Prototype Version 1	6 months after award
Configuration and Installation Manual for Working Prototype, Version 1	6 months after award
Proof of Concept Demonstration Evaluation Plan	8 months after award
Conduct Proof of Concept Demonstration/Pilot Within a Customer Test Environment	10 months after award
Design Document, Version 3	11 months after award
Working Prototype, Version 2	11 months after award
User Manual for the Working Prototype Version 2	11 months after award
Configuration and Installation Manual for Working Prototype Version 2	6 months after award
Transition Package Submission for Customer	12 months after award
Deliver Final Report (Lessons Learned, Demonstration)	12 months after award

4.2 TTA #2: Key Deliverables

The following key deliverables for TTA #2 are required for each severable year of performance (note: for Type I and Type II awards, the version numbers will increase sequentially if options are exercised for out-year tasking):

DELIVERABLES	DUE DATE
Monthly Technical and Financial Status Reports	Starting 45 days after award
Requirements Specification with release phasing	45 days after award
Transition Plan, Version 1	45 days after award
Design Document	6 months after award
Target Capabilities Definition Document, Version 2	6 months after award
Working Prototype, Version 1	6 months after award
Proof of Concept Demonstration Evaluation Plan	8 months after award
Conduct Proof of Concept Demonstration/Pilot Within a Customer Test Environment	10 months after award

Proof of Concept Demonstration Evaluation Plan	10 months after award
Design Document, Version 3	11 months after award
Working Prototype, Version 2	11 months after award
Transition Package Submission for Customer	12 months after award
Deliver Final Report (Lessons Learned, Demonstration)	12 months after award

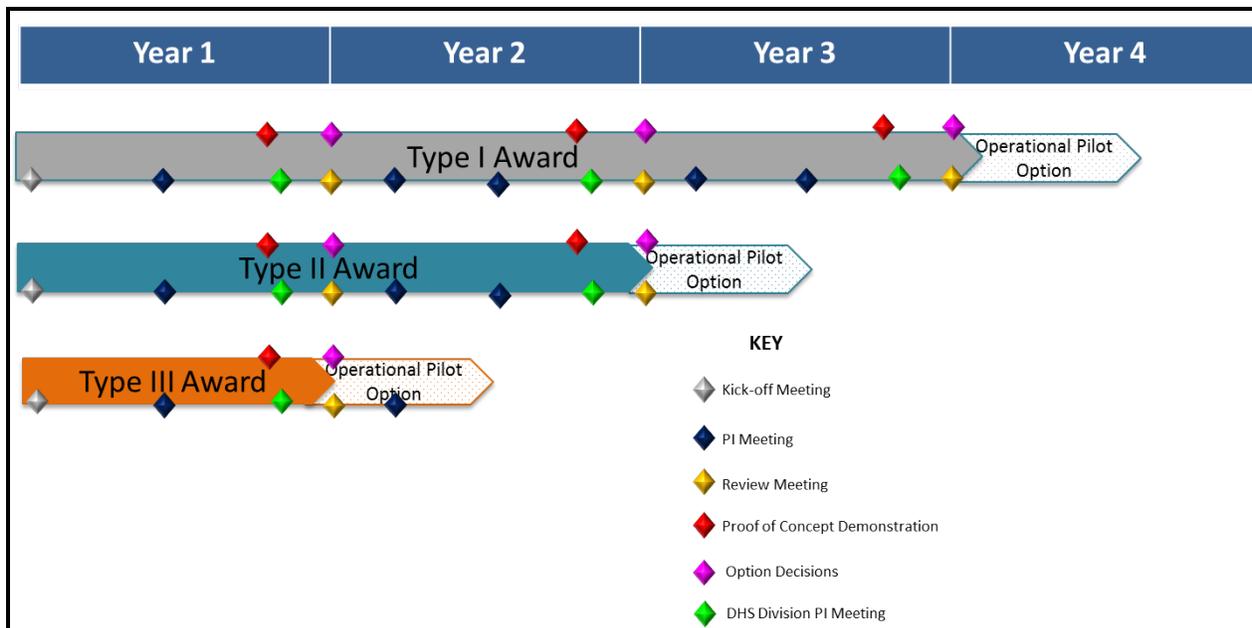
4.3 TTA #3: Key Deliverables

The following key deliverables for TTA #3 are required for each severable year of performance (note: for Type I and Type II awards, the version numbers will increase sequentially if options are exercised for out-year tasking):

DELIVERABLES	DUE DATE
Monthly Technical and Financial Status Reports	Starting 45 days after award
Design Document, Version 1	45 days after award
Target Capabilities Definition Document, Version 1	45 days after award
Design Document, Version 2	6 months after award
Target Capabilities Definition Document, Version 2	6 months after award
Working Prototype, Version 1	6 months after award
User Manual for the Working Prototype Version 1	6 months after award
Proof of Concept Demonstration Evaluation Plan	8 months after award
Conduct Proof of Concept Demonstration/Pilot Within a Customer Test Environment	10 months after award
Design Document, Version 3	11 months after award
Working Prototype, Version 2	11 months after award
Working Prototype, Version 2	11 months after award
Transition Package Submission for Customer	12 months after award
Deliver Final Report (Lessons Learned, Demonstration)	12 months after award

5. Project Schedule/Milestones

A notional schedule is shown below including anticipated meetings and demonstrations. The depiction shows the difference between how Type I, Type II and Type III will be monitored and progress measured.



6. Special Instructions/Notifications

6.1 Response Dates.

Event	Time Due	Date Due
Industry Day	N/A	June 24, 2014
White Papers Due	4:30pm EDT	July 22, 2014
Notification of White Paper Evaluation Results	N/A	On or About August 29, 2014
Proposals Due	4:30pm EDT	September 30, 2014

6.2 General Instructions and Information.

6.2.1 This BAA solicitation (HSHQDC-14-R-B0014) includes a requirement to submit white papers, prior to the submission of proposals, subject to the date identified in the “Response Dates” table above.

6.2.2 Procedures for submission of white papers and proposals in the DHS S&T Portal are provided in paragraph 10 of DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00001. 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 located in paragraph 10.1 of DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00001. In addition, each white paper and subsequent proposal requires registration in the portal. Information regarding white paper and proposal registration is located in paragraph 10.2 of DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00001.

6.2.3 Offerors may provide multiple white paper and proposal submissions; however, each submission must only address one TTA and must be distinct and self-contained without any dependencies on other work of any kind.

6.2.4 All software developed and delivered is required to be subject to security auditing; therefore, the offeror's technical approach must identify how security auditing will occur. Also, DHS expects offerors to follow best practices on software design and encourages the use of the DHS Software Assurance Marketplace [5].

6.2.5 DHS has a strong preference for open source licensing of software for all software developed and delivered and the licenses for all proposed software deliverables will have to be identified in submitted white papers and proposals (note: the DHS HOST [6] project provides directions and opportunities for promoting open source software). However, as an alternative to open source release, offerors may also offer a strong technical transition plan for deployment of the technologies developed.

6.2.6 As stated in DHS S&T CSD BAA HSHQDC-14-R-B0005, 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 solicitation.

6.2.7 The Evaluation Criteria in DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00001 Section 11 "EVALUATION OF WHITE PAPERS AND PROPOSALS" applies.

6.3 Foreign Participation.

Offerors are reminded that foreign participation may occur as defined in DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00001 Section 1.3. Therefore, offerors should provide unit costs for any deliverable not anticipated for delivery in a softcopy format.

6.4 Export Control Requirements.

Offerors are reminded of the export control markings required by DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00001 Section 8.6.8 (for white papers) and Section 9.6.4 (for proposals).

6.5 Type Classification Ceilings.

DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, AMENDMENT 00001, describes the Type Classifications for proposals. Specific to this call, the ceiling values for each type are as follows:

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

6.5.2 Type II – Type II awards are limited to a total contract value not to exceed \$1,000,000.00, not including operational evaluation, pilot, and/or transition options.

6.5.3 Type III – Type III awards are limited to a total contract value not to exceed \$500,000.00, not including operational evaluation, pilot, and/or transition options.

6.6 Travel.

6.6.1 For purposes of estimating costs for white papers and proposals, offerors should anticipate travel to 3 project meetings per year.

6.6.2 DHS Cyber Security Division holds an annual PI meeting where all DHS CSD funded performers are expected to present. Projects will be required to provide a briefing, typically 20 minutes, and are strongly encouraged to provide demonstrations when appropriate. The PI meeting is typically 2.5 days and attendance at the full event is encouraged.

6.6.3 In addition to the annual DHS PI Meeting, the Data Privacy Technologies R&D Project will hold two meetings each year. Meetings will be arranged by TTA and the meeting for each TTA is expected to last one day. When possible, TTA meetings will be held on adjacent days so funded efforts in one TTA can optionally attend other TTA meetings.

6.7 White Paper Requirements

6.7.1 This BAA solicitation (HSHQDC-14-R-B0015) requires the submission of a white paper, compliant with the aforementioned response dates, to be considered for participation in the submission of proposals. Offerors MUST submit a white paper in accordance with the Department of Homeland Security (DHS), Science & Technology (S&T), Cyber Security Division (CSD), 5-Year Broad Agency Announcement (BAA), HSHQDC-14-R-B0005, Amendment 00001. Submissions not in compliance with DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00001, may be rejected (note: the cover page created by the DHS S&T BAA Portal must be included, but does not count against the page count).

6.7.2 In addition to the white paper submission requirements outlined in DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00001, the information outlined in Section 6.9 below must be included in any submitted white paper.

6.8 Proposal Requirements

To be considered for award, offerors **MUST** submit a proposal, compliant with the aforementioned response dates, in accordance with the DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00001. Submissions not in compliance with DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00001 may be rejected (note: the cover page created by the DHS S&T BAA Portal must be included, but does not count against the page count). The DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, AMENDMENT 00001 [3] Section 9 discusses proposal preparation and describes the required proposal content; however, in addition to the guidance in Section 9, the following special instructions are added:

6.8.1 The maximum number of pages for Volume 1 is 25 pages.

6.8.2 The information outlined in Section 6.9 below must also be included in any submitted proposal.

6.8.3 Subcontractor Cost Submission: Referencing, DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00001, Section 9.6.2.b.(6), if the subcontractor costs cannot be included with a prime's 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 BAA-14-R-B0005@hq.dhs.gov. The subject line of the email shall say "Separate Subcontractor Cost Submission – [insert the proposal number assigned from the DHS S&T BAA Portal]". The body of the email shall contain the following:

- 1) The prime entities name which should be the same entity that is registered in the BAA portal;
- 2) A POC (name and phone number) from the prime entity; and
- 3) 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 as detailed as the offerors's cost proposal and must be received at the location designated in the individual solicitation no later than the closing date and time specified by the solicitation. 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 by the in-box for BAA-14-R-B0005@hq.dhs.gov. **NO SEPARATE SUBCONTRACTOR COST PROPOSALS RECEIVED WILL BE ACCEPTED IF RECEIVED AFTER THE AFOREMENTIONED PROPOSAL DUE DATE.**

6.9 Special Submission Requirements for both White Papers and Proposals

Given a goal of this BAA solicitation is to develop solutions that are mature enough for deployment, submissions, in both the white paper phase and the proposal phase, must specifically address the items below:

6.9.1 Clearly state which of the three TTAs are being covered.

6.9.2 Define the Target Capabilities consisting of technical and operational capabilities that the developed solution will provide. This information is to be included along with the information required by the following sections of DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00001:

- Section 8.7.3.c, which outlines the requirements for “Technical Approach” for white paper submissions;
- Section 9.6.1.g, which outlines the requirements for “Detailed Technical Approach” for proposal submissions;
- Section 9.6.1.i, which outlines the requirements for “Testing and Evaluation” for proposal submissions; and
- Section 9.6.1.l, which outlines the requirements for “Transition Plan” for proposal submissions.

6.9.3 As part of defining the Target Capabilities, propose technical and operational metrics that measure progress towards the final capability along with targets specified at 3 month intervals. The technical approach to measure the metrics should also be described. This information is to be included along with the information required by DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00001, Section 8.7.3.c, which outlines the requirements for “Technical Approach” for white paper submissions, and Section 9.6.1.i, which outlines the requirements for “Testing and Evaluation” for proposal submissions.

6.9.4 Propose a Proof of Concept demonstration in a customer (i.e., Federal, State, Local, Public or Private Sector entity) environment, for execution at month ten (10) after award. This information is to be included along with the information required by the following sections of DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00001:

- Section 8.7.3.c, which outlines the requirements for “Technical Approach” for white paper submissions;
- Section 9.6.1.g, which outlines the requirements for “Detailed Technical Approach” for proposal submissions;
- Section 9.6.1.i, which outlines the requirements for “Testing and Evaluation” for proposal submissions; and
- Section 9.6.1.l, which outlines the requirements for “Transition Plan” for proposal submissions.

6.9.5 Describe a “Transition Package Submission for Customer” that addresses all of the supportability requirements for fielding the developed prototype into an operational customer

environment. The Transition Package deliverable should ultimately cover requirements for licensing of any software, hardware requirements, system architectural details, and any interface requirements.

6.9.6 Propose an optional Transition Task for an additional six (6) months. The context for DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00001, section 9.6.1 l (Transition Plan), is for offerors to describe the delivery of a solution that fulfills a capability gap for the homeland security customer. While the option will be dependent on identification of an interested DHS entity or Federal Government partner, offeror's should plan for a monthly level of effort similar to the base effort and factor in delivering updated design documents, user manuals (if applicable), and prototypes, from their base effort, as well as a test plan and a test report. Also, noting that the transition task venue could include Federal, State, Local, Public or Private Sector entities, examples of transition tasking yield the following:

6.9.6.1 A repeatable model for other non-Federal agency communities to integrate (knowledge product);

6.9.6.2 Software to be deployed into a customer's environment; and

6.9.6.3 An enterprise or cloud-based service (Service-based cost).

6.10 Link to Industry Day

An industry day for this solicitation will be held as outlined in the Federal Business Opportunities Notice which can be accessed at the following link:

<https://www.fbo.gov/index?s=opportunity&mode=form&id=b4dddb2ece697bd31211e38e3ce9babf&tab=core&cvview=1>

6.11 Contractual or Technical Inquiries

All contractual or technical inquiries to this BAA solicitation (HSHQDC-14-R-B0014) must be emailed to BAA-14-R-B0005@hq.dhs.gov no later than 4:30 PM EDT on July 21, 2014. Emails submitting questions are to include "Questions for Data Privacy Technologies R&D BAA Solicitation" in the subject line. All questions and responses will be posted on the Federal Business Opportunities website <http://www.fbo.gov>. Questions will only be accepted and answered electronically.

6.12 Order of Precedence

In the event that any of the terms and conditions contained in this solicitation (HSHQDC-14-R-B0014) conflict with terms and conditions included in DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00001, the terms and conditions in this BAA solicitation (HSHQDC-14-R-B0014) shall take precedence.

Footnotes:

1. Federal Information Processing Standards Publication 197, *Advanced Encryption Standard*, 2001. (<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>)
2. OMB Memorandum 06-16, *Protection of Sensitive Agency Information*, 2006. (<http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf>)
3. OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, 2007. (<http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf>)
4. DHS, *Handbook for Safeguarding Sensitive Personally Identifiable Information*, 2012. (<http://www.dhs.gov/xlibrary/assets/privacy/dhs-privacy-safeguardingsensitivepiihandbook-march2012.pdf>)
5. DHS Software Assurance Marketplace (SWAMP); <https://continuousassurance.org/>
6. DHS Homeland Open Security Technologies (HOST); <https://www.dhs.gov/csd-host>

References:

1. Office of Science and Technology Policy, *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*, 2011. (<http://www.cyber.st.dhs.gov/documents.html>)
2. DHS, *A Roadmap for Cybersecurity Research*, 2009. (<http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf>)
3. DHS Sensitive Systems Policy Directive 4300A. (http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_4300a_policy_v8.pdf)
4. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, 2012. (<http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>)