

Amendment
Published: December 19, 2014
Broad Agency Announcement Solicitation HSHQDC-14-R-B0015
Project: Mobile Technology Security

This amendment is identified in Federal Business Opportunities (FBO) as “Amendment 00007;” however, it is the first and only amendment to HSHQDC-14-R-B0015. The numbering for this amendment (Amendment 00007) is portrayed this way in FBO (rather than as the Amendment 00001 to HSHQDC-14-R-B0015) because this solicitation is posted in FBO as “Solicitation 3, CSD BAA Mobile Tech Security” on the same FBO page as the overarching 5-yr CSD BAA, HSHQDC-14-R-B0005. Therefore, FBO identifies this as the next amendment in the sequence of all amendments issued to HSHQDC-14-R-B0005 or any solicitations/calls posted on the same page under the overarching CSD 5-yr BAA.

1. Introduction

1.1 Mobile technology has greatly changed where and how people get work done. However, a lack of security is preventing some businesses from taking advantage of mobility. The lack of security is, in part, due to the economics of the mobile market, a market that is driven by consumers who are quick to adopt and are sold on features and capabilities; not surprisingly, phone developers have focused on that instead of enterprise security requirements. This has led to a model for mobile technology where the User has control over the device settings and its personalization. Additionally, the rise of mobile applications (or “Apps”) has also created the expectation of being able to easily add and remove an App as needed. This is at odds with the traditional approach to enterprise security, which is based upon being able to manage the end device and restrict its functionality and which applications it can load.

1.2 Within the Federal government, the potential impact of mobile technology is clear. Improving the government’s use of mobile technology is a cornerstone element in the 2012 Digital Government Strategy, led by the White House and the Federal CIO’s Council [1, 2]. A survey document, Government Use of Mobile Technology, was created as a follow up to the Digital Government Strategy, and it identifies how the government currently uses mobile technology, as well as barriers and opportunities to expanding its use. The report identified security and privacy as a major gap that needs to be addressed in order to enable more effective use of mobile technologies to meet Government missions.

2. Project Description/Scope

2.1 Increasing Government productivity by leveraging more features available to mobile platforms would benefit all Government agencies, and in response, the Cyber Security Division (CSD), in the Homeland Security Advanced Research Projects Agency within the Department of Homeland Security, Science and Technology Directorate has initiated the Mobile Technology Security project. The Mobile Technology Security project will focus on work needed in the area of security and privacy for mobile technologies. As learned through past efforts to address Federal mobile device security requirements, the solution can’t compromise the benefits of mobile technology and its potential gains in productivity. Solutions that significantly impact the mobile user experience, such as adding too many additional steps to everyday actions or severely

restricting a user's control over the device, will result in a device that doesn't get used. Ideally, a successful security solution would be applicable to a significant range of commercial devices. Government Off-The-Shelf technology should also be avoided because Government-unique solutions typically stagnate and do not benefit from a competitive marketplace (the goals of this BAA solicitation are further described in the next section).

2.2 Current mobile technology security guidelines evolved from an architecture where desktops were the only form of endpoint. However, mobile devices have a number of different capabilities and usage characteristics than desktop computers, and they operate in a different context, so requiring them to mirror the same management and security controls as a desktop is challenging, and may not even result in the same level of security. One possible way to address this challenge is to re-imagine a security strategy that leverages mobile's unique characteristics to provide a more native approach. With the unique security requirements for mobile technology in mind, there are, of course, many desktop-centric security controls that remain valuable for mobile devices. For these controls, the goal would be to find the most efficient way to implement them in a mobile environment. The development of innovative mobile native security solutions and intuitive management tools will allow for the development of more compatible security guidance.

2.3 One of the most obvious differentiators for mobile devices in the enterprise is that they are mobile and used outside of the office, which means they require different security measures, because unlike desktop computers, they are not physically secured by guards and locked doors. However, their mobile nature also means that location can be an important characteristic that can be used to improve security. And the way users physically interact with mobile devices is very different than desktops and the increased number of sensors on devices to detect this interaction can also be used to improve security.

2.4 To users, mobile devices are inherently connected devices and there is little expectation to data stored locally. They are also accustomed to accessing their data divided between multiple apps based upon the type of data it is, each protected by a different authentication process. This is in contrast to desktop environments, where users generally expect to have all their data stored locally and to have complete access to it after authenticating a single time with the operating system. This change in user expectations allows for a transactional approach to securing data. Instead of only having a single opportunity and method for authenticating a user, it is now possible for a system to evaluate risk each time data is requested and either restrict the amount of data returned or request additional authentication if risk is determined to be too great. Risk can be informed by some of the mobile characteristics described above and by the user's pattern of interaction with the system.

2.5 In order for mobile native solutions to be successful, a new approach for managing security is also needed. Instead of managing devices and their configurations, it will also be necessary to manage security at the user level. This means connecting the actions users take with the identities they authenticate over the multiple devices and services they use. Additionally, a combinatorial approach will need to be taken, where a number of indicators taken in concert trigger an alert. In order to make these alerts actionable for security personnel, it will be critical to describe in human terms what led to an alert and the context surrounding it.

3. Technical Topic Areas (TTAs)

3.1 TTA #1: Mobile Device Instrumentation

This TTA seeks approaches for the instrumentation of mobile devices to continuously authenticate a user and perform a risk based assessment of the context in which a device is being used. Offerors should describe risk management from an information processing policy perspective and detail technical implementation of the risk management policy. Further, proposals should relate the risk management implementation to the device specifics and provide explicit parameters for the time intervals necessary to accomplish meaningful continuous authentication, as well as any architectural details pertinent to authenticating across logical boundaries within the device. The key deliverables for this TTA are described in section 4.1.

3.2 TTA #2: Transactional Security Methods

3.2.1 This TTA seeks to generate methods that support a transactional approach to security for accessing data in a mobile device context. This includes both the accessing of data between boundaries on a device and also over a network. Proposed methods should provide a continuum of risk-based responses for data requests in two different contexts:

3.2.1.1 Within a device this could include more granular control over the amount of data and level of detail for sharing data between applications and between the operating system and applications.

3.2.1.2 For accessing data over a network, this includes methods for ascertaining risk that are not reliant on the participation of an end device, but are able to benefit from it. These analyses may include developing a risk framework based on the applications used, patterns of data access, or even the location of the data external to the device.

3.2.2 The key deliverables for this TTA are described in section 4.2.

3.3 TTA #3: Mobile Security Management Tools

This TTA seeks to develop mobile security management tools that will facilitate the Government's increasing use of mobile devices. In particular, DHS is seeking mobile security management tools that operate not only at the device layer, but also incorporate user identities and actions; one approach of particular interest for exploration, are tools that would operate across a range of time rather than generating instantaneous decisions based upon discreet events. Regardless of approach, DHS seeks tools that identify actions, for implementation by either a device user, or security staff, that mitigate security vulnerabilities while presenting information in an actionable way that provides the necessary context around why an event was triggered. The key deliverables for this TTA are described in section 4.3.

3.4 TTA #4: Protecting Mobile Device Layers

Like all information processing platforms, mobile devices have many physical and logical abstraction layers that can be subject to security vulnerabilities. This TTA seeks novel

approaches for protecting the layers and components of a mobile device (e.g., firmware, baseband, and operating system) from infection by a malicious application. This technical topic area may lead to novel methods to re-imagine traditional operational approaches to fixed location computing such as, but not limited to, data at rest, access controls and others. In operation, these approaches may be accomplished through prevention or detection and remediation and, therefore, proposals should describe an operational implementation that relates the proposed approach to NIST Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems [3]. The key deliverables for this TTA are described in section 4.4.

4. Project Structure

To achieve an immediate impact, the Mobile Technology Security project will not be phased, rather it will seek only one and two year efforts, with a six (6) month option for transition to an operational environment or pilot demonstration. To support this project structure, only Type II and Type III proposals will be considered. The optional Transition Task for an additional six (6) months beyond either the one or two year proposed work efforts should focus on the integration or deployment of the completed solution into operation. The option would only be exercised after the successful development and the identification of an interested DHS entity, Federal Government partner, or international partner within the homeland security enterprise. The partnering organization can be identified during the execution of the base effort. Finally, project management will be accomplished by having a kick-off meeting on or about one month following awards being made. There will be progress meetings for DHS to be apprised of developments toward project goals. Go/No-Go demonstrations will occur at the eleventh month of development periods leaving DHS decision time to make decisions on options.

4.1 TTA #1: Key Deliverables

The following key deliverables for TTA #1 are required for each severable year of performance (note: for Type II awards, the version numbers will increase sequentially for year 2):

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
Go/No-Go Demonstration Evaluation Plan	10 months after award
Design Document, Version 3	11 months after award
Working Prototype, Version 2	11 months after award
Go/No-Go Demonstration Report	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 II awards, the version numbers will increase sequentially for year 2):

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
Go/No-Go Demonstration Evaluation Plan	10 months after award
Design Document, Version 3	11 months after award
Working Prototype, Version 2	11 months after award
Go/No-Go Demonstration Report	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 II awards, the version numbers will increase sequentially for year 2):

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
Go/No-Go Demonstration Evaluation Plan	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
Go/No-Go Demonstration Report	12 months after award

4.4 TTA #4: Key Deliverables

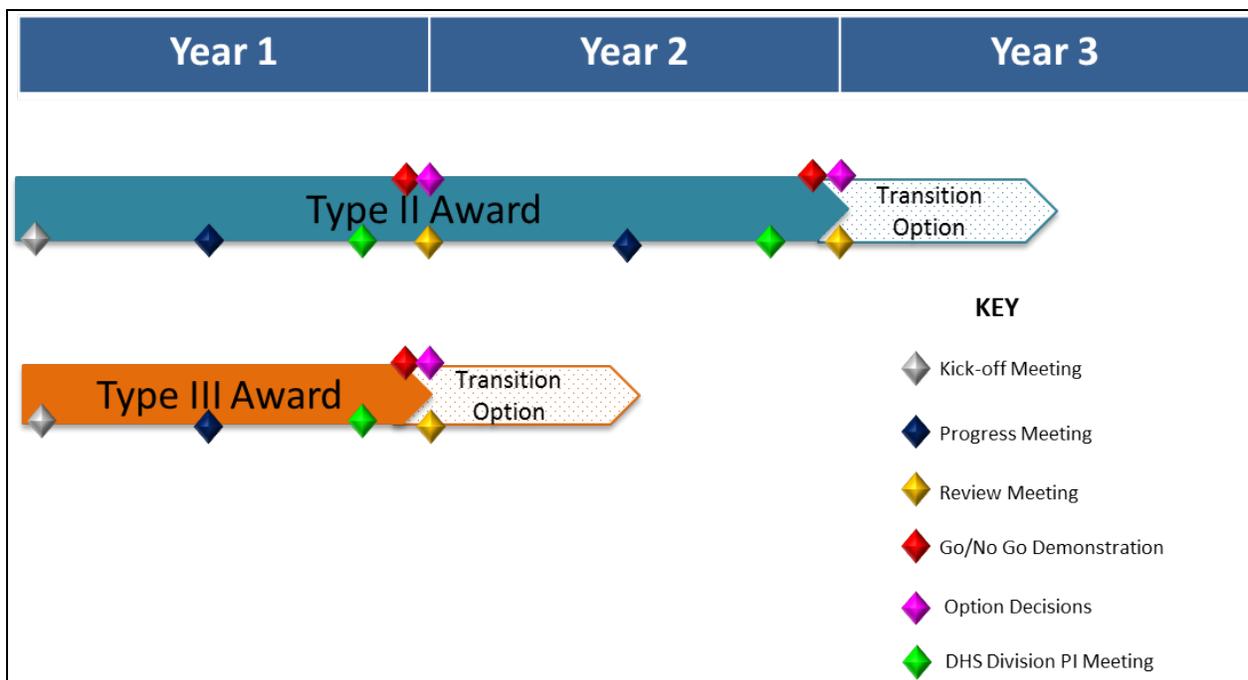
The following key deliverables for TTA #4 are required for each severable year of performance (note: for Type II awards, the version numbers will increase sequentially for year 2):

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
Go/No-Go Demonstration Evaluation Plan	10 months after award
Design Document, Version 3	11 months after award
Working Prototype, Version 2	11 months after award
Go/No-Go Demonstration Report	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 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	4:30 PM EDT	July 22, 2014
Notification of White Paper Evaluation Results	N/A	On or about August 29, 2014
Proposals Due	4:30 PM EDT Eastern Time	September 30, 2014 January 20, 2015

6.2 General Instructions and Information

6.2.1 This BAA solicitation (HSHQDC-14-R-B0015) 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 [00003](#). 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 [00003](#). 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 [00003](#).

6.2.3 Offerors may provide multiple white paper and proposal submissions; however, each submission must be distinct and self-contained without any dependencies on other work of any kind. Additionally, submissions, in either the white paper phase or proposal phase, that address a single TTA will be favored over expansive approaches that address more than one TTA. Therefore, offerors are discouraged from addressing more than one TTA per submission, unless there is a clearly complementary benefit that would yield an integrated result. Each submission must clearly state which TTA is being addressed.

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 (SWAMP) [4].

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 [5] 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, [Amendment 00003](#), 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 [00003](#) [3] Section 11 “EVALUATION OF WHITE PAPERS AND PROPOSALS” applies.

6.2.8 The resulting solution should be sustainable after the completion of the effort and continue to adapt to an evolving mobile marketplace. The required transition plan should

describe how the solution can remain current after the government funded research and development has completed. There are many potential approaches for transitioning technologies to operational use including integration into an existing product or the fostering of an open source community around the effort via licensing. Under any transition scenario described, the approach taken should have a larger target market than government.

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 [00003](#) 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 [00003](#) 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 [00003](#), describes the Type Classifications for proposals. Specific to this solicitation, the ceiling values for each type are as follows:

6.5.1 Type I – Type I awards are not applicable to this solicitation as described above. Any proposal identified as Type I in response to this BAA solicitation will be rejected as non-compliant.

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

6.5.3 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 three project meetings per year.

6.6.2 DHS Cyber Security Division holds an annual PI meeting where all DHS CSD funded efforts 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 Mobile Technology Security 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 [00003](#). Submissions not in compliance with DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment [00003](#), 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). Also, when registering to submit a white paper, the offeror must identify the TTA the white paper responds to, in the case of a white paper that will address more than one TTA, the offeror should register using the TTA that the offeror deems their effort would more completely address.

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 [00003](#), 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 [00003](#). Submissions not in compliance with DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment [00003](#) 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 [00003](#) [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 30 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 [00003](#), 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 or integration into an existing commercial device, the work proposed should be innovative and provide a capability not currently available in the market. Thus 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 four TTAs are being covered. If more than one TTA is being covered, then the submission must describe which TTA is being addressed by the different aspects of the proposed work and clearly differentiate tasks. This information is to be included along with the information required by DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment [00003](#), Section 8.7.3.c, which outlines the requirements for "Technical Approach" for white paper submissions, and Section 9.6.1.g, which outlines the requirements for "Detailed Technical Approach" for proposal submissions.

6.9.2 Identify one or more mobile platforms that the proposed work will target. This information is to be included along with the information required by DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment [00003](#), Section 8.7.3.c, which outlines the requirements for "Technical Approach" for white paper submissions, and Section 9.6.1.g, which outlines the requirements for "Detailed Technical Approach" for proposal submissions.

6.9.3 Define the current security threat model the proposed work will address, indicating where the known vulnerabilities are. This information is to be included along with the information required by DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment [00003](#), 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, and Section 9.6.1.h, which outlines the requirements for "Statement of Work (SOW), Schedule, and Milestones" for proposal submissions.

6.9.4 Define the strategy and development approach to mitigate or remove the vulnerability or impediment. This information is to be included along with the information required by DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment [00003](#), Section 8.7.3.c, which outlines the requirements for “Technical Approach” for white paper submissions, and Section 9.6.1.g, which outlines the requirements for “Detailed Technical Approach” for proposal submissions.

6.9.5 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 [00003](#):

- 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.

6.9.6 As part of defining the Target Capabilities, propose technical and operational metrics that measure progress towards the final capability along with targets specified at 6 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 [00003](#), 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.

6.9.7 Propose a Go/No Go demonstration, for execution at month eleven (11) after award that shows the viability of the approach taken and its potential to address the targeted security threat model. 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 [00003](#):

- 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.

6.9.8 Propose an optional Transition Task for an additional six (6) months. 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. This information is to be included along with the information required by DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment [00003](#), Section 8.7.3.c, which outlines the requirements for “Technical Approach” for white paper submissions, and Section 9.6.1.g, which outlines the requirements for “Detailed Technical Approach” for proposal submissions.

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/spg/DHS/OCPO/DHS-OCPO/Mobile_Technology_Security/listing.html

6.11 Contractual or Technical Inquiries

All contractual or technical inquiries to this BAA solicitation (HSHQDC-14-R-B0015) 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 Mobile Technology Security 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

Additional Information: In the event that any of the terms and conditions contained in this solicitation (HSHQDC-14-R-B0015) conflict with terms and conditions included in DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment [00003](#), the terms and conditions in this BAA solicitation (HSHQDC-14-R-B0015) shall take precedence.

Footnotes:

1. Digital Government: Building a 21st Century Platform to Better Serve the American People <http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf>
2. Government Use of Mobile Technology https://cio.gov/wp-content/uploads/downloads/2012/12/Government_Mobile_Technology_Barriers_Opportunities_and_Gaps.pdf
3. NIST Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>
4. DHS Software Assurance Marketplace (SWAMP); <https://continuousassurance.org/>
5. DHS Homeland Open Security Technologies (HOST); <https://www.dhs.gov/csd-host>

References:

1. Government Mobile and Wireless Security Baseline <https://cio.gov/wp-content/uploads/downloads/2013/05/Federal-Mobile-Security-Baseline.pdf>

2. Guidelines for Managing the Security of Mobile Devices in the Enterprise [NIST Special Publication 800 - 124 Rev 1] <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf>
3. Security and Privacy Controls for Federal Information Systems and Organizations [NIST SP 800-53 Rev. 4] <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>
4. Guidelines for Derived Personal Identity Verification (PIV) Credentials [Draft NIST Special Publication 800 – 157] http://csrc.nist.gov/publications/drafts/800-157/sp800_157_draft.pdf