Amendment
Published: October 3, 2016

Broad Agency Announcement Solicitation HSHQDC-16-R-B0006
Project: Mobile Application Security Research and Development (R&D)

This amendment is identified in Federal Business Opportunities (FBO) as "Amendment 00022;" however, it is the second amendment to HSHQDC-16-R-B0006. The numbering for this amendment (Amendment 00022) is portrayed this way in FBO (rather than as the Amendment 00002 to HSHQDC-16-R-B0006) because this solicitation is posted in FBO as "Solicitation 7, CSD_Mobile_App_Security_BAA_Call-HSHQDC-16-R-B0006." 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. Changes to this solicitation are identified in red with change marks in the left hand margin.

1. Introduction

This BAA solicitation/call (HSHQDC-16-R-B0006) 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 (current issue). All terms and conditions of the DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005 (current issue) apply to this solicitation unless otherwise noted herein. The "current issue" of the DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005 used herein refers to the latest issue posted in Federal Business Opportunities (FBO). It is posted in FBO as DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00013 and incorporates all changes made to date.

Mobile device capabilities are delivered via mobile applications. The ability for users to access and act upon data through mobile technology is changing the way missions are performed. Mobile applications, also known as mobile apps, offer opportunities to improve mission effectiveness and productivity by providing always-on connectivity, real-time information sharing, and unrestricted mobility. User demand for mobile apps includes commercial apps as well as custom-developed apps designed to meet mission needs. However, in part because of the increasing use of mobile apps to access information and services, applications are replacing operating systems as the most prominent avenue of attack [1]. As with traditional desktop and enterprise applications, mobile apps can have security vulnerabilities that could be exploited by attackers to gain access to sensitive government information and resources. Unlike desktop applications, precise location information, contact details, sensor data, photos, and messages can be exposed through mobile apps, and personal information collected by these apps can be sold to marketers or advertising agencies. The combination of traditional software vulnerabilities, the additional information and services accessible through mobile apps, and the sheer number of available mobile apps demands a different approach to application security.

Commercial apps from the official Apple iTunes and Google Play stores are vetted against criteria defined by Apple and Google, respectively. While these criteria include security and privacy considerations, each app store has its own unique, and not necessarily transparent, requirements and vetting processes. Federal agencies cannot assume that a mobile app that is available through an official app store has been vetted in accordance with the agency's security requirements, such as cryptography requirements, nor do they address security throughout the

app's lifecycle.[2] Mobile apps custom developed for the government, whether intended for internal use by the Department/Agency, by state/local governments, or the public, need to be designed, developed and continually assessed for security and privacy issues. The use of shared code available from multiple sources worldwide and the rapid refresh cycle of mobile apps exacerbate security concerns with commercial and custom apps.

The need for standardized, cost effective methods and tools to develop, vet, deploy and manage mobile apps has been identified as a key enabler to the federal government's adoption of mobile technologies. Reports and activities of the Federal Chief Information Officers Council and its Mobile Technology Tiger Team have consistently raised concerns about mobile app security and the cost of vetting apps as barriers to expanded use of mobile technologies [3, 4].

2. Project Description/Scope

The mobile application lifecycle can be defined by the following phases identified in Figure 1: application concept; application development; pre-deployment test and evaluation; application deployment; and application maintenance. A holistic approach to building security into an application and providing a means for continuous evaluation is needed.

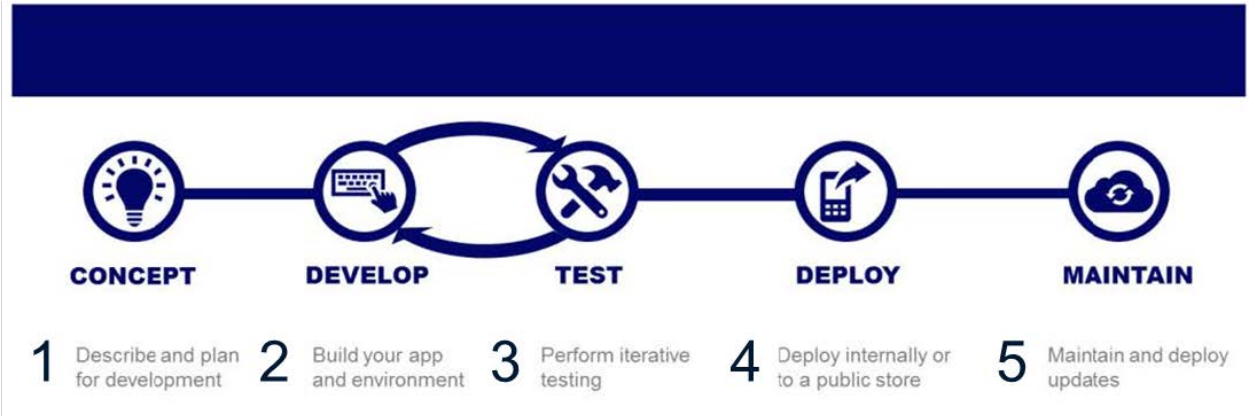


Figure 1: Mobile Application Lifecycle [5]

The commercial sector has responded to the need for more secure mobile devices and mobile application security by refining device capabilities and operating systems and by providing products and services that evaluate applications against a set of security characteristics. Application vetting solutions are often point solutions, meaning any changes to the application require re-applying the vetting process. Also, application vetting products often employ proprietary means of evaluating the security of an application with inconsistent reference to standards or criteria. Additionally, solutions may employ a multitude of test types. Current tool vendors have three basic approaches to automated analysis: Static, Dynamic, and Behavioral Analysis. Within Static Analysis, there are two methodologies used to evaluate the raw code with the use of available source code, and analysis of binary code. The option to utilize binary for Static Analysis originated from the fact that source code is normally unavailable, so the scanning of binary code became an alternative. Thus, there is a need to extend and build upon commercial app vetting to provide a consistent security determination framework across mobile app sources or stores. One step in this direction is the coordination between DHS S&T Directorate, HSARPA, Cyber Security Division and the National Information Assurance Partnership (NIAP)

program to automate the NIAP protection profile requirements for vetting mobile applications, while demonstrating quality (e.g., sufficient evidence) efficiency, and minimize overall costs.

A separate, but closely related need, is the ability to update threat and vulnerability data as it develops, so that applications are continually evaluated against the current threat environment. Additionally, there is a need to provide some measure of protection against threats that have yet to be discovered but that may be variants of known malicious or vulnerable code, or threats that exhibit known malicious behavior (e.g., command and control).

To proliferate secure mechanisms into the mobile device ecosystem, DHS S&T has initiated the Mobile Application Security Research and Development (R&D) project. This project will seek automation and incorporate-security-by-design into a series of security tools for mobile apps that assist developers, analysts, and security or network operators.

3. Technical Topic Areas (TTAs)

The objective of this Broad Agency Announcement (BAA) call is to identify innovative approaches that extend beyond deployment of an app to provide continuous assurance of mobile app security throughout an app's lifecycle; and the following TTAs capture the desired focus of research and development to support this objective. Specifically, TTA #1 is focused on the continuous monitoring, vetting, and security assurance of mobile applications to safeguard against vulnerabilities and future threats. In this case, proposed innovation in TTA #1 may consider incorporation with enterprise mobility management (EMM) solutions and should assist analysts and security/network operators to defend the IT enterprise and enable the development of secure mission-centric apps for mobile platforms. TTA #2 will establish a security framework and integrated models for enabling the development of mobile applications for mission use. As a result, the focus of TTA #2 is targeted toward the creation and development of individual apps and security verification throughout the mobile application lifecycle. TTA #2 proposed innovation shall consider mobile app development platforms and should enable developers to ensure security and functionality are reliable and optimized to support mission needs.

3.1 TTA #1: Continuous Validation & Threat Protection for Mobile Applications

This TTA seeks innovative approaches to validating security throughout a mobile application's operational use, as measured against the security criteria established by the Federal Mobile Application Security Vetting Working Group and currently maintained by National Information Assurance Partnership (NIAP) [6]. Also, this TTA seeks to develop capabilities, specific to the mobile device operating environment, to respond to current known threats and vulnerabilities, including, but not limited to the identification of malware or the identification of vulnerable code. This entails developing the capability to anticipate and, if needed, react to future threats and vulnerabilities while continuously monitoring a mobile device's security posture.

3.1.1 Goal #1 – Actionable Threat and Vulnerability Analytics for the Enterprise. To create the capability to respond to current known threats and vulnerabilities is a goal of this TTA because it is an enabler for continuous validation of security posture for mobile applications. Thus, technical approaches must describe the continuous monitoring of mobile applications, continuous vetting against known vulnerabilities, coding and configuration flaws, and mobile threat intelligence. Another characteristic that is desired for the continuous validation capabilities, are tools to protect against future threats. Ideally, these tools would provide

predictive security for mobile apps, or use mobile app security to detect a range of mobile malware or even extend its application to rogue base stations, for example.

3.1.2 Goal #2 – Mobile Threat Integration and Situational Awareness. Threat and vulnerability information sharing is a proven method to reduce the number of exploits. Applying this principle to mobile apps, a goal of this TTA is the exploration and development of methods to integrate federal or commercial sources of known or newly-discovered vulnerabilities and threats to mobile devices, mobile enterprises and mobile infrastructure. A notional approach could address developing a mobile app focused system integrating threat information sources (e.g., US-CERT Cyber Security Alerts and Bulletins, NIST National Vulnerability Database, Open Web Application Security Project [OWASP], proprietary sources) and providing a mechanism to notify the app developer which app by version(s) and where the vulnerabilities are present. Ultimately, this goal is intended to lead to a system that provides actionable mitigation responses to threat intelligence. Therefore, technical approaches must explore multiple avenues of threat intelligence to ensure current information is incorporated into their solution. Further, technical approaches should address remediation capabilities to mitigate new vulnerabilities as they are discovered. Ideally, the intelligence source integration will include an automated capability to respond to threat/vulnerability data resulting in some action on the application, such as sequestration, removal, updating with newer secure versions, or providing an alternative mobile app with similar functionality. Demonstrating that the total solution can react to this information will be a key component of any evaluation.

3.1.3 Goal #3 – Initial Operational Capability (IOC) Pilot. A goal of this TTA is to support verification that targeted capabilities have been achieved and are demonstrable in an operational setting through piloting. With Go/No-Go decision points that will occur on six (6) month intervals, technical approaches should include a description of a pilot, which will serve as the Go/No Go milestone eighteen months after contract award, to occur in a Federal Government or enterprise setting. This pilot will demonstrate Initial Operational Capability (IOC). The IOC pilot should describe information technology (IT) infrastructure integration and operational use of the technology developed. For example, pilots may need to integrate with an organization's authentication capabilities or with existing mobile infrastructure such as enterprise mobility management solutions. Pilots should also account for the intended organization's infrastructure.

3.2 TTA #2: Integrating Security throughout the Mobile Application Lifecycle

To enable incorporation of security mechanisms into the mobile app development process, this TTA seeks approaches and implementations to fortify mobile app development tools with functionality that, transparently to the developer, incorporates secure mechanisms as mobile apps are developed.

3.2.1 Goal #1 – Security Framework for Mobile Application Development. Identifying and fixing weaknesses in a mobile app during development will help to reduce the attack surface for mobile apps, as well as reduce the cost of software failures by finding weaknesses before they expose vulnerabilities or result in exploits. Technical approaches must address this goal by detailing an approach to develop and deliver an assessment and remediation tool(s) for correlation against known vulnerabilities while identifying specific mobile app development environments and targeted mobile devices.

3.2.2 Goal #2 – Integration with Mobile App Development Platforms. Recognizing that mobile application development has different challenges than traditional software development [7]. S&T is looking for comprehensive solutions that address security during development and throughout the mobile application lifecycle (see Figure 1). Technical approaches shall consider incorporating the monitoring of app performance and behavior, ensuring security compliance, and continuously assessing security risk. Possible remediation activities could include the response to threat/vulnerability data to perform some action on the application and device, such as sequestration, removal, or updating with newer secure versions. Given the unique nature of mobile technology, technical approaches must consider integration into existing commercially-available development environments, which would ensure that the capability can be used during development.

3.2.3 Goal #3 – Initial Operational Capability Pilot.
A goal of this TTA is to support verification that targeted capabilities have been achieved and are demonstrable in an operational setting through piloting. With Go/No-Go decision points that will occur on six (6) month intervals, technical approaches should include a description of a pilot, which will serve as the Go/No Go milestone eighteen months after contract award, to occur in a Federal Government or enterprise setting. This pilot will demonstrate Initial Operational Capability (IOC). The IOC pilot should describe information technology (IT) infrastructure integration and operational use of the technology developed. For example, pilots may need to integrate with an organization's authentication capabilities or with existing mobile infrastructure such as enterprise mobility management solutions. Pilots should also account for the intended organization's infrastructure.

4. Project Structure

To keep pace with the mobile threat environment, the Mobile Application Security project emphasizes frequent evaluations and requires piloting. Section 5 shows the project schedule and milestones, which includes progress meetings for DHS to be apprised of development toward project goals, and a required Go/No-Go demonstrations on six (6) month intervals (excluding the Pilot Option). The optional Pilot Task for an additional six (6) months beyond the proposed technology development R&D work effort should focus on the integration and/or deployment of the completed solution into operation, as coordinated with DHS. The Pilot option would only be exercised after the successful development and 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 award. Key technical deliverables, pilot deliverables, and program status deliverables, are listed below.

In addition, the intent of the Go/No-Go decision points on six (6) month intervals is to allow the Government to have flexibility to not only ensure that technical progress is being achieved, but also to adapt to trending mobile technologies; as such, award terminations may occur based on the Go/No-Go determinations.

4.1 Project Status Deliverables

The following project status deliverables are required throughout the period of performance:

DELIVERABLE	DUE DATE
Presentation Materials from Project Meetings	Within five (5) days of presentation
Monthly Technical Status Reports	Starting on the fifteen (15) day of the month, beginning in the calendar month after award, and the fifteen (15) day of each month thereafter throughout the period of performance.
Monthly Financial Status Reports	Starting on the fifteen (15) day of the month, beginning in the calendar month after award, and the fifteen (15) day of each month thereafter throughout the period of performance. May be sent with the Monthly Technical Status Report.
Program Reviews	3 and 5 months after award of the base period, and 4, 8 and 11 months after the exercise of each option thereafter

4.2 Key Technical Deliverables

The following key deliverables are required for each severable period of performance (note: for Type I and Type II awards, the version numbers will increase sequentially for each year):

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	5 months after award
Target Capabilities Definition Document, Version 2	5 months after award
Working Prototype, Version 1	5 months after award
Go/No-Go Demonstration Evaluation Plan	5 months after award
Go/No-Go Demonstration	5 months after award
Go/No-Go Demonstration Report	6 months after award
Go/No-Go Demonstration Evaluation Plan	10 months after award
Design Document, Version 3	11 months after award
Target Capabilities Definition Document, Version 3	11 months after award
Working Prototype, Version 2	11 months after award
Go/No-Go Demonstration	11 months after award
Go/No-Go Demonstration Report	12 months after award

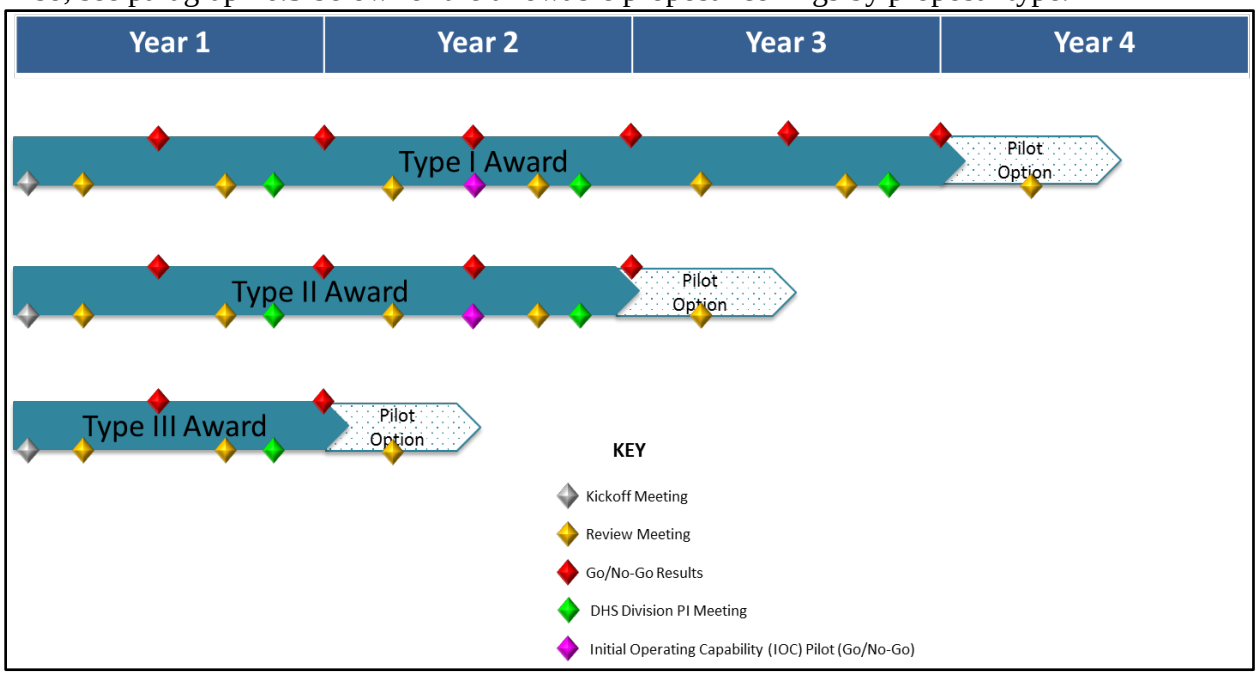
4.3 Pilot Deliverables

The following key deliverables are required for all pilots, including the Pilot Option:

DELIVERABLES	DUE DATE
Pilot Demonstration Plan	1 month before Pilot execution
Pilot Demonstration Report	1 month after Pilot execution

5. Project Schedule/Milestones

A notional schedule is shown below including anticipated milestones, meetings and demonstrations for each proposal type as defined by BAA HSHQDC-14-R-B0005 paragraph 2.2. Also, see paragraph 6.5 below for the allowable proposal ceilings by proposal type.



6. Special Instructions/Notifications

6.1 Response Dates

Event	Time Due	Date Due
Industry Day	N/A	June 9, 2016
White Papers Due	4:30 PM EDT	August 1, 2016
Notification of White Paper Evaluation Results	N/A	On or about ~~September 30, 2016~~ October 17, 2016
Proposals Due	4:30 PM EST	~~November 17, 2016~~ December 5, 2016
Notification of Proposal Selections	N/A	~~February 8~~ February 22, 2017

6.2 General Instructions and Information

6.2.1 This BAA solicitation (HSHQDC-16-R-B0006) 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 (current edition). 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 (current edition). 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 (current edition).

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 Given the rate of change in mobile technologies in the marketplace and related threats, DHS intends to conduct Go/No-Go evaluations on six (6) month intervals; decisions to terminate awards thereafter may be made.

6.2.5 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 penetration testing to ensure functionality and security for all software deliverables. This is intended to support readiness for deployment.

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 (current edition) [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.

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 (current issue) 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 (current issue) 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 (current issue), 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 limited to a total contract value not to exceed $2,500,000.00, not including the Pilot Option which may be proposed for up to six (6) months.

6.5.2 Type II –Type II awards are limited to a total contract value not to exceed $2,000,000.00, not including the Pilot Option which may be proposed for up to six (6) months.

6.5.3 Type III – Type III awards are limited to a total contract value not to exceed $1,000,000.00, not including the Pilot Option which must be proposed for up to six (6) months, using paragraph 6.9.6 as a guideline. Any proposal identified as Type III in response to this BAA solicitation that does not include a Pilot Option will be rejected as non-compliant.

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 required 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 Application Security Project will hold two program review meetings each year. Meetings may 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 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 (current edition). Submissions not in compliance with DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005 (current edition), 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 (current edition), 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 (current issue). Submissions not in compliance with DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005 (current issue) 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 (current issue) [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 (current issue), 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 offeror'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 Proposals

Given a goal of this BAA solicitation is to develop solutions that are mature enough for deployment or integration into an existing mobile technology enterprise, 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 two 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, (current issue), 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 environments 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 (current issue), 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 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 (current issue):

- 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.

6.9.4 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 (current issue), 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.

6.9.5 Go/No Go Demonstrations. Go/No Go demonstrations are required to be proposed for execution on six (6) month intervals after award. Go/No Go demonstrations must describe how target capabilities will be verified. . Also, Go/No-Go evaluation data must be addressed in the Data Management Plan, described below, for incorporation into DHS' Information Marketplace for Policy and Analysis of Cyber-risk & Trust (IMPACT) program (https://www.impactcybertrust.org), if appropriate. 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 (current issue):

- 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 Pilot Option Scoping. Parameters for the optional (but required for Type III proposals) Pilot 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 (current issue), 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.

6.9.7 Data Management Plan. All proposals must include a data management plan (DMP). The DMP should be no more than two pages and must be included at the end of Volume 1. The DMP does not count toward the page limit in 6.8.1and is required to address the following:

- The types of data, metadata, samples, physical collections, software, curriculum materials, and other materials to be collected and/or generated in the course of the project;
- The standards to be used for data and metadata format and content (where existing standards are absent or deemed inadequate, this should be documented along with any proposed solutions or remedies);
- The physical and/or cyber resources and facilities (including those supplied by third parties) that will be used to store and preserve the data after the award ends;
- The policies for access and sharing including provisions for appropriate protection of privacy, confidentiality, security, intellectual property, or other rights or requirements;
- The policies and provisions for re-use, re-distribution, and the production of derivatives;
- The plans for archiving data, samples, and other research products, and for preservation of access to them after the award ends; and
- The roles and responsibilities of all parties with respect to the management of the data (including contingency plans for the departure of key personnel from the project) after the grant ends.

The DMP should reflect best practices in the relevant research community and be appropriate for the data to be generated as part of the proposed activities.

Definition:
As noted in the Code of Federal Regulations (2 CFR 215.36), "research data" is defined as:

> *"the recorded factual material commonly accepted in the scientific community as necessary to validate research findings, but not any of the following: preliminary analyses, drafts of scientific papers, plans for future research, peer reviews, [or]*

communications with colleagues. This "recorded" material excludes physical objects (e.g., laboratory specimens)."

This definition includes not only original data but also "metadata" (e.g., experimental protocols, software code written for statistical or experimental analyses or for proofs-of-concept, etc.).

Additional Guidance for DMP Content:
The DMP should clearly articulate how the offeror plans to manage and disseminate data generated by the project. The plan should outline the rights and obligations of all parties as to their roles and responsibilities in the management and retention of research data. It should describe how the research team plans to deposit data into any relevant and appropriate disciplinary repositories (e.g., see https://www.impactcybertrust.org and https://continuousassurance.org) that are appropriately managed and that are likely to maintain the metadata necessary for future use and discovery.
The DMP should describe the types of data, metadata, scripts used to generate the data or metadata, experimental results, samples, physical collections, software, curriculum materials, or other materials to be produced in the course of the project. The plan should then describe the types of data to be retained, managed, and shared, and the plans for doing so. The DMP should cover the following, as appropriate for the project:

- the period of time the data will be retained and shared;
- how data are to be managed, maintained, and disseminated;
- factors that limit the ability to manage and share data, e.g., legal and ethical restrictions on access to human subjects data;
- provisions for appropriate protection of privacy, confidentiality, security, and intellectual property;
- mechanisms and formats for storing data and making them accessible to others, which may include third party facilities and repositories; and
- other types of information that would be maintained and shared regarding data, e.g. the means by which it was generated, detailed analytical and procedural information required to reproduce experimental results, and other metadata.

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/Movile_Application_Security_Industry-Day/listing.html

6.11 Contractual or Technical Inquiries
All contractual or technical inquiries to this BAA solicitation (HSHQDC-16-R-B0006) must be emailed to BAA-14-R-B0005@hq.dhs.gov no later than 4:30 PM EDT on July 26, 2016. Emails submitting questions are to include “Questions for Mobile Application 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-16-R-B0006) conflict with terms and conditions included in DHS S&T

CSD 5-Year BAA HSHQDC-14-R-B0005 (current issue), the terms and conditions in CSD 5-Year BAA HSHQDC-14-R-B0005 shall take precedence.

References:

1. Hewlett Packard Enterprise Cyber Risk Report 2016, Theme #6: Attackers have shifted their efforts to directly attack applications http://www8.hp.com/us/en/software-solutions/cyber-risk-report-security-vulnerability/)
2. National Institute of Standards and Technology (NIST) Special Publication 800-163, Vetting the Security of Mobile Applications, January 2015.
3. Use of Mobile Technology—Barriers, Opportunities, and Gap Analysis. https://cio.gov/cio-council-report-on-barriers-gaps-opportunities-for-government-use-of-mobile-technology/
4. Government Mobile and Wireless Security Baseline https://cio.gov/wp-content/uploads/downloads/2013/05/Federal-Mobile-Security-Baseline.pdf
5. MOBILE APPLICATION PLAYBOOK (MAP), U.S. Department of Homeland Security (DHS), Office of the Chief Technology Officer (OCTO) http://www.atarc.org/wp-content/uploads/2016/04/DHS-Mobile-Application-Playbook.pdf
6. National Information Assurance Partnership (NIAP) - https://www.niap-ccevs.org/
7. NIST Special Publication 800-163 (Draft), http://csrc.nist.gov/publications/drafts/800-163/sp800_163_draft.pdf