

Amendment
Published: December 21, 2015

Broad Agency Announcement Solicitation HSHQDC-16-R-B0002
Project: Static Tool Analysis Modernization Project (STAMP)

This amendment is identified in Federal Business Opportunities (FBO) as “Amendment 00015;” however, it is the second amendment to HSHQDC-16-R-B0002. The numbering for this amendment (Amendment 00015) is portrayed this way in FBO (rather than as the Amendment 00002 to HSHQDC-16-R-B0002) because this solicitation is posted in FBO as “Solicitation 5, CSD BAA Call STAMP” 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

1.1 This BAA solicitation/call (HSHQDC-16-R-B0002) 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.

1.2 The current state-of-the-art static analysis software tools have not kept pace with modern software. For example, no software analysis tool was able to find the weakness or flaw in OpenSSL that exposed the Heartbleed vulnerability. The complexity and size of software make it more difficult for software analysis tools to perform. Oftentimes these tools have difficulty tracking data flows through complex and large software systems, to the point that software analysis tools oversimplify and make assumptions about software code that is inaccurate. As indicated in the whitepaper, “Why Do Software Assurance Tools Have Problems Finding Bugs like Heartbleed”, these inaccurate assumptions cause the tools to miss things, which reduces the fidelity of the analysis results.

1.3 Detecting weaknesses that could lead to vulnerabilities before it leaves a software developer’s desktop would reduce the cost of software failures, while also reducing the overall attack surface of the software system. Studies have shown that developers are less likely to use software analysis tools if they generate a considerable amount of false-positives. With the rise of DevOps and SecDevOps, software analysis tools need to work “At Speed”, and hook into a developer’s continuous integration pipeline to help improve not only tool adoption, but continuous delivery of secure software that supports an organization’s mission. Today’s software development process is agile and moving faster, current software analysis tools and technologies must keep pace with this growing demand and trend. Improving the capabilities

and techniques in software analysis tools will give developers more confidence in using them earlier in the software development process.

2. Project Description/Scope

2.1 There are a host of free and open-source static analysis tools that have been neglected and, therefore, underperform meaning they are not relevant for use. Modernization of these static analysis tools is needed to help advance and improve software analysis capabilities, because lower cost software analysis tools will make secure software more prevalent. Innovation in software analysis capabilities is needed to keep pace with the evolution in software systems; to improve static analysis tools there must be advancements in research and development to discover new techniques, methods, services, and capabilities in testing and evaluating software for critical weaknesses and flaws that expose vulnerabilities. This BAA solicitation/call, Static Tool Analysis Modernization Project (STAMP), is focused on closing the gaps in two key areas: research and development, and implementation, of new techniques for static software analysis; and applying new and improved testing and evaluation activities capabilities.

The goal of STAMP is to modernize a list of candidate software analysis tools to improve tool performance and coverage, to seamlessly integrate and support continuous integration and DevOps operational environments, and provide stronger analysis of results by reducing false-positives, and provide more visibility into false-negatives that often leave residual risks. STAMP should be designed to create new techniques that advance the state-of-the-art capabilities found in software analysis tools.

3. Technical Topic Areas

This STAMP BAA solicitation/call is comprised of four technical topic areas (TTAs), as follows: developing a test case generator; conducting tool study and analysis based on derived test cases; developing a modernization framework base to close gaps that exist in software analysis tools; and developing a tool scoring and labeling capability to identify strengths and weaknesses areas of software analysis tools. The TTAs are intended to accomplish the following, which are STAMP goals:

- Improve the quality and performance of software analysis tools by creating new, comprehensive quantifiable test cases using complex code structures that model real programs.
- Identify gaps in tool coverage areas in open-source and state-of-the-art software analysis tools
- Explore innovation and deliver new techniques and capabilities for vetting mobile applications
- Create capability to benchmark, score, and label software analysis tools
- Provide a consumer report with detailed analysis to better educate and assist organizations regarding software analysis tool selection process
- Modernize capabilities and techniques in open-source tools
- Provide deeper support analysis for dynamic programming languages
- Develop a robust scanning engine that can scale large and complex code bases

The interactions between the TTAs are shown below in Figure 1, which depicts a conceptual representation of how each TTA relates to other TTAs. Based on the TTA relationships, STAMP is anticipated to be a phased development, notionally captured in Figure 3, where the results of TTA #1 and TTA #2 will be used in the development efforts of TTA#3 and TTA #4.

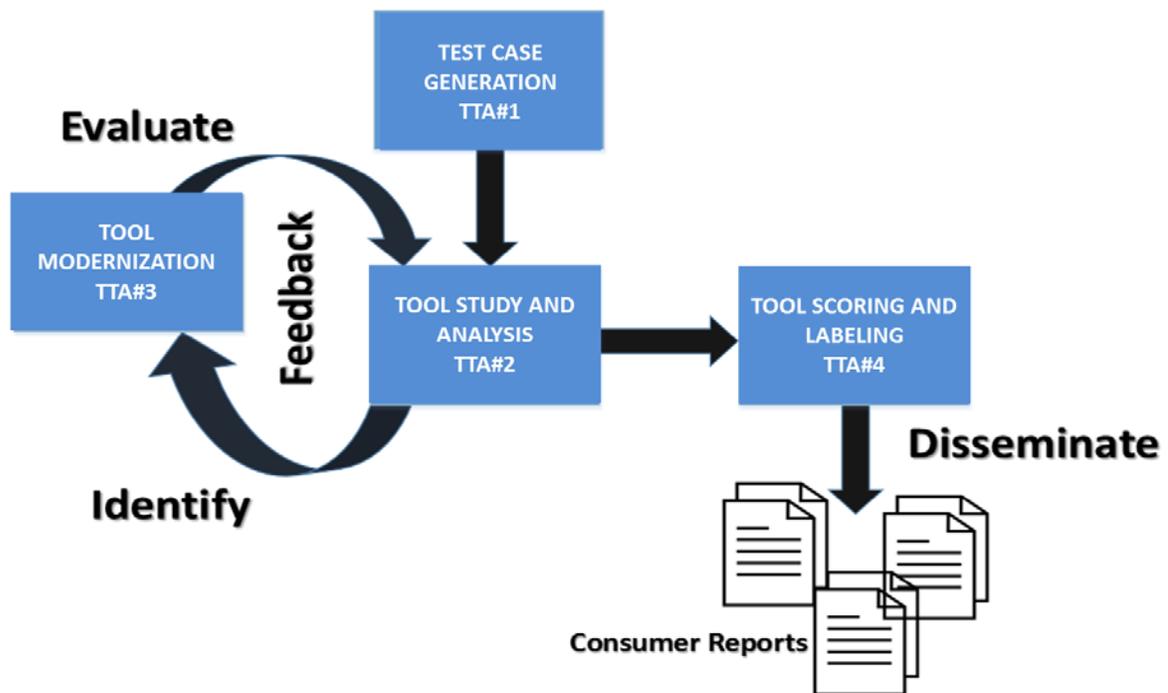


Figure 1 – STAMP TTA interactions

3.1 TTA #1 Test Case Generator

In order to assess the strengths and weaknesses, and to determine the gaps in software analysis tools, a test case generator prototype will need to be created to measure the performance of tools and determine tool coverage. This work is required to build off the Juliet Test Suite¹ and the Center for Assured Software (CAS) Static Analysis Tool Study – Methodology² to help evolve software analysis tools. The deliverables required for TTA #1 are in Section 4.2. To align with STAMP goals, the test case generator is required to address following objectives:

3.1.1 Objective 1 – Development of a set of test cases of complex code constructs to be used to improve the quality of static analysis tools. These test cases should represent examples of “real programs” and would be used to evaluate software quality assurance tools in the area of precision and soundness (recall)², where the context of “precision” and “soundness (recall)” is below.

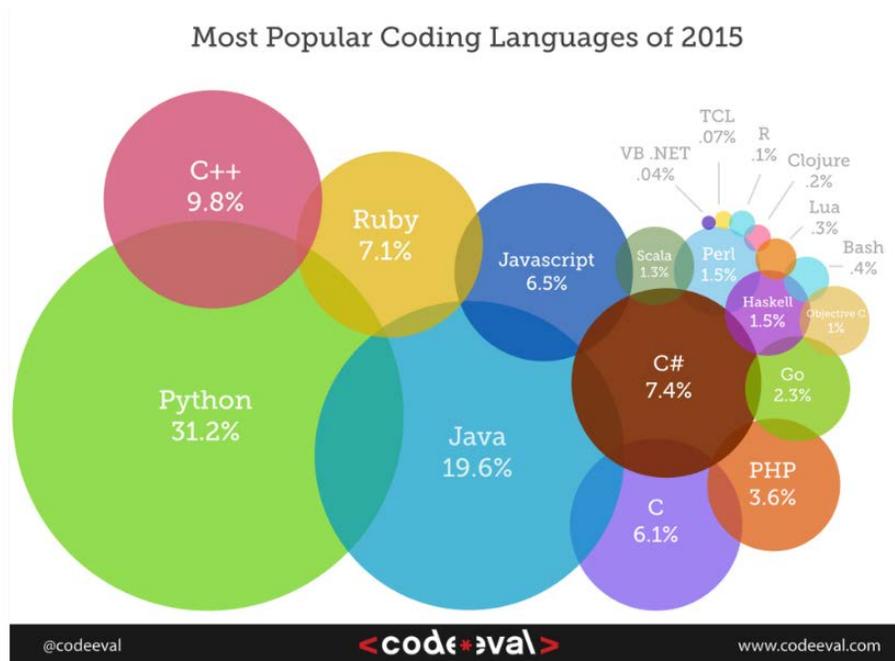
- Precision: Precision describes how well a tool identifies flaws. A tool that achieves precision by only reporting issues that are real flaws on the test cases. That is, it does not report any false positives.

- Soundness (recall): Soundness (recall) determines the extent a tool correctly identified the target weaknesses within the test cases.

3.1.2 Objective 2 – Development of a diverse set of code constructs to include both static and dynamic programming languages. Presently, the Juliet test suite only covers Java and C/C++, but this objective is intended to enhance the capabilities of the Juliet test suite. The diagram in Figure 2 is an example of static and dynamic programming languages in 2015 and should be considered as one of many references that could be used to formulate and prioritize which programming languages to address when proposing code constructs.

3.1.3 Objective 3 – To transition and integrate test case generator into the Software Assurance Marketplace (SWAMP)³ as part of the SWAMP’s corpus of software. This is intended to help provide the continuous assurance capabilities in the SWAMP that will help improve the existing software assurance tools hosted in the SWAMP, in addition to assisting software assurance researchers in finding new advancement in software assurance capabilities.

3.1.4 Objective 4 – To coordinate with the National Institute of Standards and Technology (NIST) to ensure sure that test cases, and associated datasets, are incorporated into the Static Assurance Metrics and Tool Evaluation (SAMATE)⁴ program. This is intended to proliferate benchmarks to measure tool performance and tool coverage.



Most Popular Coding Languages of 2015

Figure 2 – Popular Programming Languages for 2015⁵

3.2 TTA #2 Tool Study and Analysis

Understanding what a tool can and cannot do is important to help identify gaps in tool coverage to improve. Related to software analysis tools, a systematic approach to understand tool characteristics, tool behavior and tool performance capabilities, to analyze software for weaknesses and vulnerabilities is needed. Implementing a systematic approach to software tool analysis should identify the gaps in tool capabilities and lead to the development of a modernization strategy that identifies software assurance candidate tools for improvement. With the aforementioned backdrop, this TTA is intended for offerors to propose an approach to identifying a candidate list of static analysis tools for modernization that factors in a comparison of current capabilities with the best capabilities of the state-of-the-art. The deliverables required for TTA #2 are in Section 4.3, and to align with STAMP goals, this TTA requires an approach addressing the following objectives:

3.2.1 Objective 1 - Identification and selection of a list of ten (10) candidate tools to modernize as part of STAMP, which may include free and open-source software analysis tools, as well as commercial tools.

3.2.2 Objective 2 - Development of criteria for scoring² and rating tools⁶ as referenced in TTA#4.

3.2.3 Objective 3 - Identification of baseline capabilities required of static analysis tools. The baseline capabilities are required to identify gaps in tool coverage, understand tool characteristics, model the behavior of each tool across programming languages and weakness classes, measure performance and develop analytics to identify commonalities in tool characteristics, behavior and performance.

3.3 TTA #3: Tool Modernization

The phased approach to STAMP should lead to a repeatable analysis methodology for identifying and updating static analysis tools, while also identifying tools not worth updating, with enhanced. This TTA will start with a review of the candidate list developed and baseline capabilities list required of static analysis tools for TTA#2 and then choose four to six, at the discretion of the proposer, for modernization and enhancement. The resulting decision process will be documented to establish a process for the development of research criteria for modernizing static analysis software tools. The deliverables required for TTA #3 are in Section 4.4, and to align with STAMP goals, this TTA requires an approach addressing the following objectives:

3.3.1 Objective 1 - Development of a modernization framework to be used to improve the capabilities in candidate tools. This framework should encompass new techniques, methods, services and capabilities in the candidate tools. Technical approaches must also address soundness and precision that can scale across multiple languages (at the discretion of the offeror), as well as weakness classes.

3.3.1 Objective 2 - Documentation of a detailed and comprehensive analysis report describing improvements to candidate tools, and gaps that still exist in the candidate tool coverage.

3.3.1 Objective 3 - Transition and integrate candidate tools to the SWAMP.

3.3.1 Objective 3 - Delivery of static analysis tools at a Technology Readiness Level⁷ 6 maturity.

3.4 TTA #4: Operational Pilot Implementing Tool Scoring and Labeling

DHS is seeking to support transition of the STAMP products into use into appropriate operational environments through operational pilot evaluation. To facilitate the pilot and identification of appropriate operational venues for STAMP piloting, a scoring and labeling tool is needed to guide federal organizations purchasing and acquiring software analysis capabilities. Currently there is no way to ascertain the residual risks associated with using software analysis tools. The deliverables required for TTA #4 are in Section 4.5, and to align with STAMP goals, this TTA requires an approach addressing the following objectives:

3.4.1 Objective 1 - Development of a comprehensive scoring framework to assess the performance of software quality assurance tools. The developed framework should include software assurance labels presented in a way that could better educate acquirers regarding tool coverage, tool strengths and weaknesses, and tool characteristics.

3.4.2 Objective 2 - Document a methodology for combining multiples tools to improve tool coverage and determine tool features and characteristics that can be used to mix and match tools.

3.4.3 Objective 3 - Coordination with NIST to establish guidance for selecting software analysis tools and developing a benchmark that can be used to rate and rank software analysis tools to help decision makers in procuring/acquiring software analysis tools and capabilities.

3.4.4 Objective 4 - Document analysis of Common Weakness Enumeration (CWE) coverage and mappings to NIST SP 800-53A for FISMA compliance to support understanding static analysis tool coverage.

4. Project Structure

The STAMP project is structured into a one year base period and three (3) one year options where the third option is for operational pilots. Key deliverables for each TTA are described below and should be planned for in conjunction with the Statement of Work severability requirements HSHQDC-15-R-B0005, paragraph 9.6 h are required for each severable year of performance.

4.1 Project Deliverables

The project-level deliverables required are:

DELIVERABLE	DUE DATE
Base and Option Periods	
Presentation Materials from Project Meetings	Within five (5) days of presentation
Quarterly Technical Status Reports	Starting 105 days after award, and every ninety (90) days thereafter throughout the base period of performance. For last 75 days of base period, report due 5 days prior to end of base period of performance. For each option period, report due every 90 days from effective date of option.
Monthly Financial Status Reports	Starting 45 days after award, and every thirty (30) days thereafter throughout the base period of performance. For last 15 days of base period, report due 2 days prior to end of base period of performance. For each option period, report due every 30 days from effective date of option.
Program Reviews	6 and 11 months after award and exercise of each option thereafter
Option Period 1	
Go/No-Go Demonstration	10 months after award of Option 1
Go/No-Go Demonstration Report	11 months after award of Option 1
Annual Report including SWAMP Integration	12 months after award of Option 1
Option Period 2	
Go/No-Go Demonstration	10 months after award of Option 2
Go/No-Go Demonstration Report	11 months after award of Option 2
Annual Report including SWAMP Integration	12 months after award of Option 2

4.2 TTA #1 Key Deliverables

The key deliverables required for TTA #1 are:

DELIVERABLE	DUE DATE
Base Period	
Testcase Development Methodology	90 days after award
Initial Code Constructs	6 months after award
Report of SAMATE coordination	6 months after award
Analysis report identifying selection of programming languages and weakness class coverage for the planned Test Case Generator Prototype	9 months after award

Option Period 1	
Initial Test Cases and Test Datasets	3 months after award of option period 1
Test Case Generator Prototype Design document for test cases that outlines features and characteristics of code constructs	4 months after award of option period 1
Test Case Generator Prototype	6 months after award of option period 1
Package of data sets for test cases	8 months after award of option period 1

4.3 TTA #2 Key Deliverables

The key deliverables required for TTA #2 are:

DELIVERABLES	DUE DATE
Base Period	
Analysis document of candidate tools	60 days after award
Analysis document on tool coverage	6 months after award
Tool study report that provides detailed analysis of strengths and weakness in tools, Version 1	9 months after award
Technical report on overlapping tool coverage and complimentary tool coverage	12 months after award
Option Period 1	
Technical report outlining tool benchmark scoring criteria	3 months after award of option period 1
Modernization framework report to support Phase 2	3 months after award of option period 1
Final tool study report that provides detailed analysis of strengths and weakness in tools, Version 2	6 months after award of option period 1
Technical report on overlapping tool coverage and complimentary tool coverage	6 months after award of option period 1

4.4 TTA #3 Key Deliverables

The key deliverables required for TTA #3 are:

DELIVERABLES	DUE DATE
Option Period 1	
Technical report on modernization framework for candidate tools	6 months after award of option period 1
Tool improvements analysis report	6 months after award of option period 1
Develop Modernization framework	9 months after award of option period 1
Gap Analysis Report, Version 1	9 months after award of option period 1
Analysis report of Common Weakness Enumeration (CWE) coverage and mappings to NIST SP 800-53A, Version 1	9 months after award of option period 1

Candidate tool User’s Guide, Version 1	12 months after award of option period 1
Feasibility Study Report for transition into NIST’s SATE	12 months after award of option period 1
Delivery of candidate tools – iteration #1	12 months after award of option period 1
Scoring and Benchmarking Tool Version 1	12 months after award of option period 1
Option Period 2	
Technical report on modernization framework for candidate tools	3 months after award of option period 2
Tool improvements analysis report	6 months after award of option period 2
Gap Analysis Report, Version 2	9 months after award of option period 2
Analysis report of Common Weakness Enumeration (CWE) coverage and mappings to NIST SP 800-53A, Version 2	9 months after award of option period 2
Candidate tool User’s Guide, Version 2	12 months after award of option period 2
Delivery of candidate tools – iteration #2	12 months after award of option period 2
Scoring and Benchmarking Tool Version 1	12 months after award of option period 2

4.5 TTA #4 Key Deliverables

The key deliverables required for TTA #4 are:

DELIVERABLES	DUE DATE
Option Period 3	
Operational Pilot Demonstration Plan Version 1	2 months after award of option period 3
Capability Matrix of candidate tools	2 months after award of option period 3
Operational Pilot Demonstration Version 1	3 months after award of option period 3
Operational Pilot Demonstration Report Version 1	4 months after award of option period 3
Software Assurance labels that identify tool coverage	6 months after award of option period 3
Scoring and Benchmarking Tool Version 2	6 months after award of option period 3
Consumer report and buyer guide for list of candidate tools	6 months after award of option period 3
Analysis of Common Weakness Enumeration (CWE) coverage and mappings to NIST SP 800-53A, Version 3	8 months after award of option period 3
Operational Pilot Demonstration Plan V2	10 months after award of option period 3
Operational Pilot Demonstration V2	11 months after award of option period 3
Operational Pilot Demonstration Report V2	12 months after award of option period 3
Final Tool Study Report	12 months after award of option period 3
Pilot Design/SWAMP Integration Report	12 months after award of option period 3

5. Project Schedule/Milestones

STAMP will be accomplished in three phases, not to be confused with any base or options explicitly, where the TTAs and phases align as depicted in Figure 2.

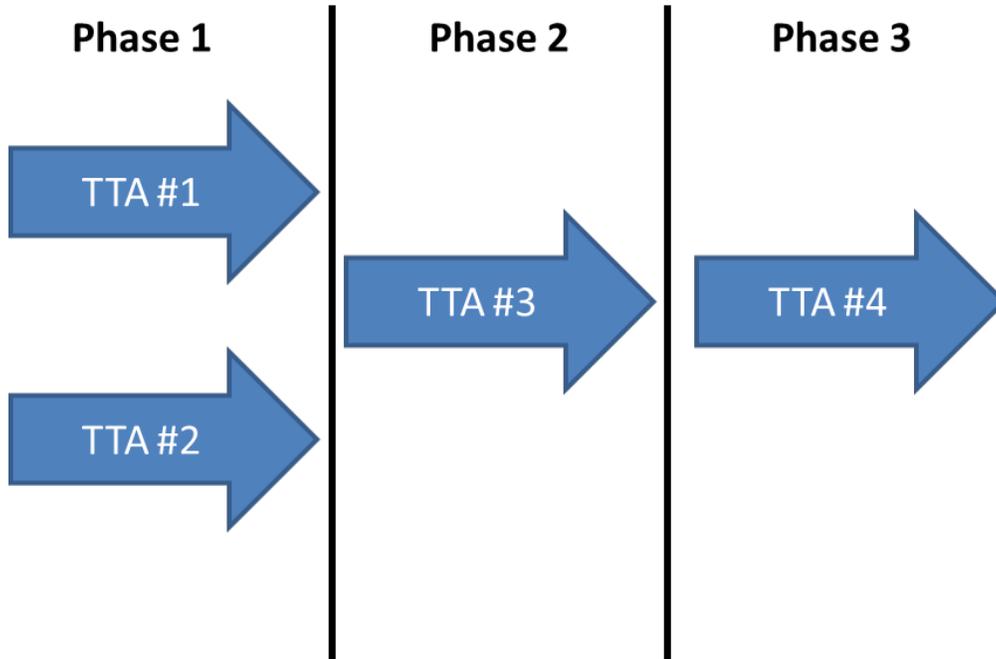


Figure 3 - STAMP Phases

A notional schedule and project funding profile is shown Figure 3, below:

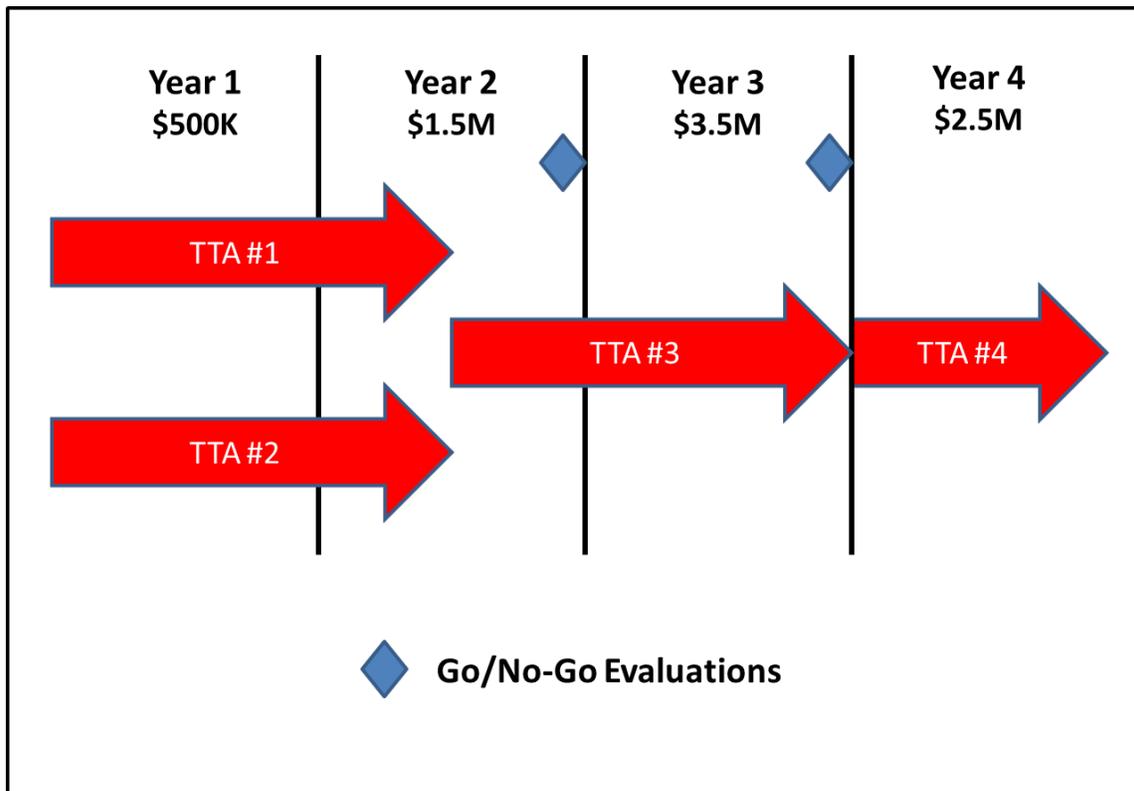


Figure 4 - STAMP Program Structure

6. Special Instructions/Notifications

6.1 Response Dates

Event	Time Due	Date Due
Industry Day	N/A	December 8, 2015
Proposals Due	4:30 PM EST	January <u>28</u> , 2016
Notification of Proposal Selections	N/A	June 1, 2016

6.2 General Instructions and Information

6.2.1 This BAA solicitation/call (HSHQDC-16-R-B0002) *does not include a requirement for white papers* and only requires the submission of proposals subject to the date identified in the “Response Dates” table above. However, given the variety of technologies and techniques that will be required to make STAMP a success, DHS expects strong collaboration and integration among teammates and may make up to two (2) selections.

6.2.2 Procedures for submission of proposals in the DHS S&T Portal are provided in paragraph 10 of DHS S&T CSD 5-Year BAA HSHQDC-15-R-B0005. Note that offerors must complete the company/organization portal registration PRIOR to submitting a proposal 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, or organization, registration information is located in paragraph 10.1 of DHS S&T CSD 5-Year BAA HSHQDC-15-R-B0005. In addition, each proposal requires registration in the portal. Information regarding white paper (not required for the STAMP solicitation) and proposal registration is located in paragraph 10.2 of DHS S&T CSD 5-Year BAA HSHQDC-15-R-B0005.

6.2.3 Offerors may provide multiple proposal submissions; however, each submission must be distinct and self-contained without any dependencies on other work of any kind, while providing an approach to meet all of the TTA objectives for every TTA. In addition, STAMP should include at least five open-source static analysis tools as candidates for modernization. The candidate tools should address in-depth tool coverage specifically in support for various programming languages and weakness classes (Seven Pernicious Kingdoms, OWASP Tool Benchmark⁸). Tool coverage for static and dynamic (scripting) programming languages should be included as part of STAMP, as dynamic programming languages are becoming more popular.

6.2.4 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 proposals as required for the Assertions Table (reference DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005 (current issue), Section 9.6.1.u). However, as an alternative to open source release, offerors may also offer a technical transition plan detailing a commercialization plan that explicitly identifies the consumer market(s) and market(s) adoption forecasts for the technologies developed.

6.2.5 As stated in DHS S&T CSD BAA HSHQDC-14-R-B0005 (current issue), 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/call.

6.2.6 The Evaluation Criteria in DHS S&T CSD 5-Year BAA HSHQDC-15-R-B0005 [3] 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-15-R-B0005 Section 1.3. Therefore, for 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-15-R-B0005 (current issue) Section 9.6.4 (for proposals).

6.5 Type Classification Ceilings

DHS S&T CSD 5-Year BAA HSHQDC-15-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 \$8,000,000.00 and are required to conform to the funding profile depicted in Figure 4 (STAMP Program Structure).

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

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

6.6 Travel

6.6.1 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.

6.6.2 In addition to the annual DHS PI Meeting, the STAMP Project will hold two meetings each year, one in the Washington, DC area and the other the contractor facility.

6.7 Proposal Requirements

To be considered for award, offerors **MUST** submit a proposal, compliant with the aforementioned response date, 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. This portal generated cover page is a different page than that identified in HSHQDC-14-R-B0005 Section 9.6.1(a).) The DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005 (current issue), 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:

6.7.1 Maximum Page Count.

6.7.1.1 Volume 1 – Technical Proposals.

6.7.1.1.1 For any proposal submitted in response to this solicitation/call, Volume 1, the technical proposal, ***SHALL NOT*** exceed fifty (50) pages. This maximum page count of 50 pages includes ***all*** information required to be included in Volume 1 of any submitted technical proposal. Information required to be included in Volume 1, Technical Proposal, is outlined in:

- Sections 9.6.1(a) through 9.6.1(v) of BAA HSHQDC-14-R-B0005 (current issue); ***and***
- Any additional proposal information required by Section 6.8 of this solicitation/call (HSHQDC-16-R-B0002).

6.7.1.1.2 Any Volume 1, Technical Proposal, received in response to this solicitation/call exceeding the maximum page count of 50 pages ***WILL NOT BE EVALUATED AND THEREFORE, WILL NOT BE ELIGIBLE FOR AWARD.***

6.7.1.2 Volume 2 - Cost Proposals. ***THERE IS NO PAGE COUNT LIMITATION FOR VOLUME 2, PRICE/COST PROPOSAL SUBMISSIONS.*** Information required to be included in any submitted Volume 2, Cost Proposal, is outlined in:

- Sections 9.6.2(a) through 9.6.2(c) of BAA HSHQDC-14-R-B0005 (current issue);

6.7.3 Subcontractor Cost Submission: Referencing, DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005 (current version), 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 DHS S&T 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.**

6.8 Special Submission Technical Requirements for Proposals

Given a goal of this BAA solicitation/call (HSHQDC-16-R-B0002) is to develop solutions that are mature enough for deployment or integration into an existing enterprise, the work proposed should be innovative and provide a capability not currently available in the market. Thus proposal submissions must specifically address the items below:

6.8.1 Define the Target Capabilities consisting of technical and operational capabilities that the developed solution will provide. The proposal should discuss a plan or outline on how the metrics and analytic techniques will evolve to accomplish this work. Also, integration with Integrated Development Environments (IDEs) should be addressed as a way to enable getting tools and capabilities closer to developers' desktops, which would help ensure that potential weaknesses and vulnerabilities can be detected early in the software development process. 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 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.

6.8.2 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 9.6.1.i, which outlines the requirements for “Testing and Evaluation” for proposal submissions.

6.8.3 Propose project-level Go/No Go demonstrations based on timing of the project deliverables, in 4.1, 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 (current issue):

- 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 to include proposal for Pilots in an operational setting; and
- Section 9.6.1.l, which outlines the requirements for “Transition Plan” for proposal submissions. Specific to this BAA solicitation/call, a transition strategy plan for each TTA is required that outlines how the technology will be transitioned to the broader user community. The transition strategy plan should include strategies for transitioning to the Software Assurance Marketplace (SWAMP), identification and targeted list of potential transition partners, commercialization plans and a detailed description as to how the transition strategy plan will be executed. Lastly, for optional period 3, the transition plan should address how the pilots could be used to support transition.

6.8.4 All software developed and delivered is required to be subject to security auditing; therefore, the offeror’s technical approach (reference DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005 (current issue), Section 9.6.1.g) 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)³.

6.9 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/STAMP-ASTAM_Industry_Day/listing.html

6.10 Contractual or Technical Inquiries

All contractual or technical inquiries to this BAA solicitation/call (HSHQDC-16-R-B0002) must be emailed to BAA-14-R-B0005@hq.dhs.gov no later than 4:30 PM ET on **January 8, 2016**. Emails submitting questions are to include “Questions for STAMP 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.

6.11 Order of Precedence

Additional Information: In the event that any of the terms and conditions contained in this BAA solicitation/call (HSHQDC-16-R-B0002) 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 this BAA solicitation/call (HSHQDC-16-R-B0002) shall take precedence.

Footnotes:

- 1) Juliet Test Suite - Software Assurance Reference Dataset,
<http://samate.nist.gov/SRD/testsuite.php>
- 2) The National Security Agency, Center for Assured Software (CAS), Tool Study report suggest that using more than one tool can improve the accuracy of results.
Website - http://samate.nist.gov/docs/CAS_2011_SA_Tool_Method.pdf
- 3) DHS Software Assurance Marketplace (SWAMP); <https://continuousassurance.org/>
- 4) SAMATE - Software Assurance Metrics And Tool Evaluation
http://samate.nist.gov/Main_Page.html
- 5) Most Popular Coding Languages 2015,
<http://blog.codeeval.com/codeevalblog/2015#.VijLbVKtQ7E=>
- 6) Qualitative & Quantitative Evaluation of Static Code Analysis Tools, December 2014, Indiana University - Purdue University Indianapolis, Dr. James H. Hill,
<https://www.signup4.net/Upload/TERA10A/20142362E/3-T1-4-Indiana%20University-Hill.pdf>
- 7) Technology Readiness Level
http://www.dhs.gov/xlibrary/assets/product_realization_chart.pdf
- 8) Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors.
<https://cwe.mitre.org/documents/sources/SevenPerniciousKingdoms.pdf>