Amendment
Published: December 21, 2015
Broad Agency Announcement Solicitation HSHQDC-16-R-B0003
Project: Application Security Threat Attack Modeling (ASTAM)

This amendment is identified in Federal Business Opportunities (FBO) as "Amendment 00016;" however, it is the first amendment to HSHQDC-16-R-B0003. The numbering for this amendment (Amendment 00016) is portrayed this way in FBO (rather than as the Amendment 00002 to HSHQDC-16-R-B0003) 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-B0003) 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 Software is ubiquitous; it powers our critical infrastructure, as well as our personal lives. The growing reliance on software makes us all vulnerable and susceptible to cyber-attacks. [1] With the increasing number of attacks aimed at targeting poorly developed software systems, there is a need to address security early and often throughout the software development process especially as risks are compounded by software size and complexity. Software programmers and developers tend to design, develop, and maintain software systems and applications with a focus on the customer needs, and often neglect to fundamentally understand ways in which software systems and applications can be exploited and compromised by potential attackers. Having the right software analysis tools and capabilities to detect weakness and vulnerabilities in software is critically important because software analysis tools and capabilities have not kept pace with the evolution in software and the platforms software runs on. Fundamentally, current software analysis tools have not performed well, and as a result these tools are not adopted early in the software development process. Additionally, existing software analysis and application security tools in the market are proprietary, closed systems that lack interoperability and are not designed to leverage context from other tools and technologies.

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 that could expose sensitive information. Understanding vulnerabilities and ways in which software systems can be attacked is an important capability that will help organizations be

more proactive in mitigating threats to their software systems. Providing software analysis and testing capabilities throughout the software development lifecycle will help organizations protect the confidentiality, integrity and availability of operational systems.

2. Project Description/Scope

2.1 The goal of the Application Security Threat and Attack Modeling (ASTAM) project is to create a Unified Threat Management (UTM) system that allows cyber security professionals to monitor and manage a wide variety of security-related applications and infrastructure components through a single management console. The UTM will be comprised of tools and an environment to analyze software systems and applications to identify potential risks, security threats, and exposures to the system environment, and then develop appropriate countermeasures to prevent, or mitigate the effects of threats to the system environment by bringing together independent assessment activities to build better situational awareness regarding potential threats. To meet project goals, the components of the UTM will need to model all of the information that affects the security (e.g., confidentiality, integrity, and availability) of software systems and applications to provide a view of threats in the environment from both a risk management and security perspective.

ASTAM should be designed and developed to provide coverage throughout the entire software development lifecycle (SDLC). The goal is to identify weaknesses in software before it leaves the developer's desk, helping to reduce the attack surface for software applications, as well as reduce the cost of software failures by finding weaknesses before they expose vulnerabilities. Each of the technology areas outlined in Figure-1 provides the context to provide security as software moves through the SDLC. Automating key aspects of the technology areas will close the gaps that exists in delaying security activities often neglected to keep the project on schedule.

ASTAM will leverage the context of each technology area to improve tool coverage to reduce false-positives, and provide greater analysis depth to find weaknesses that actually exists (false-negatives). Many state-of-the-art software quality assurance tools provides a single context which is prone to generate too many false-positives, and miss actual weaknesses that are present in software applications.

2.2 There are four component Technical Topic Areas (TTAs) of the UTM system. Figure 1, below, depicts a notional integrated UTM architecture, and while the primary goal of this BAA solicitation/call is to develop a system of systems that will operate in Integrated Development Environments (IDEs), and all proposals must address all TTAs, a secondary goal is for each TTA component to function independently as standalone technology and capability.

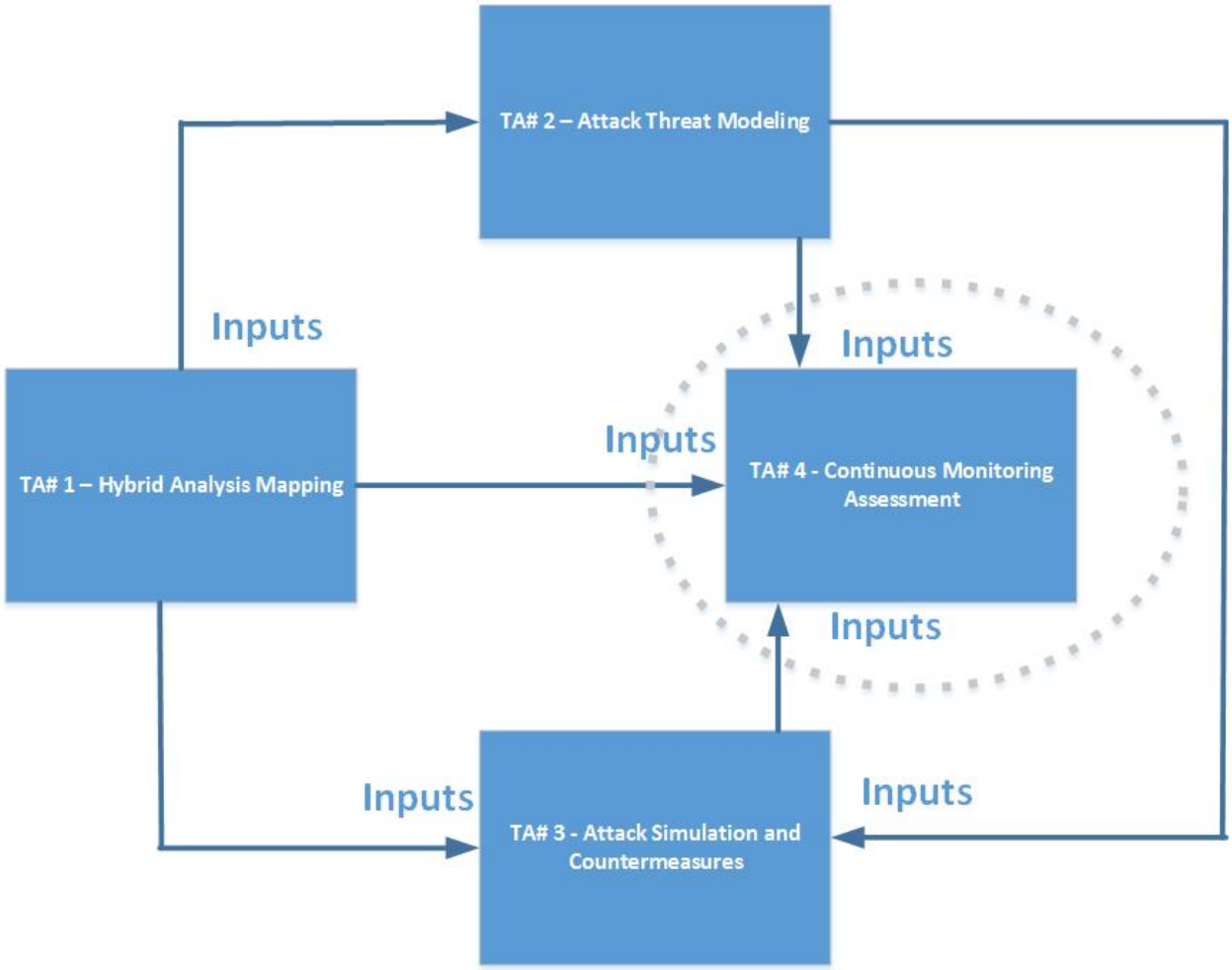

Figure 1: Integrated Unified Threat Management (UTM) System Architecture

3. Technical Topic Areas

The scope and descriptions of each UTM component TTA and their function are described below. Each TTA has applicability at a different phase of the software development and application operations lifecycle and while each TTA component is distinct, DHS seeks novel technical approaches to integrate all UTM technologies, that will leverage context of each TTAs to develop a more robust and comprehensive capability in software analysis and application security technologies that are not presently available commercially or to the Government. Of particular note, it is anticipated that both metrics and analysis techniques to measure the development progress will evolve during the project.

3.1 TTA #1 Hybrid Analysis Mapping (HAM) Component

Often static application security testing and dynamic application security testing are conducted independent of each other and at different times of the software development and deployment

lifecycle. Each application security testing technique has strengths and weaknesses; however, a hybrid approach should improve the analysis, pinpoint more exploitable weaknesses in software, reduce false-positives, and provide better situational awareness across cyber security assessment activities. Therefore, the desired product of this TTA is an integrated functional Hybrid Analysis Mapping (HAM) component that meets the following objectives and results in the key deliverables listed in Section 4.2. The objectives below may, at the discretion of a proposer, be sub-components of the HAM component, and as such the technical approach to integration is critical.

3.1.1 Objective 1 –Hybrid Analysis Engine. An objective of the HAM component is to provide a hybrid analysis capability that results from the integration of static application security testing tools (SAST) and dynamic application security testing tools (DAST). To support the UTM system, the hybrid analysis will need to be implemented through mapping SAST and DAST to an appropriate risk management framework and standards, where the risk management framework, tool coverage, and standards to be used are at the discretion of the proposer. The mappings should accurately identify weaknesses in software systems, and describe improvements to vulnerability detection, as well as describe how the approach will reduce false-positives and improve the ability to identify false-negatives, which would be implemented as a hybrid analysis engine. The development of the hybrid analysis engine is expected to be iterative and technical approaches should include a timeline for subsequent updates based on lessons learned from test and evaluation or deployment activities. Additionally, the hybrid analysis engine will serve as a mechanism for software developers to understand the breadth of analysis that the tools in their development environments provide and potentially assess the capability gaps in the coverage they need their tools to provide.

3.1.2 Objective 2 – Data Ingestion and Abstraction. To provide an interface to the hybrid analysis engine, an objective of the HAM component is to provide a data ingestion and abstraction component that provides a mechanism to bring in results from disparate SAST and DAST tools (e.g., proprietary, and open-source) into a format (industry acceptable) that is supported by the hybrid analysis engine.

3.1.3 Objective 3 – Source Code Monitoring. Continuous monitoring of source code while in development to determine impacts and potential changes in system architecture is a required capability for the HAM component. The source code monitoring capability needs to connect threats, exposures, attack scenarios and vulnerabilities during the development phase. Technical approaches should consider appropriate aspects of threat modeling and decompose the applications and systems for in-depth analysis.

3.1.4 Objective 4 – Penetration Testing Platform. An objective of the HAM component is to provide a user interface; to meet this objective and to leverage the other objectives of the HAM component, a penetration testing platform uses the hybrid analysis engine and the data ingestion and abstraction component to augment accepted penetration testing practices is required. A key feature of the penetration testing platform is the ability to provide a visualization of the code coverage (e.g., what parts of the code was reached by the penetration testing and HAM components), and to provide an analysis of the application attack surface. The penetration platform must also identify potential paths that can be used to attack the system.

3.2 TTA #2 Application Threat Modeling (ATM) Component

Many organizations have systems deployed in production and do not fully understand the extent to which the application or system can be attacked or exploited. "Threat modeling is best applied continuously throughout a software development project. The process is essentially the same at different levels of abstraction, although the information gets more and more granular throughout the lifecycle. Ideally, a high-level threat model should be defined in the concept or planning phase, and then refined throughout the lifecycle. As more details are added to the system, new attack vectors are created and exposed. The ongoing threat modeling process should examine, diagnose, and address these threats." [Open Web Application Security Project - OWASP] A threat modeling composition tool should be developed that provides visualization for software systems that identify potential attack vectors, system and software components and the fidelity of each, assessment of threats and risks, correlation of Common Vulnerabilities and Exposures (CVE) with Common Weakness Exposures (CWE), and architectural flaw analysis. A resulting capability is a Threat Modeling platform and analysis engine that will aid and inform the developer of risks, threats, and exposures. It should be noted that integration with Integrated Development Environments (IDEs) should be explored to get tools and capabilities closer to the developer's desktop, and help ensure that potential weaknesses and vulnerabilities can be detected early in the software development process. Therefore, the desired product of this TTA is an integrated Application Threat Modeling (ATM) assessment tool that meets the following objectives, integrates into the UTM system, and results in the key deliverables listed in Section 4.3. The objectives below may, at the discretion of a proposer, be sub-components of the ATM component, and as such the technical approach to integration is critical.

3.2.1 Objective 1 – Lifecycle Adaptive Threat Modeling. The capability to model application threats throughout the application development and operation lifecycle is an area of interest and therefore an objective for DHS' ASTAM project. For this objective, DHS is seeking to develop adaptation techniques that address methods for assessing ways in which applications can be attacked by decomposing an application is important for securing application systems. Identifying exposure points where sensitive data can be exfiltrated or leaked, entry points and attack vectors that can be used by attackers, and the interactions and data flows within the application environment are important factors for protecting against system compromise. In addition, developing decision making aids based on understanding the impact of the architectural decisions, the design principles used to develop source code toward protecting the confidentiality, integrity, and availability for applications and systems are important objectives for ATM.

3.2.2 Objective 2 – Identification of Vulnerabilities and Countermeasures. Functionality to automate application threat modeling to identify potential vulnerabilities, and define countermeasures to prevent and mitigate the effects of threats to the application or system is a requirement for the ATM component. Traditionally, application threat modeling has been regarded as a manual process; the focus of the desired research is to automate the application threat modelling process to provide full context and accurate representation of the system environment.

3.2.3 Objective 3 - Threat Profiler. A threat profiler that connects threats, exposures, attack scenarios and vulnerabilities is a required sub-component of ATM; specifically, an approach that determines what to protect and how to protect it against threats and attacks is a critical capability to DHS. Technical approaches should consider incorporating an application inventory component to track all aspects of the application or system environment and determine the overall security posture.

3.3 TTA #3: Attack Simulation and Countermeasures Modeling (ACSM) Component

Automating penetration testing and red teaming to mimic the capabilities, behavior, and activity of an attacker as part of a continuous monitoring process will provide a proactive approach to detect and identify vulnerable systems. Poorly developed software leads to vulnerabilities that could be exploited by an attacker. Having an on-demand capability to probe, test, and detect potential vulnerabilities is an important capability. Reports and studies suggest that the window of exposure for unpatched or vulnerable systems can range between 244 to 275 days, which essentially means that a given vulnerability was exposed, not patched or mitigated for at least 275 days [5]. This significantly increases the chances of system compromise. This TA intends to not only detect, but provide real-time remediation responses, capabilities, and countermeasure to help eliminate security exposures. Leveraging an understanding of attack patterns such as OWASP database of attack patterns and Common Attack Pattern Enumerations and Classification (CAPEC), Common Weaknesses Enumerations (CWE), Common Vulnerability Exposures (CVE), Software Fault Patterns (SFP), and penetration testing methodologies is critical. Thus, the desired product of this TA is an integrated Attack Simulation and Countermeasures Modeling (ASCM) component that factors in the preceding narrative and meets the following objectives and results in the key deliverables listed in Section 4.4.

3.3.1 Objective 1 –Penetration Testing Automation. A tool to automate penetration testing and red teaming for on-demand capabilities for organizations to test their security posture is required to be part of the ASCM tool. To meet this objective, technical approaches must present a methodology to address automating penetration testing and red teaming through all phases of the software development process.

3.3.2 Objective 2 – Attack Simulator. Related to the automation of penetration testing is a requirement for attack simulation capabilities. Therefore, an objective of the ASCM component is an attack simulator. Technical approaches to simulators must identify and pin-point weaknesses in software applications, and provide organizations with the capability to use these weakness to uncover critical vulnerabilities before an attacker can find them. As part of this development, an on-demand capability that can generate and initiate potential attacks should be included.

3.4 TTA #4: Continuous Monitoring and Assessment (CMA) Component

Continuous monitoring and testing of key technical security controls is essential for organizations to validate and verify that security controls are commensurate to risks and are needed to protect the confidentiality, integrity and availability of critical systems. Organizations must take a proactive approach to help detect changes in their security posture that may lead to weaker or inadequate security controls. This provides organizations ongoing awareness of information security, vulnerabilities, and threats to support organization risk management decisions. Far too often, continuous monitoring is focused just on the network and neglect to incorporate an application security or software assurance context to help improve overall situational awareness. This TTA will seek to address incorporating application security and software assurance context into the continuous monitoring process in a real-time, automated fashion. As such, the desired product of this TTA is an integrated Continuous Monitoring and Assessment (CMA) component prototype that meets the following objectives and results in the key deliverables listed in Section 4.5.

3.4.1 Objective 1 – Continuous Monitoring Dashboard. A dashboard platform that depicts a continuous monitoring of the threats, risks, weaknesses and vulnerabilities of application security and software assurance is required to be part of the CMA component. Technical approaches must address the development of a dashboard monitoring platform for an operational environment to visualize the reporting of CWEs, CVEs, and compliance frameworks to include incorporating real-time checks using NIST 800-53A controls, NIST 800-160, OWASP Top 10, and Defense Information Systems Agency (DISA) Application Security and Development Security Technical Implementation Guides (STIGs), as well as other applicable standards, guidelines, and policies that may be addressed at the discretion of an offeror.

3.4.2 Objective 2 – Compliance Framework Monitoring. The CMA requires functionality to monitor compliance with standards, policies, and guidelines; as well as best practices to measure security compliance in real-time. The Compliance Framework Monitoring (CFM) functionality is required to automate: NIST 800-53A assessment activities, NIST 800-160 for building secure systems (as well as other compliance frameworks), provide mappings to relevant security controls, Common Weakness Enumeration (CWE), and other industry regarded best practices (and frameworks). The ability to export CFM into FISMA reporting tools for metrics and reporting is also required.

3.4.3 Objective 3 – Real-time Countermeasure Response. As vulnerabilities are discovered for critical application systems, organizations need a way to protect these assets until code can be reengineered to mitigate the weaknesses that exposed vulnerabilities. For operational systems, it becomes difficult to take mission critical systems offline, or interrupt the availability of these systems. Providing a real-time response to known vulnerabilities affords organizations an effective countermeasure which is required to be part of the CMA component. Approaches to satisfy this objective should consider existing network and application security control already in place, such as network firewalls, web application firewalls, and proxy (reverse) technologies. In addition, technical approaches should include developing custom signatures profiles for real-time protection and enforcement.

3.4.4 Objective 4 – Integration with Other ASTAM Objectives. To develop an integrated ASTAM capability, the products of this TA should: integrate with Continuous Diagnostic and Mitigation (CDM) dashboards; provide continuous assurance services throughout the system development lifecycle (SDLC); and provide knowledge learning and remediation guidance for secure coding practices.

3.5 TTA #5: Unified Threat Management (UTM) Integration

The integration of the individual ASTAM components into a UTM tool is a primary objective of this BAA call. DHS is seeking innovative solutions to integrate the UTM components. While key deliverables are listed in Section 4.6, offerors may propose other deliverables and delivery times based on their integration approach.

3.6 TTA #6: UTM Pilots

DHS is seeking to support transition of the UTM into use in operational environments. Therefore, proposals are required to include two pilot evaluations to occur in option period 3, where the pilots should relate to transition approach. Key deliverables for UTM pilots are listed in Section 4.7, and in option 3 there are deliverables for each TTA that correspond to updated documentation for the UTM components, and UTM prototypes required for the pilots.

4. Project Structure

The ASTAM 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 the UTM system and for each TTA are described below and should be planned for in conjunction with the Statement of Work severability requirements HSHQDC-14-R-B0005, paragraph 9.6 h (are required for each severable year of performance).

4.1 Project Status Deliverables

The project status 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	4, 8 and 11 months after award and exercise of each option thereafter

4.2 TTA #1 Key Deliverables

The key deliverables required for TTA #1 are:

DELIVERABLE	DUE DATE
Base Period	
Hybrid Analysis Design Document V1	60 days after award
Target Capabilities Definition Document	60 days after award
Hybrid Analysis Working Prototype V1	6 months after award
Hybrid Analysis Design Document V2	6 months after award
Hybrid Analysis Go/No-Go Demonstration Plan	9 months after award
Hybrid Analysis Working Prototype V2	10 months after award
Hybrid Analysis Go/No-Go Demonstration	10 months after award
Hybrid Analysis Go/No-Go Demonstration Report	11 months after award
Hybrid Analysis Design Document V3	12 months after award
Option Period 1	
Hybrid Analysis Working Prototype V3	6 months after award of option period 1
Hybrid Analysis Go/No-Go Demonstration Plan	9 months after award of option period 1
Hybrid Analysis Working Prototype V4	10 months after award of option period 1
Hybrid Analysis Go/No-Go Demonstration	10 months after award of option period 1
Hybrid Analysis Go/No-Go Demonstration Report	11 months after award of option period 1
Hybrid Analysis Framework Release V1	12 months after award of option period 1
Technical Report/Feasibility Study for SWAMP Integration	12 months after award of option period 1
Hybrid Analysis Design Document V4	12 months after award of option period 1
Option Period 2	
Hybrid Analysis Installation Guide V1	3 months after award of option period 2
Hybrid Analysis Working Prototype V5	6 months after award of option period 2
Hybrid Analysis User's Guide V1	6 months after award of option period 2
Hybrid Analysis Go/No-Go Demonstration Plan	9 months after award of option period 2
Hybrid Analysis Working Prototype V6	10 months after award of option period 2
Hybrid Analysis Go/No-Go Demonstration	10 months after award of option period 2
Hybrid Analysis Go/No-Go Demonstration Report	11 months after award of option period 2
Hybrid Analysis Design/SWAMP Integration Report	12 months after award of option period 2
Hybrid Analysis Design Document V5	12 months after award of option period 2
Option Period 3	

Hybrid Analysis Installation Guide V2	3 months after award of option period 3
Hybrid Analysis User's Guide V2	3 months after award of option period 3
Hybrid Analysis Installation Guide V3	11 months after award of option period 3
Hybrid Analysis User's Guide V3	11 months after award of option period 3

4.3 TTA #2 Key Deliverables

The key deliverables required for TTA #2 are:

DELIVERABLES	DUE DATE
Base Period	
ATM Design Document V1	60 days after award
Target Capabilities Definition Document	60 days after award
ATM Working Prototype V1	6 months after award
ATM Design Document V2	6 months after award
Go/No-Go Demonstration Plan	9 months after award
ATM Working Prototype V2	10 months after award
Go/No-Go Demonstration	10 months after award
Go/No-Go Demonstration Report	11 months after award
ATM Design Document V3	12 months after award
Option Period 1	
ATM Working Prototype V3	6 months after award of option period 1
ATM Go/No-Go Demonstration Plan	9 months after award of option period 1
ATM Working Prototype V4	10 months after award of option period 1
ATM Go/No-Go Demonstration	10 months after award of option period 1
ATM Go/No-Go Demonstration Report	11 months after award of option period 1
Technical Report/Feasibility Study for SWAMP Integration	12 months after award of option period 1
ATM Design Document V4	12 months after award of option period 1
Option Period 2	
ATM Installation Guide V1	3 months after award of option period 2
ATM Working Prototype V5	6 months after award of option period 2
ATM User's Guide V1	6 months after award of option period 2
Go/No-Go Demonstration Plan	9 months after award of option period 2
ATM Working Prototype V6	10 months after award of option period 2
Go/No-Go Demonstration	10 months after award of option period 2
Go/No-Go Demonstration Report	11 months after award of option period 2
ATM Design Document V5	12 months after award of option period 2
Option Period 3	
ATM Installation Guide V2	3 months after award of option period 3
ATM User's Guide V2	3 months after award of option period 3
ATM Installation Guide V3	11 months after award of option period 3
ATM User's Guide V3	11 months after award of option period 3

4.4 TTA #3 Key Deliverables

The key deliverables required for TTA #3 are:

DELIVERABLES	DUE DATE
Base Period	
ASCM Design Document V1	60 days after award
Target Capabilities Definition Document	60 days after award
ASCM Working Prototype V1	6 months after award
ASCM Design Document V2	6 months after award
ASCM Go/No-Go Demonstration Plan	9 months after award
ASCM Working Prototype V2	10 months after award
ASCM Go/No-Go Demonstration	10 months after award
ASCM Go/No-Go Demonstration Report	11 months after award
ASCM Design Document V3	12 months after award
Option Period 1	
ASCM Working Prototype V3	6 months after award of option period 1
ASCM Go/No-Go Demonstration Plan	9 months after award of option period 1
ASCM Working Prototype V4	10 months after award of option period 1
ASCM Go/No-Go Demonstration	10 months after award of option period 1
ASCM Go/No-Go Demonstration Report	11 months after award of option period 1
ASCM Framework Release V1	12 months after award of option period 1
Technical Report/Feasibility Study for SWAMP Integration	12 months after award of option period 1
ASCM Design Document V4	12 months after award of option period 1
Option Period 2	
ASCM Installation Guide V1	3 months after award of option period 2
ASCM Working Prototype V5	6 months after award of option period 2
ASCM User's Guide V1	6 months after award of option period 2
Go/No-Go Demonstration Plan	9 months after award of option period 2
ASCM Working Prototype V6	10 months after award of option period 2
Go/No-Go Demonstration	10 months after award of option period 2
Go/No-Go Demonstration Report	11 months after award of option period 2
ASCM Design/SWAMP Integration Report	12 months after award of option period 2
Option Period 3	
ASCM Installation Guide V2	3 months after award of option period 3
ASCM User's Guide V2	3 months after award of option period 3
ASCM Installation Guide V3	11 months after award of option period 3
ASCM User's Guide V3	11 months after award of option period 3

4.5 TTA #4 Key Deliverables

The key deliverables required for TTA #4 are:

DELIVERABLES	DUE DATE
Base Period	
CMA Design Document V1	60 days after award
Target Capabilities Definition Document	60 days after award
CMA Working Prototype V1	6 months after award
CMA Design Document V2	6 months after award
CMA Go/No-Go Demonstration Plan	9 months after award
CMA Working Prototype V2	10 months after award
CMA Go/No-Go Demonstration	10 months after award
CMA Go/No-Go Demonstration Report	10 months after award
CMA Design Document V3	12 months after award
Option Period 1	
CMA Working Prototype V3	6 months after award of option period 1
CMA Go/No-Go Demonstration Plan	9 months after award of option period 1
CMA Working Prototype V4	10 months after award of option period 1
CMA Go/No-Go Demonstration	10 months after award of option period 1
CMA Go/No-Go Demonstration Report	11 months after award of option period 1
Technical Report/Feasibility Study for SWAMP Integration	12 months after award of option period 1
CMA Design Document V4	12 months after award of option 1
Option Period 2	
CMA Installation Guide V1	3 months after award of option period 2
CMA Working Prototype V5	6 months after award of option period 2
CMA User's Guide V1	6 months after award of option period 2
CMA Go/No-Go Demonstration Plan	9 months after award of option period 2
CMA Working Prototype V6	10 months after award of option period 2
CMA Go/No-Go Demonstration	10 months after award of option period 2
CMA Go/No-Go Demonstration Report	11 months after award of option period 2
CMA SWAMP Integration Report	12 months after award of option period 2
CMA Design Document V5	12 months after award of option 2
Option Period 3	
CMA Installation Guide V2	3 months after award of option period 3
CMA User's Guide V2	3 months after award of option period 3
CMA Installation Guide V3	11 months after award of option period 3
CMA User's Guide V3	11 months after award of option period 3

4.6 TTA#5 Key Integration Deliverables

The key deliverables required for TTA #5 are:

DELIVERABLE	DUE DATE
Base and Option Periods	
UTM Integration Plan	45 days after award of base period and each option thereafter

Option Period 2	
UTM Installation Guide V1	12 months after award of option period 2
UTM User's Guide V1	12 months after award of option period 2
UTM Working Prototype V1	12 months after award of option period 2
UTM Design Document V1	12 months after award of option period 2
Option Period 3	
UTM Installation Guide V2	3 months after award of option period 3
UTM User's Guide V2	3 months after award of option period 3
UTM Working Prototype V2	3 months after award of option period 3
UTM Installation Guide V3	10 months after award of option period 3
UTM User's Guide V3	10 months after award of option period 3
UTM Working Prototype V3	10 months after award of option period 3
UTM Design Document V2	12 months after award of option period 3

4.7 TTA #6 UTM Pilot Key Deliverables

The key deliverables required for TTA #6 are:

DELIVERABLE	DUE DATE
Option Period 3	
UTM Operational Pilot Demonstration Plan V1	2 months after award of option period 3
UTM Operational Pilot Demonstration V1	3 months after award of option period 3
UTM Operational Pilot Demonstration Report V1	4 months after award of option period 3
UTM Operational Pilot Demonstration Plan V2	10 months after award of option period 3
UTM Operational Pilot Demonstration V2	11 months after award of option period 3
UTM Operational Pilot Demonstration Report V2	12 months after award of option period 3

5. Project Schedule/Milestones

A notional schedule and project funding profile is shown Figure 2, below.

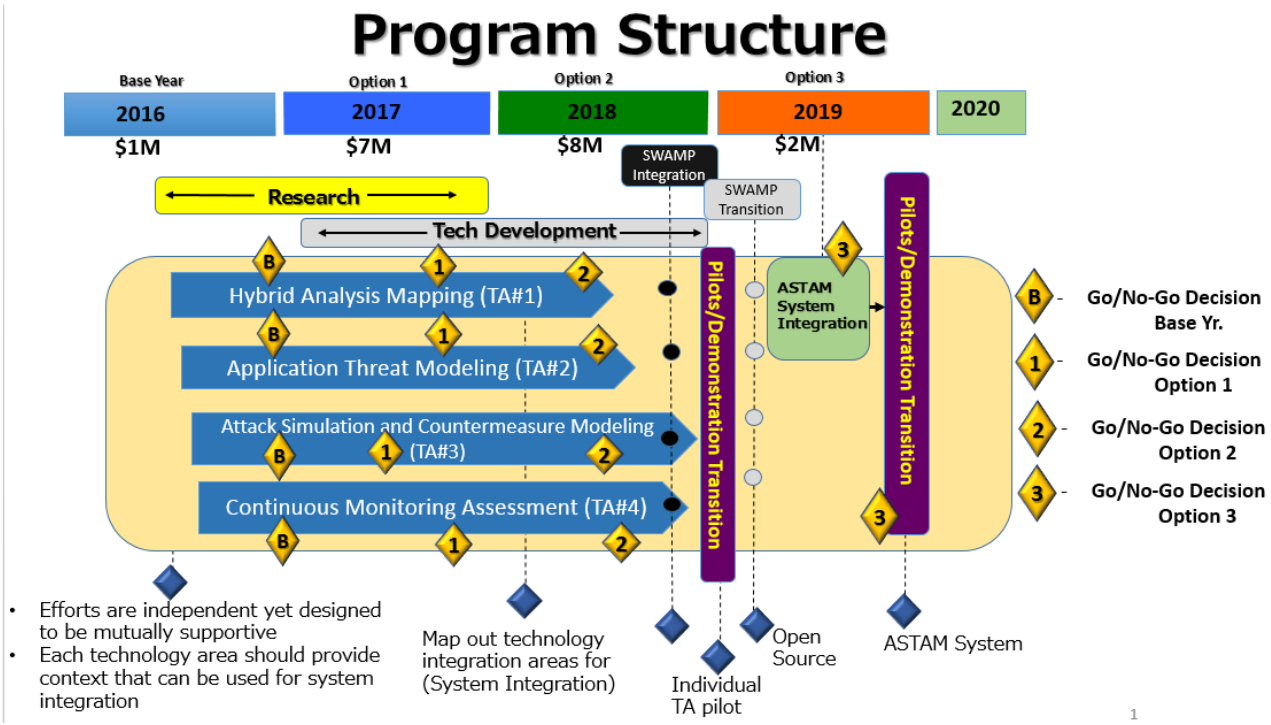

Figure 2: ASTAM Program Structure

6. Special Instructions/Notifications

6.1 Response Dates

Event	Time Due	Date
Industry Day	N/A	December 8, 2015
Proposals Due	4:30 PM ET	February 18, 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-B0003) ***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. Again, given the variety of technologies and techniques that will be required to make ASTAM a success, DHS expects strong collaboration and integration among teammates.

6.2.2 The intent of this BAA solicitation/call (HSHQDC-16-R-B0003) is to make one award that may include multiple participants or subcontracts to develop a system of systems that results in an integrated system where each of the TTA products can function independently, but also be integrated to create a Unified Threat Management (UTM) system.

6.2.3 Procedures for submission of proposals in the DHS S&T BAA Portal are provided in paragraph 10 of DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005 (current issue). 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 proposals. Company/ organization registration information is located in paragraph 10.1 of DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005 (current issue). In addition, information regarding proposal registration is located in paragraph 10.2 of DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005 (current issue).

6.2.4 Offerors may provide multiple proposal submissions; however, each submission must address all of the TTAs identified in this solicitation/call. In addition, 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.

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 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) (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 technical transition plan detailing a commercialization plan that explicitly identifies the consumer market(s) and market(s) adoption forecasts for the technologies developed.

6.2.6 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.

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

6.3 Foreign Participation

Offerors are reminded that foreign participation may occur as defined in DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005 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-14-R-B0005 (current issue), 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 $18,000,000.00 and are required to conform to the funding profile depicted in Figure 2 (ASTAM 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/call 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/call will be rejected as non-compliant.

6.6 Travel

6.6.1 For purposes of estimating costs, offerors should anticipate travel to 3 project meetings per year.

6.6.2 DHS Cyber Security Division holds an annual Principal Investigator (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 ASTAM Project will hold two program review meetings each year, one for one full day 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-B0003).

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). In addition, proposals are required to conform to the funding profile depicted in Figure 2 (ASTAM Program Structure).

6.7.2 As stated above, the information outlined in Section 6.8 below must also be included in any submitted proposal.

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-B0003) 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 for each TTA 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. 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 a Go/No Go demonstration, for each TTA (excluding TTA #5 and TTA #6), based on timing of the TTA key deliverables, 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 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) [4].

6.8.5 Detailed integration and pilot approach for Option Period 3. Given that there are many approaches that could be implemented toward meeting the goals of this BAA Call, the approach to integration of the UTM components will be a key differentiator for proposals and will be the primary basis for selection determination. 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;

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-B0003) must be emailed to BAA-14-R-B0005@hq.dhs.gov no later than 4:30 PM ET on January 29, 2016. Emails submitting questions are to include "Questions for ASTAM 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-B0003) 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-B0003) shall take precedence.

Footnotes:

1) The Software Assurance Marketplace: A response to a challenging problem; Kevin E. Green, 2014. Website http://www.net-security.org/article.php?id=2146

2) Hybrid Analysis Mapping (HAM). Small Business Innovative Research (SBIR) - https://www.sbir.gov/sbirsearch/detail/402675

3) DHS Software Assurance Marketplace (SWAMP); https://continuousassurance.org/

4) 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

5) Whitehat Security - https://www.whitehatsec.com/assets/WPstatsReport_052013.pdf