2015 DHS S&T Cyber Security Division

BAA Industry Day

Application Security Threat Attack Modeling (ASTAM)

**Voice of America Building
Wilbur J. Cohen Auditorium
300 Independence Avenue, SW
Washington, DC 20531**

December 8, 2015 12:30pm-2:00pm EDT

Question and Answer Discussion – Cyber Security Division and Office of Procurement Operations

1. DHS funding of SWAMP is supposed to end in 2017. However, the ASTAM BAA says that the penetration platform, attack simulator and countermeasure response are supposed to be integrated into SWAMP in 2018. What type of resources and infrastructure (DETER, will exist at SWAMP to support the ASTAM integration after DHS is no longer funding it?

   Response: For the purpose of proposing to the ASTAM BAA you should consider SWAMP in place as presently available.

2. What is the relationship between TTA#4 and a) the DHS Continuous Diagnostics and Mitigation (CDM) Initiative and b) DHS National Information Exchange Model (NIEM) Initiative?

   Response: ASTAM is envisioned to be able to provide information that could be leveraged by CDM when operational. NIEM has nothing to do with ASTAM.

3. It seems like there is a lot of overlap/commonality between STAMP and ASTAM. How would you summarize the differences?

   Response: STAMP is focused on static analysis tools, but per ASTAM call paragraph 3.4.4, "ASTAM should be designed and developed to provide coverage throughout the entire software development lifecycle (SDLC)…"

4. TTA4 seems to take in all results from other components. How is TTA4 different from TTA5?

   Response: TTA4 is a component of the UTM. TTA5 will integrate all UTM components.

5. Can a company/organization participate in more than one proposal?

   Response: Yes.

6. Are existing fundees encouraged to use their tools in a collaboration for ASTAM?

Response: Any offeror that can meet the requirements of the ASTAM BAA is encouraged to propose.

7. Would DHS find it acceptable to have a small business prime a project of ASTAM's size?

Response: Yes - See HSHQDC-14-R-B0005, 5 "ELIGIBILITY INFORMATION"

8. Can we use a joint venture to propose?

Response: Yes - See HSHQDC-14-R-B0005, 5 "ELIGIBILITY INFORMATION"

9. Referring to Figure 1 and the slide showing ASTAM TTA Interactions: Can you foresee other directionalities of the relationships between TTAs beyond those depicted by the arrows on the diagram. For example, could TTA2 feed into TTA1?

Response: Per 2.2, Figure 1 is notional. So, an offeror could propose an alternate UTM architecture.

10. Who is the intended user of ASTAM?

Response: From 2.1 of the ASTAM call, the intended users of the UTM to be developed for ASTAM are "cyber security professionals to monitor and manage a wide variety of security-related applications and infrastructure components through a single management console."

Part 2: What roles and user types would you expect to participate in a pilot for ASTAM?

Response: 3.6 in the ASTAM call states" DHS is seeking to support transition of the UTM into use in operational environments." Proposals should address the roles needed to use their proposed UTM in an operational environment.

11. Referring to TTA 4, Objective 4 "…products of this TTA should integrate with Continuous Diagnostic and Mitigation (CDM) dashboards." Does this requirement refer to the Continuous Monitoring dashboard in Objective 1? Or do we have to integrate with the larger DHS CDM program awarded in 2013?

Response: Referring to 3.4.4, the objective is "Integration with Other ASTAM Objectives" so the reference is specific to ASTAM and not any other "larger DHS CDM program…"

12. RE: Section 6.6 Travel, specifically 6.6.1, is it acceptable to cost travel for multiple representatives to travel to project meetings? For example, the technical leads of each of the 4 initial TTAs would benefit from attending project meetings.

Response: Yes, it is up to you to propose how much travel you believe is necessary to execute the project. Note: costs should be proposed based on travel origin and destinations and number of travelers.

13. Are the two pilot evaluations supposed to be for the entire ASTAM system or could there be a pilot of fewer than the 4 main TTAS? Note on p. 14 the diagram notes an "Individual TA pilot"

Response: ASTAM call paragraph 3.6 has been updated to clarify that pilots are for the UTM system and individual UTM component end item evaluation.

14. Section 2.1 says you want a view of threats from both a risk management and security perspective. Can you provide an example of how these perspectives are distinct and unique?

Response: See footnote 5.

15. In Section 6.8.2 of ASTAM, it indicates a need for both technical and operational metrics, how do you distinguish between technical and operational metrics? Can you give examples of each?

Response: ASTAM call paragraph 6.8.2 refers to "Target Capabilities" technical metrics refer to design targets and operational metrics refer to an operational UTM design specification for both the integrated UTM system and UTM component end items.

16. Referring to "Application Security Threat and Attack Modeling (ASTAM), Software Assurance Industry Day" dated December 8, 2015, slide 13 shows $1M in FY16. It seems that FY16 will be over by contract award. Will the schedule slip to the right year-by-year?

Response: ASTAM BAA call Figure 2 has been amended to clarify the funding profile for awards as well as the timing for required deliverables.

17. For ASTAM pilots, what is the minimum size organization that is acceptable as a pilot? Can funds be used to reimburse pilot organization for using their people?

Response: 2.2 has been amended to indicate "the primary goal of this BAA solicitation/call is to develop a system of systems that will operate in and support security operation centers and software development environments …"

Do we care if it is in government or industry?

Response: 3.6 has been revised to indicate pilots can be either with industry or government where the functionality and capabilities can be fully demonstrated in an operational environment, such as a security operations center.

Can funds be used to reimburse pilot organizations for using their people?

Response: It is conceivable that a proposal could propose tasking and teaming that would reimburse an organization participating in a pilot.

18. There is a big gap between the first year and second year funding. What are the expectations for 1st year deliverables? How much detail on year 2 and year 3 is needed in the proposal?

Response: The ASTAM BAA has been amended to clarify the funding profile for awards as well as the timing for required deliverables.

19. What are the TRL (Technology Readiness Level) goals at each of the technologies of the go/no-go demonstration points?

Response: The ASTAM is not calling for technologies to be assed for TRL.

20. Can part or all of the ASTAM solution use cloud services or does the entire technical solution have to be on premises?

Response: The introductory paragraph in section 3 of the ASTAM BAA call has been revised to indicate ASTAM is intended to be an on premise solution.

21. Re: Paragraph 6.8.4 – "the offeror's technical approach …must identify how security auditing will occur." What is DHS's expectation: A) Each team member does its own security auditing using a process described in the proposal; B) The prime selects and pays for an independent security auditor who can periodically conduct security audits of the entire project; or C) DHS provides an independent auditor who uses established security audit processes on the program.

Response: The requirement in 6.8.4 is for developed software to go through security auditing before release. Offerors are required to address how this security auditing would be conducted.

22. Re: Paragraph 6.2.5 – "DHS has a strong preference for open source licensing of software for all software developed and delivered …" –

a. Is the intent of the open source licensing is to ensure that there are no required licensing costs associated with the ASTAM solution and that other researchers or vendors can easily expand the system's capabilities because the source code is available?

Response: Yes

b. Is it acceptable to DHS to have free versions of software (that have not been open-sourced) used in the Go No-Go demonstrations and in the delivered ASTAM system? For example, there are application security tools that are free but not open source which could be useful to incorporate into both the demonstrations and delivered system.

Response: The technical approach to meet the goals and requirements of the ASTAM BAA are at the discretion of the proposer, but the requirements in BAA HSHQDC-14-R-B0005 paragraph 9.6.1 u (Assertion of Data Rights), and 9.6.1 g (2) are required. These BAA requirements are particularly important should an offeror propose any deliverable that the Government would not receive unlimited rights to.

23. We cannot find a way to initiate a proposal under https://baa2.st.dhs.gov/portal/BAA/ for ASTAM. It does not show any open calls under the Solicitation.

Is the above portal the correct one for submitting proposals for ASTAM?

Response: The DHS S&T BAA portal has been reconfigured to facilitate proposal registration and submission for ASTAM.

24. Can the pilots of the individual TTA components and of the ASTAM fully integrated system use inputs from commercial tools, but not have the commercial tools be part of the open source software delivery to DHS?

Response: It is conceivable that a proposal could have a technical approach that had inputs from commercial tools, but the requirements in BAA HSHQDC-14-R-B0005 paragraph 9.6.1 u (Assertion of Data Rights), and 9.6.1 g (2) are required. These BAA requirements are particularly important should an offeror propose any deliverable that the Government would not receive unlimited rights to.

25. Re: TTA #4 Objective 1: Does DHS prefer a solution that hooks into an existing continuous monitoring system (which would not be open sourced) or do you prefer that a new continuous monitoring dashboard for which open source would then be available?

Response: 3.4 of the ASTAM BAA has been updated to include: "one of the motivations of ASTAM is to bring application security context to the continuous monitoring process. Many continuous monitoring systems focus solely on the network and host, developing a capability that integrates application security context is somewhat of a new approach. The expectation is to leverage existing continuous monitoring systems provided they are interoperable and extensible. "

26. Re: TTA #4 Objective 1: Does the continuous monitoring dashboard need to include network level risks? If so, at what level of detail?

Response: Referring to 3.4.1, the dashboard is scoped to "application security and software assurance."

27. Section 3.5 says that the "UTM tool is a primary objective of this BAA call" and Section 6.8.5 says that "the approach to integration of the UTM components will be a key differentiator for proposals." This leads us to be believe that the UTM must be addressed fairly early in the program. However, the Design Document doesn't appear as a deliverable until the end of 2018 and TTA#5 UTM doesn't appear anywhere on Figure 2 showing the Program Structure. The work to perform the UTM is only implied as relevant in 2019 in the green block labeled "ASTAM

System Integration” in Figure 2. Can the proposer choose to start work on the UTM in the first year of the program? If not, when does DHS want significant headway to be made on TTA#5?

Response: Section 3 indicates “DHS seeks novel technical approaches to integrate all UTM technologies.” It is an offeror decision as to how to propose an approach to the work.

28. Regarding : 5-Year BAA page 18 Paragraph g, item (1) – The Five Year BAA says that the Technical Approach must “Outline and address technical challenges inherent in the approach and possible solutions for overcoming potential problems” and then two sentences later it says that the approach must “Discuss mitigation of technical risk”. These two sentences seem to mean the same thing to us. Does DHS see a difference between “identifying technical challenges and possible solutions” vs “identifying technical risks and mitigators”? If so, can you explain that difference?

    Response: HSHQDC-14-R-B0005, section 9.6.1 g (1) is written as DHS intended. Mitigation choices could be a subset of possible solutions.

29. On page 9 Section 4.2 there is a requirement for a Hybrid Analysis Framework Release in Option Period 1 and on page 11 Section 4.4 there is a requirement for an ASCM Framework Release in Option Period 1. None of the other TTAs require a Framework Release. What is a Framework Release? Why do only two of the TTAs require this?

    Response: Framework has a common definition that a proposal will have to address for TTA#1 and TTA#3. The deliverables in the ASTAM BAA call were chosen by DHS to support ASTAM goals.

30. At the Industry Day Dr. Doug Maughan said that the Deliverables as described on pages 9-13 of the ASTAM BAA Solicitation would change substantially based on expected changes to the schedule and to the number of pilots. When will DHS publish a revised list of Deliverables?

    Response: Section 4 of the ASTAM BAA call been updated via amendment.

31. The ASTAM BAA Solicitation says on page 8 Section 3.6 **“**… proposals are required to include two pilot evaluations to occur in option period 3, where the pilots should relate to transition approach.” However, at Industry Day Dr. Maughan said that there would be five required pilots: 4 individual TTA pilots at the end of 2018 and 1 pilot of the full ASTAM system in 2019. Which is correct? If neither, can you please explain how many pilots you require, of what, and when. Based on Figure-3, there will be 4 individual pilots for each TTA, and one UTM pilot for TTA5.

    Response: The description of the pilots in ASTAM paragraph 3.6 have been updated via amendment.

32. Section 4.1 of the ASTAM BAA says that there will be three Program Reviews in Months 4, 8 and 11 after award. Section 6.6.3 says that there will be two Program Reviews each year. In addition to the annual PI meeting identified as a requirement in Section 6.6.2, how many Program

Reviews will there be each year and in which months? For scheduling purposes, in what month should we assume the annual PI meeting will occur?

Response: The program reviews in section 4 are correctly described. Also, the month annual DHS S&T CSD Principal Investigator Meeting is not known from year to year.

33. At ASTAM Industry Day, Dr. Maughan said that the schedule for ASTAM was going to change from 4 years to 3 years. He said that the Base Year and Option Year 1 would be combined into a single year. Can you confirm that the new schedule for ASTAM is going to be comprised of a Base Year of 12 months with a Go/No-Go demo at the end of the Base Year, followed by an Option 1 Year (12 months) that ends in individual TTA1, 2, 3 and 4 pilots for a total of 4 individual pilots, followed by Option Year 2 that ends in a pilot of a fully integrated ASTAM System?

    Response: The schedule depicted in Figure 2 of the ASTAM BAA call has been updated via amendment.