

2014 DHS S&T Cyber Security Division

BAA Industry Day

Mobile Technology Security

June 24, 2014 1:30pm-4:00pm EDT

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

1. Of the 13 international partners, which three are not participating in this BAA?

Response from Doug: Mexico, France, and Spain, are the three, so far, of the 13 who are not participating with us. I will say, however, we do not have firm commitments yet from Germany and New Zealand for the four topics, but they have committed to do joint work with us. So, eight of the ten have committed to participate specific to these four topics.

2. Risk management is mentioned a lot in TTA 1 and TTA 4, should TTA 1 also follow the same framework as TTA 4, i.e. the NIST publications?

Response from Luke: I think this really depends on the approach you're taking. For TTA 1 there might be a more localized decision based upon that. This is really left up to the proposer for TTA 1 for whether or not the framework is applicable. If you're applying to TTA 1, please take a look at TTA 4, it calls out NIST Special Publication 800-37.

3. What certification and/or accreditation activities are needed to support deployment of mobile technology systems for usage across DHS or government in general?

Response from Vincent: I can't speak for necessarily Government in general. But specifically to DHS because our office does create the requirements that you would have to follow, we do have DHS Policy 4300A that is applicable in full. When you talk about mobile technology, the solution set, whatever that may be, if you look at on premise, it is information systems, so *FIPS Publication 199 Standards for Security Categorization of Federal Information and Information Systems* applies for system categorization. After the system is categorized, you to follow NIST 800-53, Rev 4 to get the control set that you'd have to apply to, you would traditionally have to do that for any federal information system (FISMA system), in order to get an ATO ("Authority To Operate") for our department. If you were looking for off premise, this is different, so if you're looking at Mobile Device Management (MDM) or whatever in the cloud, you're looking at a FedRAMP provisional ATO, and then additional requirements that would be tacked on by DHS Policy 4300A or different documentation we may have.

4. Please explain "Authenticating across logic boundaries within device" in TTA 1

Luke's response: The thought on this is authenticating across applications, they're usually sandboxed from each other, how do you handle that? And also, another logical boundary is between device authentication and OS authentication and looking at those logical boundaries.

5. NSS efforts were excluded from use case development. Should we assume 2 different types of devices will be used; one for classified and one for unclassified?

Response from Doug: In our case, we are only looking at the unclassified devices. That was why the classified devices were excluded from the use case development. Our concern is purely for the unclassified devices.

6. Overview/needs were rather generic. What are the unique mobility constraints of DHS's target audience that drive the need for new secure solutions?

Response from Luke: See the "DHS Mobile Use Case Development" slides presented by Vincent Sritapan, Technical Lead and Component Coordinator, DHS CISO Office, Security Architecture and Engineering Division posted to <https://www.fbo.gov/spg/DHS/OCPO/DHS-OCPO/HSQDC-14-R-B0005/listing.html>.

7. Much of the emphasis has been on securing the enterprise from untrustworthy mobile devices and users. Is there interest in protecting the mobile user from untrustworthy remote services?

Response from Luke: Yes. TTA 2 looks into this space. If you look back at the threat model that we went through from the security baseline and some of the other Digital Government Strategy documents, Man in the Middle, other type attacks, and again, traditionally just the direction of the government with FedRAMP and the use of services. It is definitely important to protect the mobile user.

8. Will you make the Digital Government Strategy results public?

Response from Luke: Yes. All of the results are available on CIO.gov. See <https://cio.gov/innovate/digital-strategy/>

9. Do you expect foreign government participation across all 3 proposal types? How was foreign government participation money distributed among past awards? How is Intellectual Property handled for foreign government participation?

Response from Doug: In Luke's case, we're only dealing with 2 proposal types instead of three, but we do anticipate Foreign Government participation across both of those types. In the past, how was Foreign Government participation distributed among the past awards? Interestingly enough, in BAA 11-02 the majority of the Foreign Government participation were in Type 1 and Type 2 awards, only 1 type 3 award that had Foreign Government participation. How is Intellectual Property handled for Foreign Government participation? The way intellectual property is handled is that the Foreign Government partner gets the same IP rights that the US government gets. So if we get unlimited rights, we are able to transfer unlimited rights to our international partners. If we get government purpose rights, we can transfer those government purpose rights to the international partner as well. So whatever IP restrictions that might be requested by you, we will transfer those accordingly to the Foreign Government.

10. Would a technology for securely offloading tasks from mobile devices to less than 100% trusted “clouds” be in scope for this BAA? If so, what TTA?

Response from Luke: This seems the best fit for TTA 2, it’s not as directly responsive, but it fits into that space.

11. Do you accept external and hardware solutions?

Response from Luke: Yes, but the tricky part on this is the commercialization and use case. No one wants to add on lots of bulk or expensive additional hardware you have to upgrade every time you get a new phone. So how do you make it practical is the real challenge for external devices, but if you have a great way than please include it.

12. For secure comms, are proposed solutions expected to use Commercial Solutions for Classified (CSfC), or Type 1 crypto?

Response from Doug: As mentioned earlier, we’re not, necessarily looking at commercial solutions for classified for type 1 crypto, so the answer is no in this case we’re not looking for a classified solution.

13. Are there opportunities for funding for hardware oriented research (new architectures, secure memories, etc.)?

Response from Luke: This is a good fit for TTA 4. One of the things we’re evaluating against is commercialization approach; it’s very tough to commercialize hardware in this space. If you have a good solution in there, that either through partnerships or a very interesting angle that makes it practical, then please include it.

14. Can you explain how the Center of Excellence funding model works?

Response from Doug: The Center of Excellence (COE) is a completely separate program at DHS S&T, it’s run by our office of University Programs, there are nine Centers of Excellence. However, the COE funding models are not relevant to this BAA because selected awards will be made directly to the offerors.

15. DHS is interested in leveraging commercial mobile devices. Are proposed solutions that require re-imaging the device in scope? Do you have a target funding budget for the transition task option?

Response from Luke: Yes, that is definitely in scope, as long as the device can be re-flashed. Commercial devices are available that can be boot loaded. If we’re talking about commercial devices that you have to use very extensive means to be able to put your own stuff on it, like extreme jail breaking, that might be on the bounds of commercialization and not very practical, but it is within scope. There isn’t target funding specifically allotted for the transition side, we’re very serious about transition, so put a practical budget in that space and include that as part of the proposal, but see Broad Agency Announcement Solicitation HSHQDC-14-R-B0015, Section 6.9.8 for instructions.

16. Could you describe (again) what should be addressed in a white paper that is responsive to more than one TTA?

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

17. Is there a requirement to use SWAMP? And or DETER?

Response from Doug: SWAMP is encouraged. If you look at section 6.2.4 of the call, would you read that section, Luke?

Response from Luke: This goes back to the fact that we all write software, but not all of it is great. From section 6.2.4 of the call, “All software developed and delivered is required to be subject to security auditing; therefore, the offeror’s technical approach must identify how security auditing will occur. Also, DHS expects offerors to follow best practices on software design and encourages the use of the DHS Software Assurance Marketplace.”

Response from Doug: As far as DETER, the answer is no. DETER is not particularly well suited in its current form for doing mobile testing, so there’s not an expectation of using DETER.

18. If one vendor has multiple sensor modalities for TTA 1, should it submit one or more white papers? Should TTA 1 focus on developing biometric technology or the risk management?

Response from Luke: It’s left to your discretion, but ideally those would be encompassed in a single proposal, unless the modality is so drastically different and severable that it would make sense for two. Should TTA 1 focus on developing biometric technology or risk management? Ideally it’s a combination of both, so it’s not purely a sensor approach, and it’s not purely risk management, how do you get more knowledge from that sensor without context. It’s a coupling of the two.

19. How do you define COTS?

Response from Doug: Our interpretation of this question is, for us, COTS is defined as Commercial Off the Shelf System or Technologies. For whoever asked that question, please let us know if there’s a deeper meaning to your question.

Response from Audience Member: Is it defined as something that literally has to come off the shelf and be used, or is it something that comes off the shelf and be tinkered with and integrated, or is it something that you buy from an integrator, there’s a huge range of what that could mean to you.

Response from Luke: As an antonym to that, it's technology that isn't owned and solely operated by the government.

Audience Member: So you're willing to buy something from a government integrator, even if it's only used by the government, as long as you're buying it from somebody it's ok.

Luke: So that's why we stick to very simple definitions. It's a gray area, I'll be the first to admit that. One thing we tried to highlight in the front text is having a broader market place, and government being a part of that broader market place, as opposed to being the only customer. When you get in a space like mobile it's very tough for the government alone to sustain that market place and actually have it advance.

20. Human subject research:

DHS has adopted the U.S. Department of Health and Human Services (HHS) policies and procedures set forth in Title 45 Code of Federal Regulations (CFR) Part 46, Subparts A-D. Subpart A of 45 CFR Part 46 is HHS's codification of the Federal Policy for the Protection of Human Subjects (also known as The Common Rule) which sets forth the United States Government's basic foundation for the protection of human subjects in most research conducted or funded by the U.S. Government. Any contracts awarded that include/involve human subjects will include terms and conditions that require human subject research be conducted in accordance with The Common Rule and DHS Directive Number 026-04.

21. How many BlackBerrys are in DHS? How long until they are replaced by Android/iOS phones and how important is it to develop mobile security solutions for BlackBerry?

The solicitation does not specify particular platforms that have to be used and instead allows for the targeted platforms to be specified in a proposal. The solutions proposed should be transitionable. Given that this is an R&D activity, approaches do not have to relate directly to the devices that a government agency is currently using. The work completed through this program may even help agencies move to a new platform.