

**2014 DHS S&T Cyber Security Division
BAA Industry Day
Cyber Physical Systems Security
June 26, 2014
Mayflower Renaissance Hotel
1127 Connecticut Avenue, Northwest
Washington, DC**

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

1. Can we submit multiple proposals?

Yes; per section 6.2.3 of BAA call HSHQDC-14-R-B0016. We are doing the BAA different from BAA 11-02 in that you are allowed to still submit a proposal even if you are “not encouraged” from the white paper. In BAA 11-02 you had to be “encouraged” in order to submit a proposal.

2. Would cloud data centers be considered part of Cyber Physical Systems?

Generally, no. What we are looking for is the combination of cyber and physical systems.

3. Can other government agencies (DOD for example) participate in this BAA?

In section 5.1 of overarching BAA HSHQDC-14-R-B0005, it outlines who can respond. It also specifically includes government laboratories, so depending on the individual who submits. If you are a government lab you may participate, if you’re a government agency and more of an operational person we would love to talk you about possibly being a partner or a transition partner.

4. The BAA says manufacturing and industry is not included as a priority driver. Should one even propose them?

Per section 2.4 of the BAA call HSHQDC-14-R-B0016, we did identify priorities but we are open to any of the areas.

- 5. If we concentrate on the Cyber Physical Systems infrastructure that interfaces 2 critical infrastructures (electric grid and transportation for example) does it matter which critical infrastructure you call as your key focus area?**

No, it does not matter. You just need to select one.

- 6. When and where will the slides be made available?**

The slides will be made available off of the FedBizOps webpage <https://www.fbo.gov/spg/DHS/OCPO/DHS-OCPO/HSQDC-14-R-B0005/listing.html> , which is the official location. We will also have them posted on our DHS/S&T BAA web portal.

- 7. Common protocols across many control devices and networks – research that cuts across many key drivers. Do we need to still focus on one of transportation (ex: transportation, energy, etc.)?**

Yes, we do want you to identify a key driver. It is also helpful if you identify how it interfaces with the others.

- 8. How should international partners be put in the proposal? (direct funding, matching, other foreign governments, etc.)**

You are not responsible for finding international partners. The international partners for DHS are government agencies that are our counterparts (DHS equivalent) in those countries. They will review proposals and make decisions on what they would like to co-fund. Feel free to include international researchers as part of your team, however they are not required.

- 9. Are we strongly encouraged to obtain letters of support or participation from industry?**

What are the requirements in terms of industry support/letters in the white paper vs proposal?

There is not a requirement for letters. We do encourage a transition to practice strategy and we want to see results deployed and we're leaving it to you as a potential performer to demonstrate that.

- 10. By building controls, do you mean smart buildings? If so, what kind of technical readiness level are you looking to fund in terms of overall technology?**

Yes, we are referring to smart buildings. As previously mentioned we are looking for transitional work at the conclusion of the project.

11. Is it encouraged to team with universities or national labs?

No, not more than anyone else. Your responsibility is to find the best team. We do not make any distinction, all sources foreign and domestic can respond.

12. Is there any preference over chip, devices, or system level proposals?

We do not have a preference. Please look at the call as written; we do not have a preference as to how your proposal comes in and what parts of the system it addresses, that is entirely up to you.

13. What are examples of first responder systems that face Cyber Physical Systems issues?

Police, Fire, etc., rely on the same technologies that we do. One great example is first responder vehicles.

14. What licensing models outside of open source will DHS entertain?

Is there a licensing model that will not work?

While we are big supporters of open source we realize that your job as a researcher is to create intellectual property and you certainly want to exploit that intellectual property. You have an opportunity when submitting your white paper and proposal to tell us what the existing intellectual property is, and what you're bringing to the table. Depending upon that intellectual property we will decide based on what you're proposing how we can use and exploit your intellectual property in some way from the government side. Everything does not have to be open source. What you will find and what was done on BAA 11-02 gives you the intellectual Property owner the opportunity to commercialize your technology. At the same time we will try to take maximum intellectual property rights that the government can take to ensure that if you don't successfully commercialize your technology we still have as many rights as possible, so we can try to commercialize on our end. We are not aware of a licensing model that will not work, however keep in mind the idea is to transition. We want you to be successful in commercializing, at the same time we try to get as many rights as we can whether that's unlimited for government purpose so that we can ensure transition in the event that you don't.

15. Do you welcome proposals to extend the DETER facility for any of the other Cyber Physical Systems areas (cars, medical devices, etc.)?

We are looking for results that provide the impact of transition. We want to see demonstrations on how these results are going to transition.

16. What is the perspective of DHS on the Internet of Things, and how does it fit in to the Cyber Physical Systems program?

The Internet of Things tends to focus on the consumer side, however for the purpose of this BAA they would overlap.

17. Would you be able to clarify the annual budget for Cyber Physical Systems Security?

DHS has gone to a different model of funding. We are internally doing new start programs and the program is funded for the total of the program rather than a specific annual budget. For example, the Cyber Physical Systems program is funded for \$16 million dollars. If you reference the pyramid from the slides, you will see that of that \$16 million, some amount over \$10 million will be used to fund efforts from this BAA.

18. Since a lot of smart technology is available outside. What is the strategy to enforce the security in design space?

There are many of these commercial available technologies that are from different domains. Do you think it is a good idea to leverage some of them?

Leveraging technologies is always strongly encouraged. In terms of design space I think that comes back to the general theme of the program, which is to try to build security in to the design. We hope to have this as an outcome of the program.

19. Evaluating Cyber Physical Systems often require the use of proprietary systems. This could make the cross vendor collaborations hard. Is it acceptable to have a single industry partner in a particular driver?

Yes, and we do understand the issue of proprietary systems that exist. That is something that you need to make us aware of in your write up, as to which proprietary systems may be included. It is certainly acceptable to have a single industry partner as part of your team.

20. How important is it to partner with companies in this BAA?

There is not a specific partnering or letter requirement. Our goal is to transition research to where it is useable and in practice. We want something other than research that will simply sit on the shelf and is never used. How you accomplish that is strictly up to you. There is an evaluation criterion that says how the results are going to be used.

21. Why separate Experiments and Pilots in to a separate TTA? It seems like TTAs 1 and 2 incorporate Experiments and Pilots.

If you look at TTA 1, which is about security models and interactions, and if you look at TTA 2, it's about system design and implementation. The reason why we have TTA 3, which is just about experiments and pilots, is because you may have existing technologies that do not fit in to TTA 1 and TTA 2, but you are interested in having an experiment or pilot with that technology. You can in fact propose an experiment or pilot with some of your existing technology and it doesn't have to fit into the other 2 TTAs.

22. In TTA 3 can you have more than a 12 month plan?

Yes. It comes back to you having to explain what your technology is and how you think it can be piloted, what key driver, would it be piloted, and what you think that pilot looks like. We will entertain as part of TTA 3 those pilots that wouldn't necessarily fit into TTA 1 or TTA 2.

23. What is the budget limit for Transition to Practice?

You are responsible for identifying the cost in each TTA. If you look at Type III which includes Testing, Evaluation, and Transition we say it's \$750k which is the budget limit for a single Type III proposal. If you have Type II, it's up to \$2 million dollars and that includes the whole spectrum from development to transition. The pilot is not limited to \$750k necessarily on the Type II. You have to explain what the development is and what's the test and evaluation under a \$2 million dollar cap. The same applies to Type I.

24. TTA 3: Is the focus on a particular technology to be evaluated, piloted, or on evaluation infrastructure?

Can we propose building a testbed open to performers from other TTA's, or do we need to have our own pilot?

Similar to the question asking if we could extend DETER. What we are looking for is a way to show the impact and for you to distinguish yourselves from existing programs and other infrastructures that may already be available.

25. Vehicle ad-hoc networks such as DSRC, Wave, 802.11p, are emerging commercial automotive standards. How can DHS affect these standards (adopt, steer, etc.)?

As part of the solicitation and the Cyber Physical Systems program by funding this type of research and development we will influence those standards that are in the middle of

the development phase. Many of which were not developed with security as a forethought or even an afterthought. That is our goal as part of the Cyber Physical Systems program not just within DHS but the whole intergovernmental Cyber Physical Systems initiative. This is illustrative of the timeliness of the work. These are standards that are currently emerging and we do believe that this is the critical opportunity where it is very different influencing an emerging standard then patching an existing standard.

26. Given the number of potential attack scenarios, vulnerability data bases, and possible platform configurations. How applicable is research to prune these combinations with the ability to persistently learn and prioritize to focus vulnerability analysis?

It is a difficult space and there are numerous attack scenarios and lots of data and vulnerability information out there, and depending on which of the key drivers you pick you have multiple platform configurations. As much as you can narrow down that combination of options and describe and discuss it within one of the key driver areas that will be considered an acceptable path forward.

27. Can you give an example in which human decision making is a critical component of Cyber Physical Security? Ex: where might a human factor in to one of these systems? To enhance, protect, restore, or address security?

This question underscores the importance of focusing on a key driver. Human decision making in smart cars may be quite different from human decision in making in smart grids. In this case of a smart car, the car's driver is clearly in the loop and is still the primary decision maker. In the case of a smart grid, a combination of technicians, operators, and perhaps even users can play a role in decision making. Proposals should focus on a single key driver and that should help more clearly define the role of human decision making.

28. DOE issued guidance to utilities on contract language and requirements that should flow down to suppliers. Much of that guidance is aimed at fit-for-purpose. Is that your objective as well?

This question again underscores the importance of focusing on a key driver. Utilities are one important area and it is important to security requirements to flow down to suppliers. In this sense, the objectives are similar. Other types of cyber physical system may have similar challenges. The overall objective is to build security into the design of these critical systems. The precise approach to building in security will vary depending on the cyber physical system and the proposed approach.

29. 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.