

**2014 DHS S&T Cyber Security Division**

**BAA Industry Day**

**Data Privacy Technologies Research and Development**

**June 24, 2014 0900-1140 EDT**

**Mayflower Renaissance Hotel  
1127 Connecticut Avenue, Northwest  
Washington, DC**

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

**1. Will the presentation slides be provided?**

Yes; they will be posted on both the FedBizOps web site <https://www.fbo.gov/spg/DHS/OCPO/DHS-OCPO/HSHQDC-14-R-B0005/listing.html> as well as the BAA2 DHS S&T portal.

**2. With shared situational awareness underpinning the U.S. government cybersecurity focus areas, what role does the Cyber Security Division envision for visual analytics across the 4 open BAA topic areas?**

We anticipate that of the 4 topics, the only one that may have a visual analytics focus is the DDoS topic, TTA #1. This topic is looking at Best Current Practice (BCP 38) and measurement of DDoS defenses. This is more of a topic for the DDoSD presentation on Thursday.

**3. For the federated search, is the focus on determining whether a query violates some policy or on ensuring that only what is specified in a legal query is revealed?**

The use of the phrase “legal query” is not clear. However, with the question rephrased to ask: for the federated search, is the focus on determining whether a query violates some policy or on ensuring that only what is specified in a query is revealed? The answer is both. Federated searches must ensure:

1. That the query must be coming from a trusted and authorized source.
2. That only pertinent information is revealed to the trusted and authorized source.

- 4. Will the DHS S&T/Cyber Security Division consider funding an effort that extends the capabilities of current commercial products under this BAA, where that product has been developed by the proposer?**

Yes, as part of the BAA we do look at additional capabilities on existing products and capabilities. As part of the submission, offerers will be required to identify the intellectual property associated with the technology you are providing.

- 5. Under BAA 11-02, the number of industry awards to submittals was a much smaller percentage than that of academia and laboratories. Will that trend continue under this BAA?**

It depends. DHS does not make awards based on who is submitting them but rather on which proposals provide the best technical solution.

- 6. Regarding Technical Topic Area #1: Homeland Security Enterprise Privacy Policy Compliance Tools, Section 3.1.2 strongly implies that the proposal MUST address Section 3.1.1.1 (Automatic E-Mail Encryption) and/or Section 3.1.1.2 (OMB Data Extract Rule Compliance). Is Section 3.1.2 really that restrictive?**

Yes.

- 7. Does DHS plan to make a few big awards, or several medium-sized awards under this BAA?**

It depends on the quality of submissions received.

- 8. Can you provide a canonical example or use case for the privacy-preserving federated search sharing scenario?**

**Is there any scale and performance requirement for the federated search capability?**

This depends on the use case and the customer. It could range from a small partnership in a collaborative environment sharing across 5 domains but it could also be state, local, public and private sector, which would be a much larger scale. We provide R&D tools for multiple customer sets ranging from DHS components (such as the Federal Emergency Management Agency, The Bureau of Customs and Border Protection, or the Bureau of Immigration and Customs Enforcement) but we also provide them to state, local, public, and private sector.

- 9. While the focus of the Cyber Security Division is on the development and transition of new technologies, the human analyst is a critical component of whether or not those technologies are effective. In general, how much of a focus will the BAA calls have on analyzing and understanding the human element?**

You will have to examine each call differently. BAA 11-02 was first time CSD considered the human elements, such as usability, insider threat, and economics, some of the non- standard Computer Science Topics. Some aspects will affect privacy and mobile space, less so with DDoS

and Cyber physical, even though it is not specifically called out in this BAA. CSD continues to look at the human aspect of cyber security.

**10. For a project on “mobile data privacy protection,” should the proposal be submitted to “data privacy,” or “mobile device security?” Could such a project be co-funded?**

If there is an angle of privacy related to it, it should be submitted to data privacy topic. The mobile device call is not addressing the privacy aspects. We want to ensure that anything dealing with privacy is kept in the same topic. Another proposal could be submitted separately for mobile device security if it meets requirements.

**11. Under technical Topic Area #2, Page 4 of the BAA solicitation says, in part, “federated searches across multiple data sources residing in multiple domains...” What is a reasonable number of domains to consider? Could it be two, five, ten, fifty, or maybe even 100?**

**Are the domains presumed to be connected via high-speed lines, offering tens of megabits per second? If not, what bandwidth can be assumed?**

Based on the varying customer requirements and needs, the range could be anything from 5-100, but generally, 5-10 is more reasonable within the Federal government. 20 domains would be on the high end. DHS has also been working with private sector organizations such as the electrical companies that are working with up to hundreds of companies across the nation, such as gas stations, to see what resources are available during an emergency event. Much of the information may contain privacy and intellectual property information. As it relates to second question on connectivity, there could be start-up companies or large government agencies involved.

**12. Do transition partners have to be submitted in white papers?**

**Does DHS help identify potential transition partners?**

If a transition partner is known, it should be submitted with the white paper. Note that transition and commercialization is one of the criteria that need to be addressed in both the white papers and proposals. Per section 6.9.6 in the call, DHS will only help identify a Federal government transition partner after award if the awardee has not identified one.

**13. Is there any interest in on-line training or interaction redesign?**

**Is gamification or scenario training of any interest?**

DHS is not looking at training or the user interface design or for that matter any kind of training or gamification. As noted in opening remarks, CSD does fund some education and training, but they aren't part of this call, or as a part of any of the four calls published to date.

- 14. Is there any interest in applying visual analytics solutions to the current text-based “privacy policy reasoning engine” as part of this BAA?**

**What is the Cyber Security Division’s current approach to privacy controls associated with other publicly available information, such as Twitter™?**

For the first question, if you believe that it would enhance a particular mission, then submit. For the second question on Twitter, we haven’t received a requirements on this, so not aware of any need or customer for this.

- 15. Regarding IRB approvals, please elaborate on which stage of the application process (such as the white paper, full proposal, or contract negotiation) IRB approval or documentation is required?**

**Update to Industry Day comment:**

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. **Note: human subject research and IRB is not part of the selection criteria.**

- 16. Other agencies use the NICE cyber workforce descriptions for their labor categories. Why doesn’t the NSA leverage the NICE work in its own standard labor categories?**

Each agency has been given the option to decide whether or not to use these workforce descriptions. It has not been mandated as policy by OMB.

- 17. Indemnification when contractors use open-source tools seems unusual, especially given the pro open-source tone of the BAA. Could you explain the rationale for this provision?**

An amendment to BAA HSHQDC-14-R-B0005 has been issued to remove this language.

- 18. If someone has a framework, or knowledge products rather than a technology to offer, can they submit a white paper and proposal about them?**

Submissions based on frameworks or knowledge products are okay. If you have multiple tools to offer, submit a separate paper for each tool. Multiple white paper submissions are okay. If you have one tool with capabilities that fall across more than one technical topic area, just submit one white paper.