2014 DHS S&T Cyber Security Division
BAA Industry Day
Distributed Denial of Service Defense
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. **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. **What is the total available funding for DDoSD?**

   The model within DHS/S&T has slightly changed and we are more focused on programs that have a beginning and an end. The program dollars available specifically on the DDoS program for the BAA is over $14 million dollars. We cannot provide an exact amount due to variances in the budget.

3. **Can you elaborate on how you expect network DDoS solutions to demonstrate 1 tbps attack handling?**

   To clarify, we are not expecting anyone to have a 1 tbps DDoS attack. You will not be required to show a 1 tbps attack, unless there is one that we can capture. We want to provide a lot of flexibility there. It may be possible to simulate and show how the simulation extrapolates up, as well as with emulation and analysis. Hopefully with the combination of simulation, emulation, and analysis you can demonstrate the effectiveness of your technology. Beyond that we cannot get more specific without discussing specific technologies.

4. **Are we permitted to create new DDoS attacks and publish them?**

   Not with DHS funding.

5. **With respect to the Best Practice TTA 1, would BCP38 extensions to IPV6 be in scope?**

   What about Best Practices around amplification of DDoS attacks?

   The answer to both questions is yes. The basic premise behind BCP38 is that the traffic leaving your network belongs to your network in to your stub, or is appropriate traffic to transfer through your network if you're transit. That's independent as to whether it is IPV4 or IPV6. The specs are relatively good in the sense that they are not too protocol dependent. Extending it to other Best Practices is certainly valid; we've focused on BCP38 as a great canonical example. You do not need to be strictly limited to that, there is a lot of good advice on operational mailing lists like NANOG to other venues that identify a number of Best Practices. BCP38 is clearly one we want to address; however expanding is welcome as well.

6. **Is the international partner's potential co-funding above and beyond the BAA 5 year budget of $95 million?**

   No. We essentially take in international funding, turn it in to US dollars and put it on contracts. It then becomes part of the $95 million dollar ceiling. Again, we do not have definitive numbers on the international funding; we just know that they have expressed interest. Please reference BAA 11-02 where they provided over $6 million dollars in funding. We anticipate similar ranges associated with these four topics.

7. **For TTA 2, to what extent are you interested in technical solutions versus organizational people solutions to communicate and collaborate in DDoS attacks?**

   It is difficult to separate the technical and organizational people solutions in DDoS attacks, therefore it is a combination of both and both are needed to deploy. When you talk to an institution attempting to respond to an attack, it's not simply a question of the technology. The technology is a key piece, but it's the technology that works with the policies and people.

8. **To what extent, if at all, is funding for these programs dependent upon the FY15 budget/appropriations law being passed by congress?**

   Of course all of our activities within DHS are dependent upon congress in some degree or another. However, we do not anticipate any issues.

9. **For TTA 2, is the collaboration you refer to in paragraph 3.2.1.3 across multiple organizations or within the organization under attack?**

   It would be across multiple organizations. If you are responding to a 1 tbps DDoS attack, then you will require assistance outside of your organization.

10. Can you elaborate on 1 tbps attacks? Most backbones are not capable of carrying this bandwidth of traffic.

That is absolutely true. To clarify, at this time a 1 tbps attack has not been seen. However, there is a trend here. As of 5 years ago a 10 gbps attack was a big deal, now it's considered minimal. Although a particular ISP may have trouble carrying that volume of traffic that doesn't mean that someone couldn't try to pump that volume of traffic into the ISP. If we generate enough traffic from enough edges we can get to those points and attempt to set a high bar. There is an upward trend that we are trying to get ahead of instead of falling behind.

11. Can you explain more clearly how the transition part of the proposal would work?

I will point you to sections 8.7.C.6 and 9.6.L of BAA HSHQDC-14-R-B0005. The idea is as mentioned, whether you are doing a Type I, II, or III you are going to have a Testing and Evaluation transition part of both a white paper and a proposal. The idea albeit more vague in the white paper than in the proposal is to identify what you believe the transition and commercialization options are for the technology that you are proposing. For example, a Type I proposal can be made for up to $3 million dollars, and those test and evaluation activities have to part of the $3 million dollar proposal. The transition plan described in the proposal supports the ability of DHS to understand the potential impact of the technology proposed, but only transition activities in the statement of work would be funded.

12. Can you discuss how visual analytics have been used in support of DDoS?

What has worked well? What has not?

There are commercial products that provide visualization and visual analytics on volume of traffic and anomalous traffic and spikes in anomalous traffic, however we cannot endorse or dissuade the use of any particular vendor products. There are certainly products that visualize traffic and are used in DDoS mitigation or situational awareness; however I would point you back to our objectives in this solicitation.

13. What role do you envision for visual analytics across Technical Topic Areas 1-3?

Visual analytics is most useful in the assessing BCP38 standards deployment. You can look at some of the work that has been done with DNS Security and how DNSSEC has been analyzed and viewed. It seems tangential for the other topics; however it is your technology proposal so that is your determination. Visualization would be a valid consideration for BCP38 deployment TTA 1 and seems tangential for TTA 2 and TTA 3.

14. How will the DDoS defense technology be used with the Department of Defense?

For example, the US Army Cyber Command is working the same problem, how will we take advantage of cross area synergies to get more bang for the buck?

We do have interactions with Cyber Command and are aware of some of the work that they are funding primarily in operational environments not in R&D environments. In fact, we are meeting with some individuals from Cyber Command the week after next. As we have done and hopefully conveyed to you, we have a fairly well connected program both to some of our operational people as well as the research community; and my expectation is that we would do the same with the DDoSD program by making sure that the technologies we are funding have opportunities to leverage other government funded research, as well as potentially transition some of those customers.

15. 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.