Amendment
Published: February 4, 2015
Broad Agency Announcement Solicitation HSHQDC-14-R-B0017
Project: Distributed Denial of Service Defense (DDoSD)

This amendment is identified in Federal Business Opportunities (FBO) as "Amendment 00008;" however, it is the third amendment to HSHQDC-14-R-B0017. The numbering for this amendment (Amendment 00008) is portrayed this way in FBO (rather than as the Amendment 00003 to HSHQDC-14-R-B0017) because this solicitation is posted in FBO as "Solicitation 1, CSD BAA DDoSD" on the same FBO page as the overarching 5-yr CSD BAA, HSHQDC-14-R-B0005. Therefore, FBO identifies this as the next amendment in the sequence of all amendments issued to HSHQDC-14-R-B0005 or any solicitations/calls posted on the same page under the overarching CSD 5-yr BAA.

Changes to this solicitation are identified in red with change marks in the left hand margin.

1. Introduction

1.1 This BAA solicitation (HSHQDC-14-R-B0017, as amended) is a call issued against Department of Homeland Security (DHS), Science & Technology (S&T), Cyber Security Division (CSD), 5-Year Broad Agency Announcement (BAA), HSHQDC-14-R-B0005, Amendment 00003. All terms and conditions of the DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003, apply to this solicitation unless otherwise noted herein.

1.2 Distributed Denial of Service (DDoS) attacks are used to render key resources unavailable [1]. For example, a classic DDoS attack might disturb a financial institution's website, and temporarily block a consumer's ability to conduct online banking. A more strategic attack makes a key resource inaccessible during a critical period. Some examples of this type of attack may include rendering a florist's website unavailable on Valentine's Day, slowing or blocking access to tax documents in mid-April, or disrupting communication during a critical trading window. Prominent DDoS attacks have been conducted against financial institutions, news organizations, providers of internet security resources, and government agencies [2]. Any organization that relies on network resources is considered a potential target and the current environment offers many advantages to the attacker. The Distributed Denial of Service Defense (DDoSD) Project aims to shift the advantage from the DDoS attacker to the defender who is providing a network service.

2. Project Description/Scope

2.1 The DDoSD project includes three complementary Technical Topic Areas (TTAs):

2.1.1 TTA #1, Measurement and Analysis to Promote Best Current Practices
2.1.2 TTA #2, Tools for Communication and Collaboration
2.1.3 TTA #3, Novel DDoS Attack Mitigation and Defense Techniques

2.2 TTA #1 aims to slow the growth rate in denial of service attacks and make current attacks more difficult by promoting the deployment of existing best practices. Recognizing that best

practices alone are not sufficient, TTA #2 will develop tools and techniques that allow organizations to collaboratively respond to attacks. Finally, TTA #3 addresses new threats as denial of service attack concepts are being applied to non-traditional targets, such as emergency management systems and cyber physical systems.

2.3 Each TTA is discussed in detail below and specific objectives for each TTA are also provided. Of particular note, it is anticipated that both metrics and analysis techniques to measure the development progress will evolve during the project.

3. Technical Topic Areas

3.1 TTA #1: Measurement and Analysis to Promote Best Current Practices

3.1.1 Some DDoS attacks make use of spoofed source addresses. Existing best practices such as Best Current Practice (BCP) 38 – Request For Comment (RFC) 2827 [4] filter out forged addresses at the network periphery. Additional best practices such as BCP 84 – RFC 3704 [5] extend this guidance to more complex deployments. The collection of anti-spoofing best practices could help mitigate DDoS attacks that rely on forged addresses. Measurement and analysis tools are required to test whether new anti-spoofing deployments are successful, verify existing anti-spoofing practices are working correctly, and provide evidence to demonstrate both advantages and limitations when anti-spoofing best practices are deployed in an organization.

3.1.1.1 Objective 1 – Open Source Software Tool for Anti-Spoofing Assessment. Efforts funded under this TTA will be expected to deliver an open source anti-spoofing measurement tool. The tool should allow a site to determine whether it has successfully deployed anti-spoofing best practices and provide on-going monitoring to verify the anti-spoofing best practices continue to operate correctly after network changes occur. An open source code release is due ***nine months from project start***; also, offerors must include a timeline for subsequent updates based on lessons learned from either test and evaluation or deployment activities. Prior to any code delivery, the code must be audited and evaluated for security concerns in an effort to make it suitable for operational deployment. One way to demonstrate the code has been audited and evaluated for security concerns is to use the capabilities provided by the DHS Software Assurance Marketplace (SWAMP) [6] to analyze, and if needed, improve the code. Offerors should detail their plans for software audits in any response to this TTA.

3.1.1.2 Objective 2 – Anti-Spoofing Metrics and Analysis. In addition to providing the measurement tool discussed above, offerors must describe how the measurement results, provided by the tool developed, can be used to assess and promote the deployment of anti-spoofing best practices. Then building on the measurement tool capabilities, the technical approach should describe how anti-spoofing best practices could be measured, identify anti-spoofing metrics, and describe a process to capture and analyze data to determine whether best practice deployment is (or is not) advancing. RFC2827 was published in 2000 and some measurement efforts have tracked deployment [7]. This can provide a starting point, but simply reporting the number of organizations that deploy BCP38 is not sufficient. The overall goal is not to achieve 100% deployment. It is anticipated that there are many organizations that will never deploy BCP38 or BCP 84, and other organizations where deployment of BCP38 cannot be accurately measured. The DDoSD goal is to document how one can measure and manage best practice deployment efforts in order to achieve the *most effective deployment*. The results will be

used to direct deployment efforts toward locations that provide the greatest marginal increases in protection against DDoS attacks. This work is intended as a companion to broader efforts by DHS and NIST aimed at promoting the deployment of anti-spoofing best practices.

3.1.2 Section 4.1 below identifies key deliverables for this TTA.

3.2 TTA #2: Tools for Communication and Collaboration

3.2.1 The distributed nature of the DDoS attacks provides several advantages to the attacker. An attack often comes from a large number of compromised computers that span multiple organizations. Further, as network bandwidth and computational power increases, the attacker benefits from the increased resources, providing the capability to conduct more powerful attacks. To counter the threat, organizations that make use of network services must invest in resources that keep pace with the increasing significance of the attacks. Organizations that fail to keep pace run the risk of being overwhelmed. In addition, organizations that deploy resources carelessly may simply provide the attacker with easily compromised resources that can then be used in future attacks. Even organizations with global scale capability, including those providing security related services, have faced challenges in keeping pace with vast DDoS attacks. [2]

3.2.1.1 Objective: Develop tools and techniques that allow a medium size organization to withstand a one terabit per second attack originating from one thousand locations.

3.2.1.2 The largest DDoS attacks have grown in scale from tens of gigabits per second to hundreds of gigabits per second. This TTA supposes that an attack might exceed one Terabit per second (Tbps) and originate from over one thousand locations. This TTA further supposes that a medium size organization is the attack target. Characteristics of a medium size organization include multi-homing to a small number of transit providers and limited geographic distribution of resources. Examples of a medium size organization might include a government agency, financial institution, critical infrastructure provider, enterprise network, or university. Implicit in the problem statement is that a medium size organization is not able to absorb 1 Tbps at its edges.

3.2.1.3 Collaboration and communication are essential to mitigating attacks and shifting the advantage from the attackers to the defenders [9, 10]. There have been significant advances in how attacks are coordinated. For example, botnet command and control systems are increasingly sophisticated. Collaboration tools for DDoS defense have not seen equally compelling advances. DDoS defense collaboration and communication may involve multiple parties including the enterprise networks under attack, Internet Service Providers (ISPs), enterprise networks with the compromised machines, and even relevant government agencies with responsibility for tracking and/or assisting in DDoS defense. Any collaboration and information sharing across these groups must address technical challenges as well as legal and organizational policy challenges. For example, technical requirements on attribution and authentication may be needed. In addition, it is equally (if not more) important that the approach to attribution and authentication respect disclosure and privacy policies and meet legal requirements.

3.2.1.4 Offerors may build upon existing preliminary tools or propose new potentially transformative approaches. Collaboration could be based on either a centralized or distributed approach. Whichever direction is chosen, the offerors must address the operational and policy challenges associated with the approach. Centralized systems for collaborating must address

issues of who would operate the centralized system, why would the community trust these operators, and how a centralized operator would sustain itself. Distributed systems must address issues of how does one join and leave the distributed network, how are malfunctioning and malicious participants handled, and what incentives drive sustained participation in the system. Technical approaches must also discuss how tools and technologies developed could be deployed into operation and must not assume universal deployment of a particular technique. Finally, applicability to critical infrastructure sectors and government agency networks is encouraged.

3.2.1.5 To demonstrate results, offerors will need to describe how their technical approach, including identifying appropriate metrics for measurement, will meet the aforementioned objective of this TTA (simulation or extrapolation from experiments is acceptable). Data used to demonstrate capabilities and information sharing across projects and performers is encouraged. Multiple performers using comparable data is beneficial to each individual performer since it can permit independent replication of results. The DHS PREDICT [12] project provides opportunities for obtaining and sharing data that may be relevant to this TTA.

3.2.2 Section 4.2, below, identifies key deliverables for this TTA.

3.3 TTA #3: Novel Attack Mitigation and Defense Techniques

3.3.1 This TTA seeks to address new variations of denial of service attacks. Denial of service attack concepts are being directed at a growing range of services. For example, in spring 2013, DHS and the Federal Bureau of Investigation (FBI) issued warnings for denial of service attacks targeting emergency management services, such as 911 systems [13]. Systems including, but not limited to, mobile devices, cyber physical systems, and critical infrastructure components are all potential targets for these attacks. Further, new variations of denial of service attacks exploit vulnerabilities, such as overwhelming power supplies, software vulnerabilities, and other features [14]. Too often the response to new types of attacks and targets is reactive; attackers develop new techniques and/or target new systems and this drives mitigation efforts. Ideally, new techniques and new targets would be anticipated and defenses would be proactively developed before large scale attacks occur. Therefore, the goal of this TTA is to identify potential targets for DDoS that have not been subject to known large scale DDoS attacks, and to develop DDoS mitigation capabilities that will be able to withstand a DDoS attack that is double in magnitude from the capabilities of the target's DDoS defense capability at the beginning of the project. Emergency management systems and cyber physical systems are examples of non-traditional targets that are vulnerable to denial of service and most relevant to this TTA.

3.3.2 To be responsive to this TTA, offerors should identify one or more non-traditional targets of DDoS attacks and describe mitigation strategies for each non-traditional target. Technical approaches will also need to describe both how the target is vulnerable to the attack and provide potential paths for mitigation of the vulnerability. Offerors must identify and explain the relevant metrics for the non-traditional DDoS target(s) they address. The metrics may vary depending on the target. For example, metrics may include standard measures, such as traffic volume in bits per second for a network device, or number of calls received for an emergency response system, or some other metric meaningful to the target(s) being considered. Further, to support evaluation and establish developmental milestones, technical approaches must provide details to define the establishment of the initial baseline capability of DDoS defense posture of the target intended to be protected.

3.3.3 To demonstrate results, offerors will need to describe how their technical approach, including identifying appropriate metrics for measurement, will meet the aforementioned goal of this TTA (simulation or extrapolation from experiments is acceptable). Data used to demonstrate capabilities and information sharing across projects is encouraged. Multiple performers using comparable data is beneficial to each individual performer since it can permit independent replication of results. The DHS PREDICT [12] project provides opportunities for obtaining and sharing data that may be relevant to this TTA.

3.3.4 Section 4.3 below identifies key deliverables for this TTA.

4. Project Structure

The DDoSD project is structured into three distinct TTAs that aim to 1) slow the growth in DDoS attacks by adopting best practices, 2) provide existing targets more effective tools and techniques for response and mitigation, and 3) anticipate new types of attacks before they occur.

4.1 TTA #1 Key Deliverables

Any awards resulting from submissions received under TTA #1 will require quarterly status reports on anti-spoofing best practice deployment. These quarterly reports will be required to both assess anti-spoofing best practice deployment efforts to date and help direct anti-spoofing best practice deployment efforts for the upcoming quarter. Also, status reports should document value to the overall effort on anti-spoofing best practice deployment. Including status reports, the key deliverables required for TTA #1 are:

DELIVERABLES	DUE DATE
Quarterly Status Reports on Deployment of Anti-Spoofing Best Practices	3 months after award
Open Source Anti-Spoofing Best Practice Monitoring Tools	9 months from project start
Subsequent Monitoring Tool Code Releases	At most 6 months from previous code release
Updated Approach to Measuring Deployment of Anti-Spoofing Best Practices	As warranted by status report results; anticipate updates will be needed at least annually

4.2 TTA #2 Key Deliverables

The key deliverables required for TTA #2 are:

DELIVERABLES	DUE DATE
Quarterly Technical Status Reports	3 months after award and quarterly thereafter
Evaluation (including metrics) and Transition Plan	To be updated as needed
Demonstration of Capabilities (using Evaluation Plan provided)	Annually

Demonstration of Ability to Withstand 1 Tbps attack from 1000 locations	At project completion

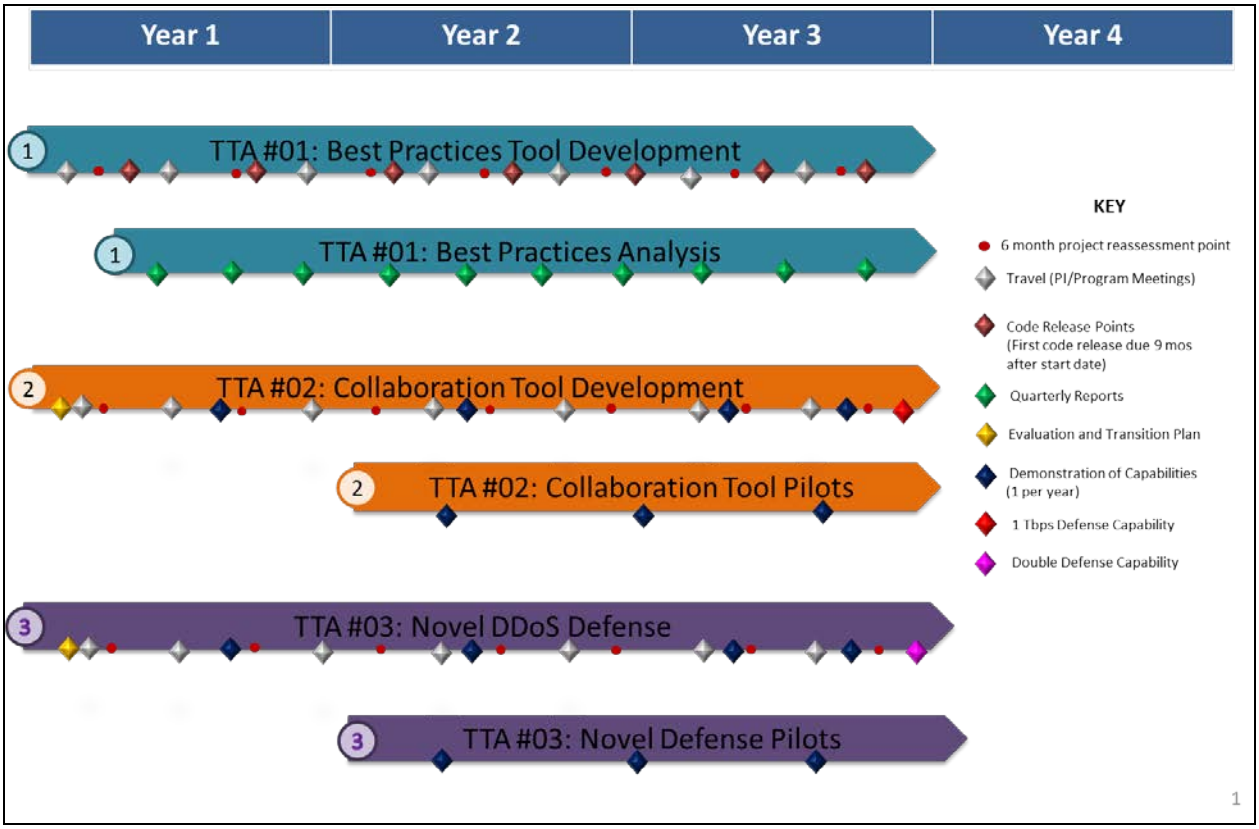
4.3 TTA #3 Key Deliverables

The key deliverables required for TTA #3 are:

DELIVERABLES	DUE DATE
Quarterly Technical Status Reports	3 months after award and quarterly thereafter
Evaluation (including metrics) and Transition Plan	To be updated as needed
Demonstration of Capabilities (using Evaluation Plan provided)	Annually
Demonstration of Ability to Double Capacity (using Evaluation Plan provided)	At project completion

5. Project Schedule/Milestones

A notional project schedule is shown below including anticipated meetings and demonstrations.



6. Special Instructions/Notifications

6.1 Response Dates

Event	Time Due	Date or Date Due
Industry Day	N/A	June 26, 2014
White Papers Due	4:30 PM EDT	July 22, 2014
Notification of White Paper Evaluation Results	N/A	On or About August 29, 2014
Proposals Due	4:30 PM Eastern Time	~~November 5, 2014~~ February 19, 2015

6.2 General Instructions and Information

6.2.1 This BAA solicitation (HSHQDC-14-R-B0017, as amended) includes a requirement to submit white papers, prior to the submission of proposals, subject to the date identified in the "Response Dates" table above.

6.2.2 Procedures for submission of white papers and proposals in the DHS S&T Portal are provided in paragraph 10 of DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003. Note that offerors must complete the company/organization portal registration PRIOR to submitting a white paper for the first time. Ensure adequate time to complete the company/ organization registration as delays in this process will not be authorization for late submissions of white papers. Company/organization registration information is located in paragraph 10.1 of DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003. In addition, each white paper and subsequent proposal requires registration in the portal. Information regarding white paper and proposal registration is located in paragraph 10.2 of DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003.

6.2.3 Offerors may provide multiple white paper and proposal submissions; however, each submission must only address one TTA and must be distinct and self-contained without any dependencies on other work of any kind. Each submission must clearly state which TTA is being addressed.

6.2.4 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 [6].

6.2.5 DHS has a strong preference for open source licensing of software for all software developed and delivered and the licenses for all proposed software deliverables will have to be identified in submitted white papers and proposals (note: the DHS HOST [11] project provides directions and opportunities for promoting open source software). However, as an alternative to open source release, offerors may also offer a strong technical transition plan for deployment of the technologies developed.

6.2.6 As stated in DHS S&T CSD BAA HSHQDC-14-R-B0005, Amendment 00003, DHS S&T reserves the right to select for award and to fund all, some, or none of the proposals received in response to this BAA solicitation.

6.2.7 The Evaluation Criteria in DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003 [3] Section 11 “EVALUATION OF WHITE PAPERS AND PROPOSALS” applies.

6.3 Foreign Participation

Offerors are reminded that foreign participation may occur as defined in DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003, Section 1.3. Therefore, for offerors should provide unit costs for any deliverable not anticipated for delivery in a softcopy format.

6.4 Export Control Requirements

Offerors are reminded of the export control markings required by DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003, Section 8.6.8 (for white papers) and Section 9.6.4 (for proposals).

6.5 Type Classification Ceilings

DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003, describes the Type Classifications for proposals. Specific to this call, the ceiling values for each type are as follows:

6.5.1 Type I – Type I awards are limited to a total contract value not to exceed $3,000,000.00, not including operational evaluation, pilot, and/or transition options.

6.5.2 Type II – Type II awards are limited to a total contract value not to exceed $2,000,000.00, not including operational evaluation, pilot, and/or transition options.

6.5.3 Type III – Type III awards are limited to a total contract value not to exceed $750,000.00, not including operational evaluation, pilot, and/or transition options.

6.6 Travel

6.6.1 For purposes of estimating costs for white papers and proposals, offerors should anticipate travel to three (3) project meetings per year.

6.6.2 DHS Cyber Security Division holds an annual PI meeting where all DHS CSD funded efforts are expected to present. Projects will be required to provide a briefing, typically 20 minutes, and are strongly encouraged to provide demonstrations when appropriate. The PI meeting is typically 2.5 days and attendance at the full event is encouraged.

6.6.3 In addition to the annual DHS PI Meeting, the DDoSD Project will hold two meetings each year. Meetings will be arranged by TTA and the meeting for each TTA is expected to last one day. When possible, TTA meetings will be held on adjacent days so funded efforts in one TTA can optionally attend other TTA meetings.

6.7 White Paper Requirements

This BAA solicitation (HSHQDC-14-R-B0017, as amended) requires the submission of a white paper, compliant with the aforementioned response dates, to be considered for participation in the submission of proposals. Offerors MUST submit a white paper in accordance with the Department of Homeland Security (DHS), Science & Technology (S&T), Cyber Security Division (CSD), 5-Year Broad Agency Announcement (BAA), HSHQDC-14-R-B0005, Amendment 00003. Submissions not in compliance with DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003, may be rejected (note: the cover page created by the DHS S&T BAA Portal must be included, but does not count against the page count). The DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003[3] Section 8 discusses white paper preparation and describes the required white paper content. In addition to the guidance in Section 8, the following special instructions are added:

6.7.1 For submissions responding to TTA #2, add to Section 8.7.1 Item C "Technical Content" address the evaluation methodology (in contemplation of the Evaluation Plan deliverable listed in the TTA #2 Key Deliverables above) such that the methodology discusses how the proposed effort could be evaluated to demonstrate effectiveness against 1 Tbps second attack from 1,000 locations.

6.7.2 For submissions responding to TTA #3, the following requirements are added to Section 8.7.1 Item C "Technical Content":

> In addition to the content already described in Section 8.7.1, the white paper should address known relevant metrics while discussing a plan to generate the metrics that would be used to assess the proposed system and how the proposed effort could be evaluated to demonstrate a capability to withstand a DDoS attack that is double in magnitude from the capabilities of the target's DDoS defense capability at the beginning of the project.

6.8 Proposal Requirements

To be considered for award, offerors **MUST** submit a proposal, compliant with the aforementioned response dates, in accordance with the DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003. Submissions not in compliance with DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003 may be rejected (note: the cover page created by the DHS S&T BAA Portal must be included, but does not count against the page count). The DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, AMENDMENT 00003 [3] Section 9 discusses proposal preparation and describes the required proposal content; however, in addition to the guidance in Section 9, the following special instructions are added:

6.8.1 Maximum Page Count.

6.8.1.1 Volume 1 – Technical Proposals.

6.8.1.1.1 For any proposal submitted in response to this solicitation/call, Volume 1, the technical proposal, ***SHALL NOT*** exceed 30 pages. This maximum page count of 30 pages

includes ***all*** information required to be included in Volume 1 of any submitted technical proposal. Information required to be included in Volume 1, Technical Proposal, is outlined in:

- Sections 9.6.1(a) through 9.6.1(v) of BAA HSHQDC-14-R-B0005, Amendment 00003; ***and***
- Any additional proposal information required by this solicitation/call (HSHQDC-14-R-B0017, as amended).

6.8.1.1.2 Notwithstanding any language used in BAA HSHQDC-14-R-B0005, Amendment 00003, Sections 9.6.1(a) through 9.6.1(v), such as "appendix", "resumes", etc., ***all*** required information in these sections counts towards the maximum page count of 30 pages. This includes the required "Cover Page", "Table of Contents", "Official Transmittal Letter", "Quad Chart", "Resumes", "Assertion of Data Rights", and so on, identified in Sections 9.6.1(a) through 9.6.1(v) of BAA HSHQDC-14-R-B0005, Amendment 00003.

6.8.1.1.3 Any Volume 1, Technical Proposal, received in response to this solicitation/call exceeding the maximum page count of 30 pages ***WILL NOT BE EVALUATED AND THEREFORE, WILL NOT BE ELIGIBLE FOR AWARD.***

6.8.1.2 Volume 2 - Cost Proposals. ***THERE IS NO PAGE COUNT LIMITATION FOR VOLUME 2, PRICE/COST PROPOSAL SUBMISSIONS.*** Information required to be included in any submitted Volume 2, Cost Proposal, is outlined in:

- Sections 9.6.2(a) through 9.6.2(c) of BAA HSHQDC-14-R-B0005, Amendment 00003; ***and***
- Any additional proposal information required by this solicitation/call (HSHQDC-14-R-B0017, as amended).

6.8.2 For proposals responding to TTA #2, the following requirements are added to HSHQDC-14-R-B0005, Amendment 00003, Section 9.6.1.i, "Testing and Evaluation":

> In addition to the content already described in Section 9.6.1, the content must discuss how the proposed effort could be evaluated in order to demonstrate effectiveness against 1 Tbps attack from 1,000 locations by the project conclusion.

6.8.3 For proposals to TTA #3, the following requirements are added to HSHQDC-14-R-B0005, Amendment 00003, Section 9.6.1.i., "Testing and Evaluation":

> In addition to the content already described in Section 9.6.1, the content must identify metrics used to assess the proposed system and discuss a plan to generate the metrics that would be used to assess the proposed system and how the proposed effort could be evaluated to demonstrate a capability to withstand a DDoS attack that is double in magnitude from the capabilities of the target's DDoS defense capability at the beginning of the project.

6.8.4 Subcontractor Cost Submission: Referencing, DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003, Section 9.6.2.b.(6), if the subcontractor costs cannot be included with a prime's detailed cost breakdown, then the prime contractor must

stipulate on the detailed cost breakdown that the costs presented only represent those from the prime and the subcontractor's costs are provided separately as an attachment to an e-mail sent to BAA-14-R-B0005@hq.dhs.gov. The subject line of the email shall say "Separate Subcontractor Cost Submission – [insert the white paper or proposal number assigned from the DHS S&T BAA Portal]". The body of the email shall contain the following:

1) The prime entities name which should be the same entity that is registered in the BAA portal;
2) A POC (name and phone number) from the prime entity; and
3) For each subcontractor proposal attached, include:
   - The name of the subcontractor for the subcontractor proposal attached; and
   - A POC (name and phone number) from the subcontractor whose proposal is attached.

The separate subcontractor cost proposal must be as detailed as the offerors's cost proposal and must be received at the location designated in the individual call no later than the closing date and time specified by the call. Note that email transmission time may vary depending on the file size of the attachment(s) included in the email. Therefore, ensure there is adequate time for receipt of the email and any accompanying attachments of the subcontractor(s) cost proposal(s) by the required closing date and time. Acceptance of the email submission is dependent upon the actual date and time the e-mail and any accompanying attachment(s) is RECEIVED by the in-box for BAA-14-R-B0005@hq.dhs.gov. **NO SEPARATE SUBCONTRACTOR COST PROPOSALS RECEIVED WILL BE ACCEPTED IF RECEIVED AFTER THE AFOREMENTIONED PROPOSAL DUE DATE.**

6.9 Contractual or Technical Inquiries

All contractual or technical inquiries to this BAA solicitation (HSHQDC-14-R-B0017, as amended) must be emailed to BAA-14-R-B0005@hq.dhs.gov no later than 4:30 PM EDT on February 11, 2015. Emails submitting questions are to include "Questions for DDoSD BAA Solicitation" in the subject line. All questions and responses will be posted on the Federal Business Opportunities website http://www.fbo.gov. Questions will only be accepted and answered electronically.

6.10 Order of Precedence

In the event that any of the terms and conditions contained in this solicitation (HSHQDC-14-R-B0017, as amended) conflict with terms and conditions included in DHS S&T CSD 5-Year BAA HSHQDC-14-R-B0005, Amendment 00003, the terms and conditions in this BAA solicitation (HSHQDC-14-R-B0017, as amended) shall take precedence.

Footnotes:

1. Distributed Denial of Service (NY Times, April 1, 2013); http://www.nytimes.com/2013/04/02/science/distributed-denial-of-service.html
2. Understanding Denial-of-Service Attacks: http://www.us-cert.gov/ncas/tips/ST04-015
3. DHS Cyber Security Division Broad Agency Announcement HSHQDC-14-R-B0005; https://www.fbo.gov/spg/DHS/OCPO/DHS-OCPO/HSHQDC-14-R-B0005/listing.html
4. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing; P. Ferguson and D. Senie; RFC 2827;

http://www.ietf.org/rfc/rfc2827.txt
5. Ingress Filtering for Multihomed Networks,; F. Baker and P. Savola, RFC 3704; http://tools.ietf.org/html/rfc3704
6. DHS Software Assurance Marketplace (SWAMP); https://continuousassurance.org/
7. Initial Longitudinal Analysis of IP Source Spoofing Capability on the Internet; Robert Beverly, Ryan Koga, kc claffy; http://www.internetsociety.org/doc/initial-longitudinal-analysis-ip-source-spoofing-capability-internet
8. A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms; Mirkovic, Martin, Reiher; http://www.lasr.cs.ucla.edu/ddos/ucla_tech_report_020018.pdf
9. REN-ISAC Alert: Prevent Your Institution From Being An Unwitting Partner In Denial Of Service Attacks; http://www.educause.edu/discuss/discussion-groups-related-educause-programs/security-discussion-group/ren-isac-alert-prevent-your-institution-being-u
10. A Framework for Collaborative DDoS Defense G. Oikonomou, J. Mirkovic, P. Reiher and M. Robinson, ACSAC 2006, http://www.isi.edu/~mirkovic/publications/ACSAC06.pdf
11. DHS Homeland Open Security Technologies (HOST); https://www.dhs.gov/csd-host
12. DHS Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT), https://www.predict.org
13. DHS, FBI warn over TDoS attacks on emergency centers, http://www.csoonline.com/article/731069/dhs-fbi-warn-over-tdos-attacks-on-emergency-centers
14. "Power Attack: An Increasing Threat to Data Centers", Zhang Xu, Haining Wang, Zichen Xu, and Xiaorui Wang, the 21st Network and Distributed System Security Symposium (NDSS 2014), San Diego, California, February 2014.
15. DHS Cyber Defense Technology Experimental Research (DETER) network, (http://deter-project.org)