	THIS SECTION WITH THE BLUE HIGHLIGHT CONTAINS UPDATES TO THE SET OF RESPONSES THAT WERE SHOWN IN THE BIDDER'S CONFERENCE ON 2/5/2025. THESE ARE ENUMERATED FROM ITEMS "A" TO "M" AND WILL BE REFERRED IN OTHER ANSWERS BELOW AS A "REFERENCE RESPONSE"	
	IN THE RFP but asked about in initial questions received	
A	TTX: Other agencies or participants	TTX 1: BRS only; perhaps a slight expansion TTX 2: City of Boston: Treasury, Group Health, IT (DoIT) plus Pension Software Vendor (Vitech)
B	TTX duration	TTX sessions are expected to be a half-day each
	GENERAL REFERENCE	
C	Are sessions in person, hybrid, or remote?	We anticipate all sessions to be in person but secondary TTX role participation could be entertained
D	Is there a budget for the work?	This is a competitive bid process; there is no predetermined budget
E	Is there an incumbent vendor or existing contract?	There are no existing vendors nor prior experience with TTX at BRS
F	Will there be security checks?	Security checks on Offeror or Offeror staff will not be conducted; however the Offeror must complete the contractual forms relating to its CORI practices and contractual documents requiring disclosure of pending legal matters, "clean" tax status, etc.
G	Are the contractual documents required?	Yes. All 8 documents at the bottom of page 6 must be completed to the extent possible by Offerors AND the two forms on page 7 must be signed and scanned in as well. Once awarded, we estimate 2 to 3 weeks for contract documents to be processed.
H	Wil the awardee need to become a Boston vendor?	BRS will direct the awardee through the online vendor registration process
I	Are there other cybersecurity activities expected during the RFP project?	There is a small companion activity not in the RFP relating to enhanced staff and partner cybersecurity awareness
	Is the infrastructure cloud based? Who manages?	Infrastructure is increasingly cloud-oriented: Google suite (email, drives, etc.) has replaced share drives (DoIT) The pension software solution (V3 from Vitech) is AWS-based Note that the cybersecurity assessment conducted in 2022 gave high marks to DoIT and Vitech
J		
K	Will BRS provide meeting rooms?	BRS will provide a suitable meeting room for planning or TTX meetings
	EXPANDED ANSWERS (after the Bidders' Conference)	
L	KPI, success metrics, etc.	Per BRS cybersecurity advisors: (a) Measurable increase in the cyber fluency and confidence of BRS executives (b) best practice deliverables
M	How will project lessons learned be used / applied?	BRS has committed to at least annual refresh of TTX activities

	QUESTIONS #1 to #36 WERE RECIVED PRIOR TO THE BIDDERS'S CONFERENCE		
#	Question	Answer	Received
1	What are the primary objectives and key focus areas for these HSEEP-compliant exercises?	"aims to enhance the agency's resilience and preparedness in safeguarding sensitive financial information and maintaining trust with stakeholders" (RFP page 3)	2/3/2025
2	Are there specific threats, hazards, or scenarios (e.g., natural disasters, cyber incidents, active shooter) the exercises should address?	No	2/3/2025
3	Who are the key stakeholders and agencies expected to participate?	See Reference Response "A"	2/3/2025
4	Will there be multi-jurisdictional or multi-agency involvement?	See Reference Response "A"	2/3/2025
5	Are there specific roles or functions (e.g., law enforcement, EMS, public health, emergency management) other than the agencies listed in the RFP that must be included?	No	2/3/2025
6	Are there existing emergency response plans or frameworks the exercises should align with?	The current Incident Response Plan will be shared at the start of the project under NDA	2/3/2025
7	Do you have past After-Action Reports (AARs) or Improvement Plans (IPs) that should be considered when designing the exercises?	No	2/3/2025
8	Are there specific compliance requirements beyond HSEEP (e.g., FEMA, NIMS, ICS)?	No	2/3/2025
9	Will the exercises be conducted in person, virtually, or in a hybrid format?	See Reference Response "C"	2/3/2025
10	Are there specific locations or facilities designated for the exercises?	The RFP describes half day sessions in a suitable meeting room which BRS will provide	2/3/2025
11	What resources (personnel, technology, equipment) will be provided by the client?	None	2/3/2025
12	What metrics or key performance indicators (KPIs) will be used to measure exercise success?	See Reference Response "L"	2/3/2025
13	Are there specific reporting formats or templates required for the After-Action Report (AAR) and Improvement Plan (IP)?	No	2/3/2025
14	How will exercise findings be integrated into future training and preparedness efforts?	Part of proposed project	2/3/2025
15	What is the allocated budget for exercise development and execution?	Competitive bid	2/3/2025
16	Are there any cost constraints or funding limitations we should be aware of?	Competitive bid	2/3/2025
17	Are there specific invoicing, reporting, or payment schedule requirements?	No	2/3/2025

18	Are there any security clearances, certifications, or background checks required for personnel involved in the exercise?	Vendor must disclose CORI practices; see required contractual documents	2/3/2025
19	Will there be data collection or information-sharing requirements that involve confidentiality or privacy concerns?	No	2/3/2025
20	What are the biggest challenges you've faced in previous exercises, and how do you hope to address them in this one?	N/A	2/3/2025
21	How will lessons learned from this exercise be used to improve future training and preparedness efforts?"	Part of proposed project	2/3/2025
22	What is the process for signing the contract to begin work?	Submitting contractual documents included in the RFP	2/3/2025
23	What is the process to become a verified vendor for Boston Retirement System?	Submitting contractual documents included in the RFP	2/3/2025
24	How long is the process to become a vendor for BRS?	See Reference Response "G"; see Reference Response "H"	2/3/2025
25	Are you currently working with a vendor who has provided these services in the past? If Yes, who is that vendor?	No	2/3/2025
26	Are you replacing the current vendor or is this a new vendor project?	New	2/3/2025
27	1. Is it remote work or on-site work?	See Reference Response "C"	2/5/2025
28	2. Is there currently an incumbent company or previous incumbent, who completed similar contract performing these services? If so - are they eligible to bid on this project and can you please provide incumbent contract number, dollar value and period of performance?	No current incumbent or contract	2/5/2025
29	*3. Does the below mentioned forms are required to be submitted with proposal response?* ***"Form CM 10-11 Standard Contract, Form CM 15B_CORI, Form CM 16 Wage Theft Prevention, Form CM06 Certificate of Authority For Corporations Only, Form CM09 Contractor Certification, Living Wage Form 2, and Living Wage Form 8"***	See Reference Response "G"	2/5/2025
30	4. Specify the VLAN details how many is included in the Scope?	N/A	2/5/2025
31	5. Can you please provide current number of infrastructure details (Physical Server, Virtual Server, Network Devices, etc.)?	N/A	2/5/2025
32	6. How much (%) of the infrastructure is in cloud?	See Reference Response "J"	2/5/2025

33	7. In the IT department/environment, how many employees work?	BRS: 3. DoIT: over 150.	2/5/2025
34	8. Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?	See Reference Response "J"	2/5/2025
35	9. Is Q&A web meeting is mandatory to attend?	No; the session is optional.	2/5/2025
36	10. Is there a funding/financial/budget range estimated that can help us to provide a quotation for this project?	See Reference Response "D"	2/5/2025
	QUESTIONS #37 to #69 AROSE AT THE BIDDER'S CONFERENCE		
37	Does B69:C89BRS carry cyber insurance, and if so, with who?	BRS does carry cyberinsurance but declines to disclose the provider; if of interest, post award this info can be shared	
38	What time on Friday, February 14th is the submission deadline?	The submittal deadline is 5:00 pm on February 14, 2025	
39	There doesn't seem to be a formal certification for being HSEEP compliance. Are you relying on us to report how our proposed TTX is HSEEP compliant?	Yes; we would expect that from our provider. Note that BRS cyber advisors, including Bill Oates and the CITY of Boston CISO, will help monitor for compliance.	
40	How many participants and observers are expected for Tabletop Exercise 2 (in terms of maximum participants similar to what was defined for Exercise 1)?	TTX 1 was cast in the RFP (page 3) as no more than 5-10 active BRS leadership participants (executives/Key staff) and observers (but no more than 15 people in total); our best sense is that TTX will approximately double in attendees.	
41	Will this be purchase be governed ITS 75?	No.	
42	Relating to CORI - can you please send around/publish the CM Form 15B for review?	BRS will not be sending any contract documents. At the bottom of page 6 on the RFP are 8 links that a click through will lead to the documents.	
43	On the bottom of page 5 it lists minimum of 3 and max of 5 relevant projects. In the scoring table it lists 2 and 4, which should we use?	Because we stated during the Bidders' Conference that 2 to 4 would be fine for both purposes, Offerors may use the 2 to 4 range for both. However, a closer reread shows that the 3 to 5 at the bottom of page 5 refers to project experience descriptions but the second row of the Scoring Elements tables on page 6 refers to References. On the project experience customers, BRS indicated that, while under NDA, it may want to know who they are but would not expect to contact. Conversely, offerors should expect that the references will be contacted.	
44	RFP says BRS expects to be mid-March to mid-June project with all work completed by June 30, 2025. Is there any expectation this would extend further so that we can plan for resource allocation?	The timeframes can't be moved to wait on Offeror resources.	

45	Administer cybersecurity training to employees - Any idea on what they are looking for? I'm thinking some general (OWASP) training to include insider threat and mobile security training if applicable	Not applicable	
46	Implement a Managed Detection and Response (MDR) solution.- I'm assuming we will be employing some Managed Service Provider for this one. They are companies out there that specialize in this and I think it would be better than attempting to build our own solution. Do we know the size of the enviro	Not applicable	
47	Purchase and configure a hardware firewall - They specifically said they want a "hardware" firewall solution so that rules out AWS or AZURE. I don't think this will be a heavy lift. I'm assuming they only have one egress point or a DMZ they want to protect. Again, the size of the environment and	Not applicable	
48	So no state contract vehicle is required?	Correct, contracting documents are as listed in Reference Response O	
49	Currently BRS has IRP plan in place and awardee will have access to that document once award is made?	Yes to both parts of the question.	
50	o Are there any specific incident scenarios you would like to focus on for the tabletop exercises (e.g., cyberattack, physical security breach, natural disaster)?	No. As discussed, the focus will be a cyber incident as opposed to natural disaster or some of the other HSEEP scenarios.	
51	Is preference given for local offerors?	No. We suspect that reduced or no travel expenses may indirectly favor local vendors.	
52	For execution of the two TTX's do you want them to be executed back to back or would you want a gap between those exercises with AAR given after each?	With a gap, not back to back. Please see steps 3 to 6 on page 3 of the RFP for context.	
53	Estimated number of participants for the first TTX?	TTX 1 was cast in the RFP (page 3) as no more than 5-10 active BRS leadership participants (executives/Key staff) and observers (but no more than 15 people in total).	
54	Can the TTX's be a combination of both remote and onsite tabletops?	No. Please see Reference Response "C" for a narrow possible exception.	
55	So we should have two AAR's for each TTX correct?	Yes.	
56	Delivery mode of the project, onsite, off-site, hybrid?	Please see Reference Response "C"	
57	do we need any special access for onsite work? US Citizens? Background Checks?	No	
58	How many injects are expected in each activity	Not yet determined; expect to be part of the planning for each TTX.	
59	Expected duration/mandays for each ttx?	Please see Reference Response "B"	
60	Could offerors provide additional cybersecurity capabilities as an Appendix in the RFP?		

61	Costs proposal should be firm fixed pricing correct?	Yes. Firm fixed price.	
62	We will get copies of the responses correct?	They will be posted to the BRS website as described and shown during the session.	
63	Is the TTX scenario limited to the scope of BRS's Incident Response Plan and stakeholder roles? Is there an expectation that scenario design will need to consider other crisis management plans relevant to multi-agency stakeholders?	No.	
64	clarification responses to the questions presented in this meeting?	They will be posted to the BRS website as described and shown during the session.	
65	Does offeror need have government clearance	No	
66	Are revisions/negotiations to the "Standard Contract Document" amenable?	Generally no, and wholesale replacements are not on the table. However, if there is a specific issue or concern, it can be addressed with the BRS General Counsel (email address in the RFP). Please note that the question submittal period has ended.	
67	When was the IRP created or last updated?	Within the last year to update cyber insurance contact information but otherwise, no. Improving the IRP is a key goal of the RFP project.	
68	Will you let us know when the Q/A has been posted? Or should we just remember to review the website by Friday EOD?	As discussed, we don't have a notification process to Bidder's Conference attendees so the approach will be to use the BRS website.	
69	Regarding STEP 5. IMPLEMENT IMPROVEMENTS "...Ensure that everyone involved understands the changes and is prepared for future incidents." To what extent should vendor expect to provide training and awareness activities relating to IRP recommendations and updates?	Training and awareness activities are not expected.	