EDWARDS
PERFORMANCE SOLUTIONS

6085 Marshalee Drive, Suite 140
Elkridge, MD 21075
www.EdwPS.com

Dana L. Pickett, CISSP, CISM
Principal, Cybersecurity/CISO

DPickett@EdwPS.com
443.561.2634 (Direct)
410.215.1803 (Cell)

Sean Molony
Account Executive

Valsatech
Start Innovating Now

3104 Lord Baltimore Drive
Suite 207
Baltimore, MD 21244
Phone:410-720-2422
Fax:443-288-2222
Cell:410-935-3376
Sean.Molony@valsatechcorp.com

DK Consulting, LLC
A Woman-Owned Small Business

DK CONSULTING
www.dkconsult.net

Scott Peterson
Workforce and Client Continuity Manager

443-552-5851 ext. 109
443-235-2292 (cell)
443-283-4010 (fax)

speterson@dkconsult.net
www.dkconsult.net

8955 Guilford Road Suite 240 Columbia, MD 21046

AnchorTechnologies
Cyber Risk | Strategy, Identification, Management & Monitoring

BRIAN NELSON
Account Executive

Direct 202.888.1611
Main 410.295.7601
bnelson@anchortechnologies.com
6315 Hillside Court, Suite J
Columbia, MD 21046

www.anchortechnologies.com

Companion
DATA SERVICES

David Sorrell
Business Development Manager
Phone: 803-264-3961
Mobile: 803-201-6582
DAVID.SORRELL@companiondataservices.com

Columbia, SC Dallas, TX Baltimore, MD

Ashley Boykin
Business Development Manager

T: +1 443 449 0903
F: +1 443 672 2575
ashley.boykin@serigor.com
www.serigor.com

SeRigor
Strategy. Execution. Rigor.

400 East Pratt Street, Suite 800
Baltimore, MD 21202 USA

WBE/MBE Certified
IT Services & Government Solutions

Alphonsos La Favor
Capture Manager

alafavor@archsystemsinc.com
o: 410.277.9781
c: 973.573.1200

Arch SYSTEMS

2017-2018 Winner
FedHealthIT
Innovation Awards

Minority, Woman-Owned Small Business | 8(a) HUBZONE-Certified

1800 Washington Blvd., Suite 421
Baltimore, MD 21230

7000 Security Blvd., Suite 101
Baltimore, MD 21244

SCD
INFORMATION TECHNOLOGY

MDOT - MBE/WE
8(a) Certified Fi

Scott Surguy
Director - Sales and Marketing

7161 Columbia Gateway Drive #C
Columbia, Maryland 21046
www.scdit.com
Helpdesk - 410.290.0875

Office: 410.290.15
Fax: 410.290.19
Mobile: 443.848.22
scott.surguy@scdit.c

Grant Thornton
An instinct for growth™

Mohammed Zakari
Senior Associate

Grant Thornton LLP
333 John Carlyle St., Suite 500
Alexandria, VA 22314

D 703.637.2692
C 571.201.3779
F 703.837.4433
E mohammed.zakari@us.gt.com

PRG
Proposals

Federal, State, and Local
Proposal Development

Aaron Churchill
Proposal Writer, Compliance Officer
(443) 841-7354
amchurchill@prgproposals.com

30 E. Susquehanna Ave. Unit 11 Towson, MD 21286

MARYLAND STATE RETIREMENT AGENCY
TORFP G20B9400007
EXTERNAL NETWORK, INTERNAL WIRELESS NETWORK AND APPLICATION SECURITY TESTING
Wednesday, March 20, 2019 at 2:00P.M.

NAME/TITLE	ORGANIZATION NAME/ ADDRESS	TELEPHONE/FAX/EMAIL
1. David Sorrell / Business Development	Companion Data Services	O: (803) 264-3961 C: (803) 201-6582 david.sorrell@companiondataservices.com
2. Brian Nelson	ATI	bnelsen@anchortechnologies.com
3. Ellis Eisen	NetorianLLC	eeisen@netorian.com
4. Aaron Churchill / Proposal Writer	Netorian LLC	443-415-5801 achurchill@netorian.com
5. Jose Fernandez / President	CompSecDirect	443-345-0503 jfer@compsecdirect.com
6. Ashley Boykin / BizDev. Mgmr.	Serigor: 400 E. Pratt, #800 Baltimore, 21202	443.449.0903 ashley.boykin@serigor.com
7. Mike Hughes	OCG 9501 Sheridan Street Landover MD	202 431-2738 MHughes@OCG-INC.com
8. Scott Peterson	DK CONSULTING 8955 GUILFORD RD. COLUMBIA, MD	443-235-2292 speterson@dkconsult.net
9. Sean Molony	3104 Lord Baltimore Dr. #207 Windsor Mill, MD 21224	4109353376 sean.molony@ukratech.com
10. DANA PICHETT	EDWARDS PERFORMANCE SOLUTION. ELK RIDGE MD	443-561-2634 dpichett@edwps.com

MARYLAND STATE RETIREMENT AGENCY

TORFP G20B9400007

EXTERNAL NETWORK, INTERNAL WIRELESS NETWORK AND APPLICATION SECURITY TESTING

Wednesday, March 20, 2019 at 2:00P.M.

NAME/TITLE	ORGANIZATION NAME/ ADDRESS	TELEPHONE/FAX/EMAIL
1. SCOTT SURGUY DIRECTOR OF SALES	SCO INFORMATION TECH COLUMBIA MD	SCOTT.SURGUY@SCOIT.COM
2. AL LAFAVOR CAPTURE MANAGER	ARCH SYSTEMS	ALAFAVOR@ARCHSYSTEMSINC.COM
3. E Merrill VP	Edwards	EMerrill@Edwps.com
4. Mohammed Zekari	GT	Mohammed.Zakari@us.gt.com ~~Mohammed.Zekari@gt~~
5.		
6.		
7.		
8.		
9.		
10.		

MARYLAND STATE RETIREMENT AGENCY

PRE-PROPOSAL MEETING
FOR
EXTERNAL NETWORK, INTERNAL WIRELESS NETWORK,
AND APPLICATION SECURITY TESTING

SOLICITATION NUMBER (TORFP #): G20B9400007

MARCH 20, 2019
120 East Baltimore Street
Room 1654
Baltimore, Maryland

2:10 p.m. - 3:05 p.m.

PRESENT FROM MSRA:

MARGIE J. GORDON, Senior Procurement Officer
JOHN W. HAYNES, Procurement Officer
DAVID S. TOFT, SR., Director, IT, Security
IRA R. GREENSTEIN, Chief Information Systems Officer
THOMAS MONTANYE, Director, Systems Development
ROBERT A. DIEHL, Deputy Chief Information Systems Officer

ALSO PRESENT:

MOHAMMED ZAKARI, Grant Thornton LLP
SCOTT SURGUY, SCD Information Technology
DAVID SORRELL, Companion Data Services
ASHLEY BOYKIN, SeRigor

HUNT REPORTING COMPANY
Court Reporting and Litigation Support
Serving Maryland, Washington, and Virginia
410-766-HUNT (4868)
1-800-950-DEPO (3376)

JOSE FERNANDEZ, Compsec Direct
SEAN MOLONY, Valsatech
MICHEAL HUGHES, Oakland
SCOTT PETERSON, DK Consulting, LLC
BRIAN NELSON, Anchor Technologies
AARON CHURCHILL, Netorian, LLC
ELLIS M. EISEN, Netorian

ALSO PRESENT CONTINUED:

DANA PICKETT, Edwards Performance Solutions
EDWARD MERRILL, Edwards Performance Solutions
ALPHONSOS LA FAVOR, Arch Systems

PRESENT VIA TELEPHONE:

JEANNETTE KEARNY, Janus Associates
VAL KORICKI, Perspecta State and Local
JOHN PRESTIDGE, Perspecta
BHEEN DUVVURI, Cool Soft
HARSHID SHAH, Navitas
ASHISH RANA, Powersolv
ANIL VARMA, Navitas
AMIT SAMRIT, Valsatech
MICHAEL ROBERTSON, Oran, Inc.

REPORTED BY: KATHLEEN A. COYLE, Notary Public

P R O C E E D I N G S

MS. GORDON: Good afternoon. My name is Margie Gordon. I'm the task order procurement officer assisting with the process of this solicitation. On behalf of Maryland State Retirement Agency, I would like to welcome you to this task order pre-proposal conference. Today we'll share information with you concerning the task order request for proposal entitled external network, internal wireless network, and application security testing. The agency control number for this TORFP is G20P, as in Paul, 9400007. (Correction: TORFP is G20B9400007) Please note, to my right we have a court reporter from Hunt Reporting Company. They will be recording and transcribing this pre-proposal conference, and a copy of this transcript will be emailed to all offerors.

I'd like to start with introductions. Our

panel will introduce themselves, and then we'll have you introduce yourself. And we ask that you speak clearly so that the court reporter can transcribe your information correctly. Starting to my left.

MR. TOFT: David Toft, director, IT Security.

MR. DIEHL: Robert Diehl.

MR. GREENSTEIN: Ira Greenstein.

MR. MONTANYE: Tom Montanye.

MR. HAYNES: John Haynes, Procurement Specialist.

MS. GORDON: And we start with you, sir.

MR. LA FAVOR: Al La Favor, Arch Systems.

MR. MERRILL: Edward Merrill, Edwards Performance Solutions.

MR. PICKETT: Dana Pickett, Edwards Performance Solutions.

MR. EISEN: Ellis Eisen, Netorian.

MR. CHURCHILL: Aaron Churchill, Netorian.

MR. NELSON: Brian Nelson, Anchor

Technologies.

MR. PETERSON: Scott Peterson, DK Consulting.

MR. HUGHES: Micheal Hughes, Oakland Consulting Group.

MR. MOLONY: Sean Molony, Valsatech.

MR. FERNANDEZ: Jose Fernandez, Compsec Direct.

MS. BOYKIN: Ashley Boykin, SeRigor, MBE/SBR.

MR. SORRELL: David Sorrell, Companion Data Services.

MR. SURGUY: Scott Surguy, SCD Information Technology.

MR. ZAKARI: Mohammed Zakari, Grant Thornton.

MS. GORDON: I'd like to next cover the important aspects of what this TORFP represents. I will ask that you hold all questions until the panel has covered all the information that you need. Then

we will hopefully answer those questions that you may have after the conference is concluded. First we'll go over the general information.

And the SRA is issuing this TORFP to obtain a master contractor to analyze and test the resiliency of the Agency's external internet facing information systems and three web enabled applications against external threats and attacks in accordance with the scope of work described in section two. In addition, the master contractor selected for contract award shall provide the Agency with a written report presenting the details, analysis and findings that support each conclusion and recommended action, and shall provide a briefing or briefings of findings and recommendations to select Agency personnel. Both the written and oral reports, and the contents thereof, shall remain confidential and shall not be disclosed to any third party without the express written consent of the task order manager.

On page two of this TORFP is the key

information summary sheet. I've made copies near the sign-in sheet in case you do not have yours with you. This sheet summarizes all of the important dates for this TORFP. It lists the contact information of the task order manager, David Toft, and myself as the task order procurement officer. This TORFP has an MBE goal of 30 percent with no subgoals and no VSBE goals.

The contract resulting from this solicitation shall be a firm fixed price. All proposals in the form set forth in section 4.2 must be received by myself, at the email address listed on the key information summary sheet, no later than 2:00 p.m., local time on April 5 in order to be considered. Nothing even a second after 2:00 deadline will be accepted. Request for extension of this time or date will not be granted, as this is the third time this has gone out. If an offeror prefers to mail in their proposals, they should allow sufficient mail delivery time to ensure timely receipt by myself. Proposals received after the due date and time listed in this

section will not be considered. Proposals may not be submitted by fax. The proposals will not be opened publicly.

All questions shall identify in the subject line the solicitation number and title, and shall be submitted in writing, via email, to my attention, no later than the date and time specified on the key information summary sheet, which is March 28, 2:00 p.m. Answers to all questions that are not clearly specific only to the requestor will be provided to all master contractors who are known to have received a copy of the TORFP. The statements and interpretations contained in response to any questions, whether responded to verbally or in writing, are not binding on the Agency unless it issues an amendment in writing. We will then turn it over to Mr. Toft for the minimum qualifications in section one.

MR. TOFT: Thank you, Margie. And thank you everyone that's joined us here today here at Baltimore Headquarters, and also those that have come

in through the conference call. And also welcome you on the first day of Spring. How about that.

MS. GORDON: Six o'clock.

MR. TOFT: Well, we're close. Let's go ahead and talk about minimum requirements here. First of all, we ask that you bring with your team someone that has at least a CISSP or a CEH, certified ethical hacker certification. The second qualification is that who you bring on board, and these all are pertaining to all. One individual must have these requirements. One of them is that they've had at least two risk assessments of web applications in the past, at least two performed within the past three years. And secondly, of those applications they should be of a .NET frame work, designed under .NET. And also, that these applications should have had people authenticated to the internet through a secure channel to these web applications. Lastly, we also, of course a team member must have penetration testing experience, experience with conducting non-intrusive

penetration tests.

Let's go down to the scope of work, which is on page two. Basically, there are four major blocks or chunks to this work order, the scope. One being the penetration test, which is testing our systems located in the DMZ. The second piece is the web applications. It would be testing of the web applications that are hosted in the DMZ. The third piece is the WiFi, our wireless network here in Baltimore, here in this building. Also, there is an optional work facet of this work, and that is actually it's a misnomer because it's pretty much guaranteed that that will be included in this work order. It's the optional work. I just want to read here, right off the form here, the task order contractor is to perform all services and produce all deliverables requested in this TORFP and expects the proposed key personnel to be available as of the start date specified in the Notice to Proceed. For the purposes of protecting efficiency and limitation of risk exposure, the task

order contractor shall propose the minimum number of persons necessary to satisfactorily perform the services requested in this TORFP. And Ira Greenstein, our chief security officer, he made a comment back in July --

MR. GREENSTEIN: Chief information systems officer.

MR. TOFT: The CIO. Although CIO in this organization means chief investment officer, which is how we make that distinction. As Ira said, back when we did this same conference, back in July of '18, he made a comment, and it's probably valid that we make it again. And that is, we're not a big organization. This is not a huge amount of work that we're asking people to perform. And the reason why we bring that up is that in the past we've seen some vendors, you know, just totally go all out and put a proposal together that's, you know, red teams, and the bells and whistles you could possibly throw at an organization. This is not what we are. We are

located right here, in this building, with a DR site in Annapolis. If you read over the proposal, the footprint is very small. It's not huge. So consider that when you're putting your proposal together.

I'm going to go down to testing specifics on page four. And that is that the penetration testing performed by the task order contractor shall be of a non-intrusive, passive nature to ensure that no agency production systems are impacted during this project. No production system down time attributed to the PEN test is acceptable. So we are dealing with production systems here. Of course it will be off hours, but still, you're dealing with live production systems and consider that in your approach to this. We don't want any down time, obviously. No production down time.

Security types. So I want to add to that, to the penetration testing. And that is, there is a facet of this that we deem very important. That is on page four, the application testing, item "A," is a code review. We're requesting a code review to be

done on these web applications. We found in the past, this will be the fourth time we've gone through this exercise, and we've found that code testing, static code analysis has brought a lot of things to the table for us. It's been a big benefit for us, and we've gleaned a lot of helpful and meaningful things. They've found things that we would have never found unless there had been a code review. So think about that. We'll be looking at that specifically in the proposals, how well you put together that piece of this.

Now I'm going to talk about deliverables, and that is from page six through page 10. Basically what we're looking at here is to put together, you will put together a project schedule, you would accumulate your results and your findings, put together your analysis of those findings, and then make recommendations with those findings. Now, let's see, at page 10 talks about the future optional work. And that is this. Right now Tom, who is our director

of systems development, his team is working to put together a member portal that will be going live, projected in September of this year. And this web portal is something we haven't done before. We're basically opening up our data to the outside, allowing our members, retirees, active members, beneficiaries to log in and actually do something with their data. That's where we're at, and it's, obviously it exposes a larger footprint than we currently have. And this application has to be secure when it goes live. And so that is kind of the core of what this optional work is, is testing that application code analysis. It also, this application uses O-pen ID connect, OAUTH, and uses ID proofing, ID management on the internet. So there's a lot of moving pieces with this application and it's critical to us that it's secure. And I just want to add a caveat here. And that is the scope of testing will be identical to that of the three applications already mentioned in section 2.1.22. So your approach to this optional work will

basically follow the same methodology that you've already put in place with the other applications. I just want to kind of put that out there.

Next, on page 15, talking about the security requirements, page 15, section 3.7. And that says, unless specifically authorized in writing to the TO procurement officer and the TO manager, the TO contractor shall not reference, discuss or disclose information related to this TORFP with a limited exception for information that has been directly and intentionally released to the general public by the Agency. The task order contractor shall not reference or disclose work performed or conducted pursuant to this TORFP in any communication that is not specifically and directly related to the services and deliverables required by this TORFP, which shall preclude the disclosure of any such information or materials to other State agencies or the departments. So that's kind of self explanatory right there.

Moving down to talk about security

clearances and the criminal background checks on page 15. The TO contractor shall obtain all, from all contractor personnel assigned to work on the task order, a signed statement permitting a background check. Prior to commencement of work the TO contractor shall secure, at its own expense, a national criminal history record check. This check may be performed by a public or private entity. At a minimum the background check must include all convictions and probation before judgment dispositions. The task order contractor may not assign an individual whose background check reflects any criminal activity to work under this task order unless prior written approval is obtained from the task order contract manager. And also, to follow up with that, in appendix three, on page 73, there is a criminal background check affidavit that will be signed and sent to us prior to any work is done.

Moving along to information technology on page 16, section 3.74. The task order contractor

shall implement administrative, physical and technical safeguards to protect State data that are no less rigorous than accepted industry best practices for information security. Basically, what that means is that all the data you accumulate, all the artifacts, any source code that we upload to your systems has to be secured. You have to ensure that that data is not exposed. Any confidentiality, integrity, risk, any kind of security, whatever can happen is done, it's secured and it's maintained, and it's protected.

Now I'm going to talk about substitution of personnel, page 22. Basically there are three sections here. And this is directed personnel replacement substitution prior to and 30 days after task order execution, and substitution greater than 30 days after execution. As we said in the last proposal we had, we have never had to invoke any of these safeguards. The personnel that are our contractors have brought to us have been all competent people. We never had a situation where we've had to jump in and

say we have a problem here, and we have to make a change. Thankfully, we haven't been able to do that. We've been fortunate. We've had good people that have worked for us. And we expect the same for this task order. And I think we said the last time, we are easy to get along with. We don't always grin. Those three guys grin. I don't. But we're easy to get along with.

Jump to page 32 real quick. The offeror shall propose up to four key personnel in response to this task order RFP. And that word "shall" is State language. You can propose less than key, less than four key personnel. But we want you to provide the number of people that will do the job. And the key word there is key, the key personnel. We don't relish the fact of reading over resumes of non-key personnel because they can be swapped out, can be substituted. So we're kind of focusing on that. And that will be important to us. And only propose individuals who you believe will be available for this engagement.

Moving along, I'm almost done here. Page 36, on evaluation criteria, it reads like this: The state prefers an offeror's response to work requirements in the task order RFP that illustrates a comprehensive understanding of work requirements and mastery of the subject matter, including an explanation of how the work will be performed. The quality and accuracy of the task order proposal will be considered as one component of the offeror's understanding of work requirements. So basically, what we're saying here is your proposal quality is important. Ira, he's a stickler for grammar, for logic, and he has taught us well, that what you put on that proposal is reflective of pretty much the work you're going to do for us. The comment made is this, we consider the proposal quality to be indicative of the deliverable quality. We have seen some come by and, wow, really it's serious, it really is, how well you craft a proposal and put this together so that we want to keep reading it.

On page 43, I'm going to talk about pricing proposal. The pricing is very simple. Here, on this sheet, is the fixed price sheet, 44. It's comprised of two stages, the penetration test and the WiFi is the first stage. That's one price. And then table ID number, IDs number, well, 2.4.4.4 and 2.4.4.5, which is the web application testing, that is the other stage of the price table there.

And I just want to go over one more thing. And Margie got me the last time on this, and I kind of brushed her off, so I'm not going to do that this time. I'm going to make her nice and happy. We're going to talk about oral presentations. That is on page 27, and that is the offerors and proposed task order contractor personnel will be required to make an oral presentation with our team here at MSRA. All proposed key personnel must actively participate in the oral presentation, responding to at least one question posed in advance by the agency and responding as appropriate to further questions posed during the

oral presentation itself. That is the last thing that I have.

MS. GORDON: I am going to basically talk to you about the submissions and the MBE, your MBE submission, your paperwork. As I had stated, some people had asked me why we canceled the last TORFP. And the reason was that we had to make some clarifications in the TORFP of which most of it was towards the MBE documentation. What we did was to attachment "D," we made you go into the website of GOSBA. It used to be called GOMA. On page 46, in attachment "D," it specifically says all required MBE forms are located at this site. And it has a URL that you will click on. It will take you to GOSBA's site. You will see all the forms there. And refer to table one in section seven of which forms must be included with your technical proposal. And let me say this, for assistance with these forms, on how to fill them out, please go to the URL that's listed on here, where it says goma.maryland.gov, pages reporting tool, MBE.

This is a self help of sample MBE forms. I can't express how important those forms D1, 2 or whatever, the ones that go to section seven. MBE forms D-1A, that is to be included with your task order proposal. And I'm begging you, please, if you think you know how to fill it out, just go to that sample first and just get a little brush up help, self help, because there are no cures on MBE paperwork. If you mess up, if you don't put an "X" in there, in a box, or if you put it in a wrong spot, you're out. I cannot make it good. Just letting you know. No MBE paperwork can be cured. They are working in legislation to change that, but we don't have it yet.

MR. GREENSTEIN: It's a subtle hint.

MS. GORDON: So other than that, I mean, that's the first thing. When I receive your technical, I go through your paperwork. And it was surprising. But just make sure that everything is I's dotted, T's crossed, boxes crossed, directions, whatever, just go in there and look on the GOSBA site

and get some help and see how they correctly fill out the forms. Don't call me because I can't help you, other than here. That's it. Other than that, task order proposal format submission, please read over those carefully.

All task order proposal emails shall be sent with password protection separately, technicals, password; financials, password. Separate emails. Also, in your technical proposals I need format of Word format, your technicals in Word format, in pdf format, and if you are redacting anything on your technical I need that. So there are three documents that I should have, other than your attachments, your MBE stuff. Once I get those, you know, I said they're all password protected, once I receive everything on April 5, then I will send an email to you to ask you for your technical password only. Do not send me your financial one until I send you an email for it. And please make sure you send me your password protected or else you will get, you could possibly get thrown

out at that point too.

So we, SRA strongly desires all submissions in email format. If an offeror wishes to deliver a hard copy, please contact me for your instructions.

The task order process will make a determination recommending awarding of the task order to the responsible offeror who has the TO proposal determined to be the most advantageous to the State, considering price and the evaluation criteria set forth above. In making this selection the task order technical proposal will be given greater weight than the task order financial proposal. That is stated in section 6.4F. As I said, there are attachments in this TORFP that shall be submitted at the time of your proposal. So we ask you to take time to review those attachments and submit those at the time they need to be submitted. And pay attention to those that need to be submitted if you are awarded the contract. And I have some questions and answers that some vendors have sent me. I will state them. And then if you have any

further questions, you can ask them after this.

Is it required to have the onsite personnel to perform PEN testing or can it be done from offsite location? Answer: Only WiFi testing requires personnel onsite. Question two: Can the work be done during off hours from offsite location? Yes. Question three: What level of clearance is required for the personnel? As defined in the TORFP, personnel must pass a security background check. Refer to section 3.7.2, security clearance/criminal background checks. For the following referenced procurement will the State allow the experience of a named subcontractor on the proposed team to be substituted for master contractor experience? The master contractor must fulfill the TORFP experience requirements that are stated in section 3.9.2, offeror experience, on page 21. I will make one statement. The master contractor must demonstrate in its task order proposal that it has previously performed PEN testing and security vulnerability assessments on all

of, one, internet-facing systems; two, network perimeter security devices and equipment; internal WLAN devices, including wireless access points; and hardware devices to include all of, but not limited to, firewalls, routers, Windows-based servers, and comparable network infrastructure devices. Question five: PEN test in 2.1.2.1 and application test in 2.1.2.2: Are all systems hosted in the two internet facing compartments? Answer: Yes. PEN, Baltimore and DR/Application testing is Baltimore only. Wireless testing in 2.1.2.3: How many SSIDs are included in the testing and how many IP addresses across the 8VLANs? There are two SSIDs and 8/16 networks. Application assessment in 2.1.2.2: Three applications are listed, but four URLs are referenced; what is the purpose of the fourth URL? That is the public website URL. For the three applications in 2.1.2.2, please provide a description of their complexity. Low to moderate complexity, mostly are SPA, which is single page application, designs.

Applications in 2.1.2.2: Which application/URLs require credentialed scanning? Two, file upload and employer payroll reporting. Question 10: For the applications requiring credentialed scanning, how many user roles should be included in the testing? Answer: One to two roles. Question 11. PEN test in section 2.1.2.1 and application testing in 2.1.2.2: Can testing be performed remotely or will testers be required to be onsite? Answer: Remotely. Application assessments in section 2.1.2.2 with code review: What languages and how many lines of code are to be reviewed for each application? Answer: All apps developed on the Microsoft platform, .NET, C#.net, VB.net, Angular with Typescript. Employer payroll: approximately 5,150 lines; secure reprints: approximately 1,100 lines; file upload: approximately 1,300 lines. Background check in 3.7.2. Can an active SECRET or Top-Secret clearance be substituted in place of the criminal background check? Yes. Will any testing be done in a non-production environment?

No.

That's all the questions I have. Now, the floor is open for questions. Anybody?

MR. NELSON: For the code review, can that be done with automated tools and are you expecting manual code review?

MS. GORDON: Can you state your name and --

MR. NELSON: Brian Nelson with Anchor Technologies.

MR. TOFT: Either one. In the past we've seen people use both. It's no preference. Either one. Or both.

MR. CHURCHILL: Aaron Churchill with Netorian. Two questions real quick. At the beginning you stated the solicitation number as G20P94.

MS. GORDON: "B."

MR. CHURCHILL: "B." That's what it says here. I thought I heard "P," so just checking. Second question. In your questions and answers, as you were reading them, about the master contractor

past performance, did you state that subcontractor past performance was allowed or was not allowed? That would be pertaining to section 3.9.2.

MS. GORDON: So the master contractor must fulfill the TORFP experience requirements in 3.9.2. It just says basically, it says the following experience is expected and will be evaluated as part of the task order technical proposal. See the offeror experience capability and references evaluation factor from section 6.2. The task order contractor shall have successfully completed at least two PEN tests within the last three years. And the master contractor must demonstrate in its TO proposal that it has previously performed PEN testing and security vulnerability assessments on all of the four items. I didn't say anything about subcontracting.

MR. CHURCHILL: There was one question about subcontracting.

MR. TOFT: That was in the questions that she's already been asked and she provided answers to.

MR. CHURCHILL: Yeah. I think it was like the second or third question.

MS. GORDON: For the following referenced procurement will the State allow the experience of a named subcontractor? We basically said that as long as you can fulfill the TORFP experience requirements that are in section 3.9.2.

MR. CHURCHILL: Okay. Cool. I was just making sure. That's what I thought I heard.

MR. GREENSTEIN: The primary focus has been on the people doing the work more than the organization itself. That's been the case from the get go on this. It's not that the organization is irrelevant; it is relevant. But we are far more focused on the people who are going to do the work. Is that a fair statement?

MR. TOFT: Yes.

MR. HUGHES: So you will allow the subcontractor's past performance flow through to the master contractor submitting the bid?

MR. GREENSTEIN: I mean, I think it is a factor. But again, it is not the -- if you look very specifically in here, and I'm not the person who is supposed to be answering this. But if you look at it--

MR. TOFT: I can answer it. We've already said that the key personnel are what we're looking for because anything outside of key personnel can be swapped out, be replaced. So our focus is really on the key personnel. We've seen many proposals with subcontractors with sterling backgrounds. But are they going to be the ones doing the work? That's the key part here.

MS. GORDON: Remember key personnel must be all the way through this technical proposal, as it says in the substitution area. It was specified in section 3.10. There are no ifs, ands, or buts as far as replacements of them unless there is some type of death in the family or something of that nature, unfortunate. If someone is going out of the country,

we don't accept that. If somebody has another commitment, we don't accept that. So just remember, your key personnel is just that, they must be available throughout the whole TORFP and 30 days afterwards.

MR. FERNANDEZ: What if they quit?

MS. GORDON: That's not our problem. That would be yours. And that would be that you were out.

MR. GREENSTEIN: And that's State language. That's not necessarily something we've imposed here. I mean, I'd refer you to section 6.2, evaluation criteria. Just look at the order of those criteria. It starts off with the experience of proposed staff, then it goes into meeting the requirements of the TORFP. And that's where our priorities are. If you look at the minimum qualifications, there is no section for minimum qualification of the offeror, just the offeror personnel minimum qualifications. That's pretty much reflective of the focus that we have. It's not that we won't consider other criteria, but if you look at the priority order, I think we've been

fairly clear.

MR. PICKETT: Dana Picket, Edwards Performance Solutions. This is a question for you, David. Early on you said that what was listed as optional work is no longer optional work. I assume referring to the web portal rolling out later on this year with the State retirement information, correct? I can only say having worn a CISO hat for four major companies for the last 32 years before joining Edwards, that could be the single point of failure. It's great to hear that you're rolling that into the scope of work requirement.

MR. GREENSTEIN: Let me address that one if I could. The timing of this, as you are aware, this is the third release of this RFP. When it was first released, the time that that application was going to be ready was anticipated to be after the initial work was complete. Given the cancellation and reissue of these things, the time has now caught up to us. The future is here. But we also didn't want to change the wording because it makes it a whole lot easier to

review the exact same document when it goes back a second time, in this case, unfortunately, a third time.

MR. SORRELL: David Sorrell, Companion Data Services. Just as clarification, as third issuance of the RFP, it sounds like really it came down to the MBE percentages or the MBE forms that kind of were hanging everything up. You were ready to go to award but maybe couldn't?

MS. GORDON: Can't answer that one.

MR. GREENSTEIN: The first cancellation I think came down to a conflict between two clauses in the State's template that was pointed out and were not reconcilable. And so we had to pull it back and fix the language that the State gave us. The second time, read between the lines.

MS. GORDON: The conference call person has a question.

MR. VARMA: This is Anil Varma from Navitas. So are they required to meet the (indiscernible) on a continuous basis or they would be a spike of the work

and then you wait for the other work to come through?

MR. GREENSTEIN: It's likely to be on a continuous basis at this point in time. That was not the case when we first issued this.

MS. KEARNY: Jeannette with Janus Associates. Please forgive me if I asked a question that was posed already because my call dropped and I had to dial back in. One of my questions is: Will you be posting or releasing the questions and answers that you read and that have been asked on the conference call?

MS. GORDON: Yes, they will be in the minutes.

MS. KEARNY: And my second question is the pricing forms. We have stage one and stage two. Are we to give pricing for the optional work?

MR. GREENSTEIN: No. That will be worked out after the award because that's the way it was originally set.

MS. KEARNY: If we prime this and bring in a sub is the sub allowed to prime also?

MS. GORDON: As long as they can fulfill the TORFP experience requirements to my --

MS. KEARNEY: So they are allowed to both prime and sub?

MS. GORDON: In section 3.9.2 I think we went to the point that as long as they are able to fulfill the experience and they have, they follow the min quals.

MS. KEARNY: Margie, when you first started this meeting you referred to TORFP number as G20P, as in Paul. Are you changing that because --

MS. GORDON: "B," as in boy. And also, Jeannette, in the personnel that you were referring to as subcontractors, as long as they are noted as key personnel. They must be able to stay within the TORFP lines of key personnel substitution. They have to be able to be your key personnel throughout this TORFP, for 30 days before and 30 days after.

MS. KEARNY: Okay. Great. Thank you.

MR. FERNANDEZ: Jose Fernandez, Compsec Direct. I have a few questions. Let me start with

the software ones first. So there was an insurance requirement for approximately five million dollars in bridge insurance, correct?

MS. GORDON: Uh-huh.

MR. FERNANDEZ: So since the applications are integrating with these third party identity providers and those are out of scope, would the State be opposed to underwriting in that insurance document that states, say, if the failure is the result of the third party identity providers, then -- that kind of language.

MS. GORDON: No. I don't think the State would take that liability.

MR. FERNANDEZ: Right. So noninvasive penetration testings are about as equal as friendly military occupations. The State did mention that the source code for these application is subject to the static review, correct?

MR. TOFT: Yes.

MR. FERNANDEZ: And we would also be able to do dynamic testing on a non-production system. We

already have the source code, like one of the questions that was posed earlier was taking, because it's on a non-production system, and the answer was no. So we can do static testing, but not dynamic testing in an enclave network; is that correct?

MR. TOFT: We're talking about the code analysis. As far as the code analysis goes, static or non-dynamic.

MR. FERNANDEZ: Right. To do dynamic testing we would have to recreate that application in an enclave network and then test it as much as we could.

MR. TOFT: Right. You'll have source code. You'll have the code. In the past we have seen very little dynamic testing. Mostly dynamic testing is something that's already past the development stage. More of the work we've seen has been done static, static analysis. As far as the comment about nonintrusive penetration testing, we've seen good results from this angle. It may seem like, I don't know bizarre to have someone come in and do a

penetration test and not be intrusive. But it's like, I guess the analogy is, you can take a picture of a criminal with a bank vault open versus, you know, that's the way we look at it.

MR. FERNANDEZ: And then so I have some questions regarding the WiFi assessment. Would we be able to de-authenticate users that are currently connected to SSIDs?

MR. TOFT: This will probably be done after hours. We probably, most definitely don't want you in here doing WiFi testing during work hours. That would be done after hours. So at that point there will be nobody on the WiFi.

MR. FERNANDEZ: So would we be provided credentials to connect to the WiFi or do we just have to literally just come in --

MR. TOFT: Yeah. We won't be giving credentials for the WiFi.

MR. FERNANDEZ: So I guess no tampering with the users. So that also means we don't have to concern ourselves about users that bring their own

devices and connect into the State network. So I think you just answered that question.

MR. GREENSTEIN: We have a guest WiFi, --

MR. FERNANDEZ: I saw it.

MR. GREENSTEIN: -- which is different from our regular internal WiFi.

MR. FERNANDEZ: Which one are you more concerned about?

MR. GREENSTEIN: Internal.

MR. FERNANDEZ: Roger.

MR. GREENSTEIN: The guest WiFi is segregated off. We have people who come in for Board meetings, other things, who are sitting in this room, who are not part of the agency, and we allow them access while they are here. Where we don't route that through our production networks. We route that separately.

MR. TOFT: Correct. Yeah. The WiFi is strictly a service that we provide. It's not, like Ira said, it's not tied into our business systems.

MR. GREENSTEIN: But we do have WiFi that

is. And that's what we --

MR. FERNANDEZ: That's the one I would care about too. Thank you guys.

MS. GORDON: Any other questions?

(No response.)

MS. GORDON: Okay. On behalf of the Maryland State Retirement Agency, we would like to thank you all for your interest in doing business with the State of Maryland. A copy of this transcript of the conference and a list of the attendees, with business cards, which that list only includes yourself and any questions and responses that were covered today, as well as any additional questions that you may have, any amendments to the TORFP will be emailed to all offerors. Also, keep in mind the closing date and time for the receipt of the proposals is April 5 at 2:00 p.m. This will conclude the task order pre-proposal conference, and we wish you a happy day.

(Whereupon, at 3:00 p.m., the meeting was adjourned.)

CERTIFICATE OF NOTARY

I, KATHLEEN A. COYLE, Notary Public, before whom the foregoing testimony was taken, do hereby certify that the witness was duly sworn by me; that said testimony is a true record of the testimony given by said witness; that I am neither counsel for, related to, nor employed by any of the parties to this action, nor financially or otherwise interested in the outcome of the action; and that the testimony was reduced to typewriting by me or under my direction.

This certification is expressly withdrawn upon the disassembly or photocopying of the foregoing transcript, including exhibits, unless disassembly or photocopying is done under the auspices of Hunt Reporting Company, and the signature and original seal is attached thereto.

_____

KATHLEEN A. COYLE
Notary Public in and for
the State of Maryland

My Commission Expires:

April 30, 2022