Security and Penetration Testing D80B5400025 (SVPT)

Questions From Pre Bid Conference

Question 1, Page 6 & 7
MR. GONZALEZ:
Once we get our questions over to you tomorrow, what's the time line for getting it back to us so that we can put our response on a final report?

Answer:
MR. SPENCE:
We're going to get them back as soon as possible.

Question 2, Page 8
MR. GONZALEZ:
So is the volume of questions or the amount of time it's going to take to get -- answer those questions, going to impact the final date? The 31st is the date today right now. Is that -- would that push that back?

Answer:
MR. SPENCE:
If we feel like we need an extension, then we will extend it.

Revised Answer:
Please see the amended TORFP. MIA has extended the closing date until 03/17/2017.

Question 3, Page 8, 9
MR. TRUMP:
The question I have is, we deliver a host of services and one of the things I noted that we've seen a lot of other agencies look for is incident response. And I was wondering if it's -- if it's too late to provide an optional service such as incident response program review, retain incident response services for instance to supplement the MIA's security program That's one of the questions I have.

It wasn't requested as one of the items in the technical scope. So we were wondering if -- if it's possible to add an optional scope to this at this time, If it's not, then understood. But we did want to ask that question.

Answer:
MR. SPENCE:

That's something we're going to research and get back to you on.

Revised Answer: Section 2.15 of the SVPT solicitation titled "SECURITY REQUIREMENTS AND INCIDENT RESPONSE," defines the incident response requirements for this solicitation. MIA does not intend to amend that section.

Question 4, Page 10
MR. MAMMO:
You have required us to have three personnel performing this project. But you have not specified which positions. In the CATS+ contract, there are positions under the contract. And usually when they run down RFPs, they will choose what the category, meaning which positions for that level categorization for this -- this RFP. So my question is can you tell us what those three positions are or is it open for us?

The job categories are – are fixed. There is a list of job positions under CATS+. So when you are -- are asking us to submit personnel, it has to be from that -- one of those listings.

Answer:
MR. SPENCE:
I'll have to take a look at what you're talking about. Please submit that in writing and we'll answer your questions.

Revised Answer: Contractor responsibilities including, KEY Personnel requirements are defined in section 2 of the solicitation. Offerors may propose job descriptions for KEY Personnel. Those job descriptions do not have to correspond with job descriptions under the CATS Plus master contract.

Question 5, Page 11
MR. MAMMO:
How does that impact -- how soon you can respond back when the project is due? Like if you do not respond by let's say January 30th and the project is due the next day, that means we didn't have enough time to send our responses. So can you give us at least one week working -- after you give the responses?

Answer:
MR. SPENCE:
We're going to do our best to get the answers to the questions out as quickly as possible. If we feel like we need to put an extension, then we will give you a reasonable amount of time to respond.

Revised Answer:
Please see the amended TORFP. MIA has extended the closing date until 03/17/2017.

Question 6, Page 12
MR. BROWN:
The level of -- one of the requirements has a level of detail for a scan. And it wants us to look at potential compromised systems. Are you expecting a forensic analysis or a very high level scale of IP addresses and those external locations that are probably coming into your environment that you weren't aware of?

Answer:
MR. COBURN: Not a forensics analysis.
MR. BROWN: So not a deep dive?
Answer:
MR. COBURN: No

Question 7, Page 13, 14
MR. BROWN:
There's a certification in there that you're requiring from some of the individuals.
MS. ESLIN: The IAM Certification
MR. BROWN: Yeah. Is that a hard stop if they do or don't have that certification for individual firms?
MR. TRUMP: Same question, same concern.

Answer:
MR. SPENCE:
If we were to change that, it would require like some sort of amendment. So I could say for now, it's a hard stop. If it's in the solicitation, then that's what we're asking.

Revised Answer: Please see the amended TORFP. The InfoSec Assessment Methodology (IAM) Certification and the Cisco Master Security Specialized Partner Certification are now preferred qualifications.

Question 8, page 15
MR. TRUMP:
Is all the work to be conducted in one facility or is there multiple MIA facilities in your --

Answer:
MR. COBURN:
One facility.

Question 9, Page 15, 16
MR. TRUMP:
And then to clarify, the three requirements -- the external testing, internal testing, PEN testing -- so there's a few ways we could bucketize [sic] this research. One, for instance, would be full vulnerability scan and so forth without invasive action on the external and internal providing all of the theoretical holes that are there with mitigation recommendations.

And then secondly, using the PEN test for actually -- an -- attack attempts. Otherwise, we could do an internal/external PEN test with full capability, which would omit the need for another PEN test following. So we're anticipating to provide a response to vulnerability scans and non-invasive testing for the internal/external with full reporting and then do the attack testing internally using the PEN test binary.

Answer:
MR. COBURN:
I would submit a question on that.

Question 10, Page 16
MR. BROWN:
Is this the first time you've done this level of testing or has it been done in the past by another vendor?

Answer:
MR. COBURN:
We've had a light testing done by DOIT. They offered a free web assessment vulnerability test.
MR. BROWN: But not a scaling test like this?
MR. COBURN: No. This is the most intensive test we've had to date.

Question11, Page 17
MR. BROWN:

MR. COBURN:
I don't want to guess. I think it's a continued in the future, I believe but I, you know -- submit that question and we'll respond.

Question 12, Page 17
MR. MAMMO:
And finally, when do you expect to start this project?

Answer:
MR. SPENCE:
As soon as possible.

Question 13, Page 17
MR. GONZALEZ:
We saw the certifications changed with the last solicitation. You know, what was the emphasis around that? Was that -- again, is that a hard stop or, you know, just questioning regarding that as far as -- again it's not a certification. It's not,

MR. COBURN: Which certification are you talking about?

MR. MAMMO: The SSCP.
MR. GONZALEZ: The SSCP --
MR. MAMMO: That was added after the last revision on January 1st.

Answer:
MR. COBURN:
Submit a question on that and we will get some clarifications. I believe all the minimum requirements are going to be required for this test.

MR. SPENCE: The minimum requirements aren't going to change.

Revised Answer: Please see the amended TORFP. The InfoSec Assessment Methodology (IAM) Certification and the Cisco Master Security Specialized Partner Certification are now preferred qualifications.

Questions From Email

1. Will InfoSec Assessment Methodology (IAM) Certification be required and can exception be granted if this not currently available?
   Please see the amended TORFP. The InfoSec Assessment Methodology (IAM) Certification and the Cisco Master Security Specialized Partner Certification are now preferred qualifications.

2. What is the budget expectation for this work effort for the base year and then optional years?
   The Budget approved for this service is $30,000.00

3. Who is the current provider of these services?
   No current provider.

4. How many document reviews and interviews will be expected for each of the specific requirements in section 2.6 (A, B, C, D, E, and K)?
   The State'sDepartment of Information Technology (DoIT) Security Policy and the MIA's Security Policy are the only internal document we expect to be reviewed. The number of interviews would be determined by the vendor.

5. How many scans per year are expected for each of the requirements in section 2.6?
   We expect that all scanning in the scope of the TORFP as defined in Section 2.8.4 would be done once during the contract year.
6. Please clarify the scope and details expected for requirement D in section 2.6, is this a detailed forensic review or a simple scan of which devices are communicating with unknown internet traffic?
   Simple scan.

7. Are there any specific threats you are concerned about?
   No.

8. Is there any specific private information stored or transmit that you are particularly concerned about?
   PII and PHI data.

9. Have there been any past information security incidents we should take into consideration while performing our testing?
   No.

10. How many users do you have? How many IT Staff? Are they in-house or outsourced?
    MIA has approx 300 internal users and 16 in-house IT staff.

11. Are there remote access capabilities for your network (such as a VPN or remote desktop software like RDP, LogMeIn, GoToMyPC, etc.)?
    Yes, VPN and Terminal Services.

12. How many Internet/public facing servers do you have (physical and virtual)? How many public IP addresses?

    One physical and three virtual servers and thirty public IP addresses – 167.102.134.128/27.

13. How many physical offices/locations do you have?
    One physical office building and one physical remote location.

14. How many internal servers do you have (physical and virtual)?
    Approx thirty servers will be in scope for security penetration testing.

15. How many network devices by type (i.e. firewalls, routers, switches, load balancers, etc.) are in scope? Do you want them assessed only from the perspective of an attacker, or will you also provide configuration files for review of configuration?
One firewall, one WAF, one router and one DMZ switch are in scope. Assessment should be from the perspective of an attacker.

16. How many (estimated) internal hosts do you have?
Thirteen VMware ESXi hosts.

17. Are your servers self-hosted or hosted elsewhere?
Self hosted.
18. How many IP addresses are in scope (internal and external)?
10.120.240.0/24 and 172.30.0.0/21 are internal IP addresses and 167.102.134.128/27 are external.

19. Are all of the in-scope systems available from a single network segment?
In separate VLAN's

20. Is port security or NAC controls present in the environment that would interfere with the presence of unmanaged systems?
No.

21. Do you self-host your email or use a hosting provider?
MIA uses the State of Maryland's Google Apps environment for email.

22. Do you self-host your website or use a hosting provider?
The MIA web site is hosted by the State of Maryland's Department of IT (DoIT).

23. Do you want a vulnerability assessment or full penetration test for the website and web applications? Will the applications be tested with and without credentials? If so, how many different user roles/sets of credentials will be tested for each application?
MIA website and web applications are not in scope for security penetration testing.

24. Are any email contact forms or forms present that may generate tickets or emails if posted to? (*Automated web application vulnerability scanners will be used during the assessment that send a multitude of posts to web forms. As a result of this scanning thousands of emails, alerts and tickets may be generated*).
MIA website and web applications are not in scope for security penetration testing.

25. Will the network be stable during the test, no changes?
Yes.

26. If vulnerability is discovered on a desktop, server or network device, does ePlus have permission to trigger the vulnerability with an exploit?
Not without advance approval.

27. If a system is compromised, does EPlus have permission to execute post exploitation commands to recover passwords, search memory and recover document and folders?
Not without advance approval.

28. If a system is compromised, does EPlus have permission to use that system as a pivot point for further network attacks?
Yes.

29. If access to a privileged account is gained, does EPlus have permission to access the Domain Controller?
Not without advance approval.

30. If access to a privileged account is gained, does EPlus have permission to access the mail servers?
Yes.

31. If access to a privileged account is gained, does EPlus have permission to access the database servers?
Not without advance approval.

32. If Domain Controller access is gained, does EPlus have permission to create accounts?
Not without advance approval.

33. If Domain Controller access is gained, does EPlus have permission to recover the password hashes?
Not without advance approval.

34. Do you wish to include Arp poisoning attacks in the penetration test?
No.

35. What types of social engineering testing do you require? (i.e. email phishing, phone phishing, onsite breach of physical security, etc.) If phishing is required, how many users will be targeted for each type of phishing, and how many separate attempts should be made for each user? Can phishing be performed in conjunction with our other testing (in which case, information obtained will be used in other testing areas), or must it be a separate and distinct test? If breaches of physical security are to be attempted, what are the locations to be tested?
    - Which physical locations are in scope for the Wireless Assessment? How many SSIDs and APs at each location will be in scope?
    - Are there any time limits for how long the exercises are to be conducted?
    - Are there any additional notes, concerns, or parameters that need to be considered that you would like to highlight?

Social engineering and wireless testing are not in scope.

36. General Information
    a. What is the primary driver for having a penetration test performed?

See section 2.2.2. of the TORFP.

b. If the penetration test driver is for regulatory compliance, which specific requirement(s) applies?

The driver is not for regulatory compliance.

c. Have you had penetration tests performed in the past? If so, when was the most recent one performed?

Yes, DoIT conducted penetration tests on the MIA's web applications in 2015.

d. Is the plan to have penetration test performed on a recurring basis or as needed? If recurring, how often?

As needed.

e. What are your currently installed security tools / suites?

IBM Q-Radar.

f. Have you conducted a Cyber Security Data Management Analytics? Do you want us to look into that?

No to both questions.

37. Application or Infrastructure

g. Is testing to be completed at an application level or infrastructure level or both?

Both.

h. When does testing need to start and/or be completed by?

We have no pre-determined schedule.

i. Do you have any specific / custom reporting requirements?

No.

j. Is there to be an allowance made for re-testing for the system after remediation?

No any re-testing would be contracted via a supplemental Work Order.

38. External Penetration Testing

k. Is the penetration test going to include network layer testing? If so, how many IP addresses will be included in the scope of testing?

Yes. 10.120.240.0/24 and 172.30.0.0/21 are internal IP addresses and 167.102.134.128/27 are external.

l. Do you want us to have any of the identified vulnerabilities exploited?

No.

m. Is the penetration test going to include application layer testing? If so, how many websites and / or web applications will be included in the scope of testing?

No and none.

n. Are the targets in the scope of testing live and in production?

Yes.

o. If websites are included in the scope and portions of the website require credentials to access, how will that be handled?

Not applicable.

p. If there are IPS solutions or web application firewalls in place that can prevent or block penetration test activities, how will they be handled?

Configured as normal.

39. Scale – Ranges – Hosts – Location

q. What range of IP address will be provided?

10.120.240.0/24 and 172.30.0.0/21 are internal IP addresses and 167.102.134.128/27 are external.

r. How many hosts or devices are to be tested?

Approximately 30 servers, one firewall, one WAF, one router and one DMZ switch are in scope.

s. Is testing to be external or internal?

Both.

t. Is testing to be conducted during business hours or non-business hours?

During non-business hours.

u. What are the affected wireless infrastructure physical addresses?

Not applicable.

40. Internal Penetration Testing Targets

v. What is the total number of targets that will be included in the scope of testing?

Approximately 50.

w. If servers are included in the scope of testing, what is the approximate number to be tested?

Approximately 30.

x. If workstations are included in the scope of testing, what is the approximate number to be tested?

Approximately 10.

y. If network devices are included in the scope of testing, what is the approximate number to be tested?

One firewall, one WAF, one router and one DMZ switch are in scope.

z. If peripherals are included in the scope of testing, what is the approximate number to be tested?

Not applicable.

aa. The conventional approach for conducting internal penetration testing is to allow the tester on the premise; connect to the corporate network and obtain a valid IP address; be placed on a network with the targets or is routable to the networks with the targets; any security systems in place treat the tester's machine as any normal user's machine. If your expectation of the approach differs from the above, please explain.

The MIA's expectation is consistent with this approach.

41. Application / Systems Testing

bb. What applications / systems are subject to testing? Please provide URLs if possible. Please provide a test login to enable us to walk through the application.

None.

cc. What are the major functions of the target applications / systems?

Not applicable.

dd. Is testing to be completed with or without valid user credentials?

Not applicable.

ee. Are the applications in-house developed or based on commercial products? If in-house, what language was used in the development?

Not applicable.

ff. Will the system be in production at the time of testing?

Not applicable.

gg. How many pages are in the application?

Not applicable.

hh. How many input fields (approx.) does the application have?

Not applicable.

42. Databases and Data Analytics

ii. How many databases are running in production? What kind? And what's the approximate size of each database?

Not applicable.

jj. Do you currently have any cloud implementation? If yes, what are the scope and protocols of your cloud infrastructure?

Cloud infrastructure is not in scope for security penetration testing.

kk. Have you conducted a Cyber Security Data Management Analytics? Do you want us to look into that?

No to both questions.

ll. Has there been any form or cyber-attack or systems / data compromise at MIA?

Not that we are aware of.

mm. Any incidents you would like to share with us?

No.

43. MIA Business Unit Locations and Wireless Infrastructures

nn. What are the physical addresses for all MIA's business units and wireless infrastructures?

Physical address is for the MIA business units is 200 St. Paul Place Baltimore, Maryland 21202 and wireless infrastructure is not in scope for security penetration testing.

44. User Training and Manuals

oo. Do you expect us to engage in user training functions?

No.

pp. Do you expect us to prepare User Cyber Security Best Practices Manuals?

No.

45. Proposed Personnel and Task Order Staffing

qq. We are required to propose three Key Personnel as per the TORFP. What are the specific CATS+ Master Contract Project Number Labor Categories for these positions? Out pricing will be determined on these labor categories.

Contractor responsibilities including, KEY Personnel requirements are defined in section 2 of the solicitation. Offerors may propose job descriptions for KEY Personnel. Those job descriptions do not have to correspond with job descriptions under the CATS Plus master contract.

46. TORFP Minimum Qualifications

rr. We have found that the InfoSec Assessment Methodology (IAM) Certification is an outdated certification. Could you please consider removing this requirement?

ss. Would you please change the requirement for a Cisco Master Security Specialized Partner Certification to a Current Industry Recognized Cyber Security solutions and services certification?

Please see the amended TORFP. The InfoSec Assessment Methodology (IAM) Certification and the Cisco Master Security Specialized Partner Certification are now preferred qualifications.

47. New TORFP Released on 1/4/2017

    tt. There are several changes on the new TORFP released on 1/4/2017. Namely the following sections have been removed from 2.6 Requirements:

        i. Regulatory Requirement Assessment
        ii. Business Continuity Assessment
        iii. Social Engineering Assessment
        iv. Web Applications and Website Security Test
        v. Wireless Infrastructure Test

    What are the purposes and scopes of these changes? What are the performance and deliverable impacts of these changes in this project?

The purpose of these changes is to reduce the scope of work. Section 2.8.4 of the TORFP has been updated to reflect a reduced number of deliverable to correspond with these changes.

48. Can we provide supplemental information on professional services that compliment or enhance what's listed in the TORFP?
    Yes

49. On page 21 of the TORFP, under 2.9.1 you have listed Cisco Master Security Specialized Partner Certification as a minimum requirement. While this Cisco certification is Cisco's partnership and marketing measure, our team possess highly regarded and industry leaders' certifications. Would MIA be willing to change these two minimum requirements: InfoSec Assessment Methodology (IAM) Certification and the Cisco Master Security Specialized Partner Certification to Industry Leaders Recognized, Current and Most Relevant Certifications?
    Please see the amended TORFP. The InfoSec Assessment Methodology (IAM) Certification and the Cisco Master Security Specialized Partner Certification are now preferred qualifications.

50. Would MIA allow proposal of the listed optional services to include our Incident Response Plan Development and Table Top Exercise Services?
    We do not need these services. However you are free to add them to your proposal.

51. Is it appropriate to propose vulnerability scans and less invasive techniques to meet the intention of the MIA Internal and External Testing requirements; while with MIS's

agreement during the rules of engagement perform more aggressive testing to identify and attack significant cyber targets to meet the Penetration Testing requirement?

To be considered "responsive" a bid must conform in all material respects to the specifications outlined in the RFP.

52. How many days are you going to allow for the submission of our proposals after you respond to our questions? At least a week would be great.
Please see the amended TORFP. MIA has extended the closing date until 03/17/2017.

STATE OF MARYLAND

MARYLAND INSURANCE ADMINISTRATION

Office of Procurement

200 St. Paul Place, Suite 2700

Baltimore, Maryland 21202

IN RE:

PREBID CONFERENCE FOR SECURITY PENETRATION TESTING

Reported by: Erica Jones, Court Reporter

EVANS REPORTING SERVICE
The Munsey Building, Suite 705
Seven North Calvert Street
Baltimore, Maryland 21202
410.727.7100 800.256.8410

PRE-BID CONFERENCE

A Pre-bid Conference in the above-captioned matter held before the State of Maryland Insurance Administration, on Tuesday, January 17, 2017, commencing at 2:03 p.m., and reported by Erica Jones, Court Reporter and Notary Public.

APPEARANCES:

MIA STAFF MEMBERS:

Rodney Spence, MIA Procurement Officer

Katrina Lawhorn, MIA Procurement Officer

Mark Coburn

OTHERS PRESENT:

Antonio Frulio, IVA Communications
Solomon Mammo, IVA Communications
Murphy Payne, IVA Communications
Mike Gonzalez, BAE Systems
Mark Trump, BAE Systems
Jennifer Eslin, ePlus
Ron Brown, ePlus

CONFERENCE PROCEEDINGS:

MR. SPENCE: My name is Rodney Spence. Good afternoon and thank you for coming here. I'm the procurement officer and this is the Pre-bid Conference for Security and Penetration Testing. The solicitation number is D80B5400025. There's no new media involved for this solicitation. There is no VSB involved in this solicitation either. This solicitation is being done by competitive sealed proposal. The State uses a two-part evaluation process as far as there's a technical evaluation. And then there's a financial evaluation.

If your technical proposal does not meet our minimum qualifications or requirements, then we will send your financial proposal back to you unopened. If we have questions about your technical, then we will need to resolve those questions before we move on to your financial.

At this point, I'm going to let the rest of the people on the panel introduce themselves and state their positions. And we will get into some

question and answer. When we do the question and answer, I would ask that we go from right to left, front to back, state your name, state the company that you work for. If you don't have a question, just for the record, we would still ask that you state your name and company that you work for.

MS. LAWHORN: I'm Katrina Lawhorn, a procurement officer also.

MR. COBURN: I'm Mark Coburn and I'm team infrastructure supervisor.

MR. SPENCE: So at this point, Mark is going to tell us about the project background in the scope report.

MR. COBURN: Yes. The MIA computing infrastructure is a redundant, highly available, secure system with firewalls, web application firewalls, reverse proxies, intrusion prevention system, intrusion detecting systems, web security appliances, anti-virus software. And the State has conducted web application penetration tests on some of the agency's web application.

But MIA is undertaking this project to conduct a more thorough assessment of cyber security vulnerabilities. And we're seeking a consultant to make recommendations on how to mitigate these risks. Some of the highlights of the project is one, we'd like the vendor to assess MIA security policies and procedures and infrastructure against industry standard best practices and document some of the deficiencies.

Some of the other brief descriptions revolve around the external system tests. We'd like them to examine the external accessible equipment for vulnerabilities from inside and outside the internet. Also, some other activities revolve around internal system and network testing, conduct vulnerability scanning and validation against internal IP address ranges and configuration review of all internal systems.

The penetration test, we'd like some activities designed to emulate an actual attack and attempt to access and obtain organizational data.

And also, we're looking to get a risk report that can basically, you know, give an assessment of the test and discuss deficiencies and make recommendations to mitigate deficiences. That's kind of it in the things that we do.

MR. SPENCE: Okay. So we're going to open this up for question and answer at this point. I just want to make sure you guys understand the questions, for any questions that we receive are due tomorrow by the close of business at 5 o'clock.

So this gentlemen is on my right.

MR. GONZALEZ: Sure. Should I stand up or --

MR. SPENCE: If you want to stand up, that's fine.

MR. GONZALEZ: No. I'll just sit.

My name is Mike Gonzalez and I'm with BAE Systems. We're partnered, we're teamed up with IVA Communications and master contractor. One of our -- one of our focuses of our questions is around -- well, I guess first the time line about once we get

our response. Once we get our questions over to you tomorrow, what's the time line for getting it back to us so that we can put our response on a final report?

MR. SPENCE: Okay. So the answer to that question is we're going to get them back as soon as possible. The time it takes us to answer all the questions is depending on how involved the questions are and how many we receive.

Hopefully, we can get them out to you by the end of the week.

MR. GONZALEZ: Okay.

MR. SPENCE: But I can't guarantee we will get them to you until we know what we're working with.

MR. GONZALEZ: Sure. I guess, can I follow that up?

MR. SPENCE: (No verbal response.)

MR. GONZALEZ: Can I follow that question up?

MR. SPENCE: Yes, sure. Go ahead.

MR. GONZALEZ: So is the volume of questions or the amount of time it's going to take to get -- answer those questions, going to impact the final date? The 31st is the date today right now. Is that -- would that push that back?

MR. SPENCE: If we feel like we need an extension, then we will extend it.

MR. GONZALEZ: Okay.

MR. TRUMP: I'm Mark Trump. I'm with BAE Systems and we're teaming with -- with IVA Communications. The question I have is we deliver a host of services and one of the things I noted that we've seen a lot of other agencies look for is incident response.

And I was wondering if it's -- if it's too late to provide an optional service such as incident response program review, retain incident response services for instance to supplement the MIA's security program. That's one of the questions I have.

MR. SPENCE: That sounds like a technical

question.

MR. COBURN: Well, I think it's more of a procedural. I mean it's like a -- like a policy-type question where you're talking about an incident response --

MR. TRUMP: Sure.

MR. COBURN: -- like what the process is in case there is a --

MR. TRUMP: Right.

MR. COBURN: -- you know, a breach.

MR. SPENCE: More like a service level agreement?

MR. TRUMP: Well, absolutely. It wasn't requested as one of the items in the technical scope. So we were wondering if -- if it's possible to add an optional scope to this at this time. If it's not, then understood. But we did want to ask that question.

MR. SPENCE: That's something we're going to research and get back to you. If you want to, submit that question in writing.

MR. TRUMP: Okay.

MR. MAMMO: My name is Solomon Mammo. I'm from IVA Communications and I'm here with my partner. The question I have for you is the specs list. You have required us to have three personnel performing this project. But you have not specified which positions. In the CATS+ contract, there are positions under the contract. And usually when they run down RFPs, they will choose what the category, meaning which positions for that level categorization for this -- this RFP.

So my question is can you tell us what those three positions are or is it open for us?

MR. SPENCE: You're asking about the CATS+ job descriptions, right?

MR. MAMMO: Well, the job's categories. On the RFP --

MR. GONZALEZ: Categories.

MR. MAMMO: The job categories are -- are fixed. There is a list of job positions under CATS+. So when you are -- are asking us to submit

personnel, it has to be from that -- one of those listings.

MR. SPENCE: Okay. All right. What I'll tell you is that I'll have to take a look at what you're talking about.

MR. MAMMO: Okay.

MR. SPENCE: Please submit that in writing and we'll answer your questions.

MR. MAMMO: Just to follow up on Michael's question. So I will have the list of entire question by tomorrow for you.

MR. SPENCE: Okay.

MR. MAMMO: Right. How does that impact -- how soon you can respond back when the project is due? Like if you do not respond by let's say January 30th and the project is due the next day, that means we didn't have enough time to send our responses.

So can you give us at least one week working -- after you give the responses?

MR. SPENCE: Okay. So I'm just going to

repeat what I told him. We're going to do our best to get the answers to the questions out as quickly as possible. If we feel like we need to put an extension, then we will give you a reasonable amount of time to respond. That's something we're going to look at, okay?

MR. FRULIO: Antonio Frulio. I'm with IVA Communications and I don't have any questions.

MR. SPENCE: Okay.

MR. PAYNE: My name is Murphy Payne. I'm also with IVA and I don't have questions either.

MR. BROWN: I'm Ron Brown from ePlus. I have a question. The level of -- one of the requirements has a level of detail for a scan. And it wants us to look at potential compromised systems.

Are you expecting a forensic analysis or a very high level scale of IP addresses and those external locations that are probably coming into your environment that you weren't aware of?

MR. COBURN: Not a forensics analysis.

MR. BROWN: So not a deep dive?

MR. COBURN: No.

MR. BROWN: Okay.

MS. ESLIN: I'm Jennifer Eslin. I'm also with ePlus. We do have other questions and I think we'll probably submit them in writing because I think a lot of them are questions that you're probably going to need to, you know, research and get back to us and you'll want to be a part of the official record.

So I think we will have a nice healthy list for you that you'll get by tomorrow to start answering.

MR. SPENCE: Thank you. I appreciate it.

MR. BROWN: Can I ask one more question?

MR. SPENCE: Sure. Go ahead.

MR. BROWN: There's a certification in there that you're requiring from some of the individuals.

MS. ESLIN: Here (indicating).

MR. BROWN: Yeah, if I can look for a sec

(perusing).

MS. ESLIN: The IAM Certification?

MR. BROWN: Yeah. Is that a hard stop if they do or don't have that certification for individual firms?

MR. SPENCE: If we were to change that, it would require like some sort of amendment. So I could say for now, it's a hard stop. If it's in the solicitation, then that's what we're asking.

MR. BROWN: Okay. You don't see a whole lot of those out there.

MR. SPENCE: I can't hear what you're saying.

MR. BROWN: You don't see a lot of those out there very often.

MR. SPENCE: Okay.

MR. TRUMP: Same question, same concern.

MR. SPENCE: Well, you can submit your questions. You know, when we put together our answers, if something changes as a result of your questions -- that's what the back and forth is

for -- we will let you know.

MS. ESLIN: Okay.

Does anybody else have any other questions?

MR. TRUMP: Follow-up. Is all the work to be conducted in one facility or is there multiple MIA facilities in your --

MR. COBURN: One facility.

MR. TRUMP: And then to clarify, the three requirements -- the external testing, internal testing, PEN testing -- so there's a few ways we could bucketize [sic] this research.

One, for instance, would be full vulnerability scan and so forth without invasive action on the external and internal providing all of the theoretical holes that are there with mitigation recommendations. And then secondly, using the PEN test for actually -- an -- attack attempts. Otherwise, we could do an internal/external PEN test with full capability, which would omit the need for another PEN test following.

So we're anticipating to provide a response to vulnerability scans and non-invasive testing for the internal/external with full reporting and then do the attack testing internally using the PEN test binary.

MR. COBURN: I would submit a question on that.

MR. TRUMP: Okay.

MR. COBURN: That way, it's clear for everybody.

MR. TRUMP: Understood, understood. That way, we can respond back and phase over --

MR. SPENCE: All right. Let's -- okay.

MR. BROWN: Is this the first time you've done this level of testing or has it been done in the past by another vendor?

MR. COBURN: We've had a light testing done by DOIT. They offered a free web assessment vulnerability test.

MR. BROWN: But not a scaling test like this?

MR. COBURN: No. This is the most intensive test we've had to date.

MR. BROWN: Again, is it a one-time with an option to continue in the future or is it --

MR. SPENCE: I will let --

MR. COBURN: I don't want to guess. I think it's a continued in the future, I believe but I, you know -- submit that question and we'll respond.

MR. SPENCE: We will get back to you.

MR. MAMMO: And finally, when do you expect to start this project?

MR. SPENCE: As soon as possible, as soon as we award it, as soon as possible.

MR. GONZALEZ: I'm sorry. Mike Gonzalez. Basically -- and another question.

We saw the certifications changed with the last solicitation. You know, what was the emphasis around that? Was that -- again, is that a hard stop or, you know, just questioning regarding that as far as -- again it's not a certification. It's not,

it's --

MR. COBURN: Which certification are you talking about?

MR. MAMMO: The SSCP.

MR. GONZALEZ: The SSCP --

MR. MAMMO: That was added after the last revision on January 1st.

MR. COBURN: Well, submit a question on that and we'll review it and determine if that is a -- because I think there was something with the minimal requirements. And I can't remember what the original was.

Submit a question on that and we will get some clarifications. I believe all the minimal requirements are going to be required for this test. It could mean like what we need or I need as far as --

MR. SPENCE: Yeah. The minimal requirements aren't going to change unless we move for it.

MR. GONZALEZ: Understood.

MR. SPENCE: So if you guys submit your questions, if we need clarity to one of those rules, we will make that announcement to everyone we know. For now, the requirements -- the minimal requirements that are in the solicitation are what you need to be able to respond to.

All right. We're going to go ahead and close this down. I thank everyone for coming today. Again, your questions are due tomorrow by 5 o'clock p.m. local time. If you have any questions about this whole meeting, just give me a call, send me an e-mail. Everyone's going to get a copy of the transcripts of this by e-mail. And that's it.

Everyone have a good day.

(The conference concluded at 2:19 p.m.)

REPORTER'S CERTIFICATE

STATE OF MARYLAND

CITY OF BALTIMORE

I, Erica Jones, a Notary Public of the State of Maryland, Baltimore City, do hereby certify that the above-captioned proceeding took place before me at the time and place herein set out.

I further certify that the proceeding was recorded stenographically by me and this transcript is a true record of the proceedings.

I further certify that I am not of counsel to any of the parties, nor an employee of counsel, nor related to any of the parties, nor in any way interested in the outcome of the action.

As witness my hand and seal this 18th day of January, 2017.

Erica Jones
My Commission Expires 02/22/2020