

CYBERSECURITY PLANNING COMMITTEE

Virtual Meeting
Tuesday, November 19, 2024, 8:00 a.m.

1. WELCOME AND CALL TO ORDER

Ms. Gutierrez called the meeting to order at 8:03 a.m. and welcomed everyone to the meeting. She reviewed meeting procedures using the Zoom application.

2. ROLL CALL

MEMBERS PRESENT

Jason Johnson, Chair	Robert Benavidez
Dr. Lorie Liebrock	William A. York
Raja Sambandam, State CISO	William (Tim) Presley
Regina Chacon, Dep. Sec. DHSEM	Dr. Srinivas Mukkamala

MEMBERS ABSENT

Michael W. Good	Cassandra Hayne
Brigadier General Miguel Aguilar	Senator Michael Padilla

OTHERS PRESENT

Melissa Gutierrez, DoIT Cybersecurity Project Mgr.
Todd Baran, DoIT Associate General Counsel
Manny Barreras, DoIT Secretary Designee
Dan Garcia (OCS), Flori Martinez (OCS), Bryan Brock, Tracy Lopez

3. APPROVAL OF AGENDA

MOTION Ms. Gutierrez called for a motion to approve the Agenda. Dr. Liebrock so moved, seconded by Mr. Benavidez. There being no opposition, the Agenda was approved.

4. Vendor recommendation and vote for SLCGP Project 3- Vulnerability & Attack Surface Management – Robert Benavidez

Mr. Benavidez reviewed the process the Subcommittee used to evaluate the applicants for this project. The Subcommittee is recommending Securin for these services, for all 26 agencies, stating that the Subcommittee believes this is the best economy of scale and best utilization of the funding and provides the ability to collaborate using the same platform, as well as standardization and reduction of complexity.

Chair Johnson called for any comments or questions from Committee members.

Mr. Sambandam stated that he agrees with the assessment provided by Mr. Benavidez.

Chair Johnson also voiced his agreement with this approach, keeping a fairly narrow portfolio at this time.

MOTION Chair Johnson entertained a motion to approve Securin as the vendor for the services included in Project 3 – Vulnerability & Attack Surface Management. Ms. Chacon so moved, seconded by Dr. Liebrock. Roll call vote was conducted by Ms. Gutierrez. Vote was unanimous to approve Securin as the vendor for services included in Project 3- Vulnerability & Attack Surface Management.

5. Vendor recommendation and vote for SLCGP Project 2 – Cybersecurity Risk Assessment (NCSR Completion Support)

Mr. Benavidez reported that the Procurement Subcommittee met the previous day and reviewed 22 responses from various vendors, from a low of \$68,000.00 to a high of \$6.3 million in terms of cost estimates. The Subcommittee has examined the detailed responses and they are recommending Compunnel as the vendor for these services, with their estimate being just under \$311,000.00 for 22 agencies. This vendor provided a very comprehensive proposal and the Subcommittee feels this provided the best mix of value for the program.

Mr. Sambandam asked for more background information regarding this vendor, such as whether or not they are a local company.

Mr. Benavidez stated that this is not a local company and none of the Subcommittee members have had previous experience with Compunnel. However, they are on the State price agreement so they meet the procurement requirement to provide these services. Compunnel was chosen based on their proposal, their quotation, and in comparison to the value received from other vendors. Their proposal showed significant evidence of understanding risks and controls effectively and understanding the cybersecurity framework, as well as the method they propose to move forward reflecting a broader understanding of the field than even that defined in the scope of work in the request for services.

Ms. Gutierrez noted that the proposal from Compunnel was sent out to Committee members yesterday.

Dr. Liebrock commented that all of Compunnel's reviews on the Better Business Bureau are only one star reviews, and they are rated as an A-, but are not accredited, so gives mixed reviews. She noted one other item that might be a red flag is they state they will conduct up to two interviews, but do not ensure that they will even conduct one.

Mr. Benavidez replied that the Subcommittee did not look at Compunnel's Better Business Bureau ratings and given what Dr. Liebrock has shared this is a concern, especially having no previous experience with this vendor. He stated that it seems as though more review and discussion is needed regarding Compunnel.

Chair Johnson stated this could be made conditional upon research of references, etc. He asked Mr. Benavidez if there was a secondary recommendation from the Subcommittee for Project 2. Mr. Benavidez stated that there was discussion in the Subcommittee about a back-up but they did not actually identify one. He commented that there would probably be agreement that there were a fair number of acceptable candidates on the short list, but he does not feel that there is a consensus in the Subcommittee to make a secondary recommendation at this time. Mr. Benavidez asked Ms. Gutierrez if she concurred with this assessment, which she did.

Mr. Benavidez concurred with Chair Johnson's proposal to give conditional approval pending direct feedback from recent Compunnel customers, and if this is positive to move forward, if negative come back to the Committee with a second recommendation.

Dr. Liebrock stated she is comfortable with this approach.

Mr. Benavidez stated that a major factor is the need to get to contract by the first week of December in order to meet the end of February deadline for the NCSR survey that is associated with this.

Mr. Sambandam agrees with this approach; having a follow up discussion, checking references and in the meantime prepare for a potential secondary recommendation.

Chair Johnson noted that time is of the essence, but there needs to be confidence in the recommendation and what could be done to pivot quickly and perhaps have another meeting to meet this deadline.

MOTION Chair Johnson called for a motion to conditionally approve Compunnel as the vendor for the services included in Project 2 - Cybersecurity Risk Assessment, (NCSR Completion Support), based upon receiving positive input from recent references. Dr. Liebrock so moved, seconded by Mr. Presley.

Mr. Sambandam asked if the motion included selection of a secondary recommendation. Chair Johnson responded that he did not believe this needed to be in the motion, however, that would be due process. Dr. Liebrock noted that if the references do not check out, that would be the expectation, but if the references do check out there would be no need. Mr. Benavidez agreed that procedurally, if the references do not check out the Subcommittee would bring a second recommendation to the Committee for approval, as they do not know who that would be at this time.

Roll call vote was conducted by Ms. Gutierrez. Vote was unanimous to conditionally approve Compunnel as the vendor for these projects with the stipulations stated.

6. Vendor recommendation and vote for SLCGP Project 4 – Cybersecurity Training

Mr. Benavidez reported that there were three responses received for quotes on this project, which were fairly tight, \$58K to \$71K. He added that there was some discussion about whether to award this to a single vendor or perhaps split it among vendors, but the consensus was there would be more leverage keeping it with one vendor, administratively as well as across the user base.

The recommendation of the Subcommittee is to move forward with KnowBe4 to provide cybersecurity training for the applicants within the Year-1 program.

Chair Johnson stated that this vendor is currently being used by some State agencies, and one of the things that these agencies like is that they can customize the platform to go back to the appropriate individual in that agency.

Dr. Liebrock commented that none of the three companies that provided quotes are on the Better Business Bureau, however, looking at Gartner's Reviews, KnowBe4 is in the middle of the reviews for these three, but the higher rated company has very few reviews, and KnowBe4 has over 2,000 reviews rating them highly. She added that many on the Committee have experience with KnowBe4 through their various organizations, making them a known partner and good choice.

Mr. York stated that he has had a good experience with KnowBe4, however, he expressed his concern about the company being highly involved with the Church of Scientology. He reported that the Department of Health is looking at a product called Hoxhunt, an excellent product with shorter training modules.

Dr. Liebrock asked Mr. Benavidez if there was a quote from Hoxhunt. Mr. Benavidez replied that the Subcommittee did not receive a quote from this company. The three which responded were Cofenc Phishme, KnowBe4 and Titan HQ.

Ms. Gutierrez commented that the training is a little more difficult to procure because there are no companies for this on the statewide price agreement. The state is using a third-party vendor SHI, in order to procure this many licenses. The quotes are from SHI, but the entities that were quoted out are also on the GSA, so there is some consistency with being on the GSA as well as the third-party SHI.

Mr. York noted that OCS offered to secure the product for them, but he does not know anything about SHI.

Mr. Presley commented that he uses Arctic Wolf and he got this through SHI as well.

Mr. Sambandam stated that more than 20+ states using KnowBe4. have onboarded their entire state using KnowBe4 because of the existing working relationship in implementing security awareness

training across those states. He is waiting for additional information from NASCIO on how many states are using this. This product has worked in the past and currently with many other states for many of the federal compliance mandates, including PCI, IRS, things of that nature. This may be a feature set available on many other products, but they are very lean. This is the opinion he has gathered communicating with other CISOs from various states.

Mr. York stated the only things he did not like about KnowBe4 were their association with the Church of Scientology and the length of the training videos. Other than this he has no problem with the company.

Chair Johnson added that as important as training is, it would not necessarily be a problem to change from one product to another in the future. He noted that timing is of the essence and there is more knowledge/experience with KnowBe4, and as other vendors become available then this could be revisited next year.

Mr. Garcia noted that because of the number of licenses needed and the options for expansion these three vendors were the only ones available on the NASCIO/GSA agreement.

Chair Johnson thanked Mr. Garcia for this additional information.

Chair Johnson stated that due to the existing time constraints it would not be feasible to pursue additional quotes and perhaps this could be addressed in the future. He added that it makes sense to proceed with KnowBe4 at this time, then take time to examine this next year when the contract is up for renewal. Mr. Benavidez agreed with this approach.

MOTION Chair Johnson called for a motion to approve KnowBe4 as the vendor for Project 4, Cybersecurity Training. Dr. Liebrock so moved, seconded by Mr. York. Roll call vote was conducted by Ms. Gutierrez. Vote was unanimous to approve KnowBe4 as the vendor for services included in Project 4 – Cybersecurity Training.

7. Public Comment

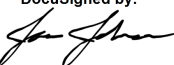
None.

8. Adjournment:

MOTION Ms. Gutierrez called for a motion to adjourn. Dr. Liebrock so moved, seconded by Mr. York. There being no objection, and no further business before the Committee the meeting adjourned at 8:32 a.m.

Mr. Sambandam thanked the Committee members for making the adjustments to their schedules to attend today's meeting and getting these important activities addressed.

Chair Johnson thanked Mr. Benavidez and the Engagement and Procurement Subcommittees for their work and effort to gather this information so the Committee can make these important decisions.

DocuSigned by:

17B63C4A596D447...

Jason Johnson, Chair