Department of Health

Puerto Rico Medicaid Program

AWARD NOTIFICATION
Independent Security & Privacy Control Assessment
2024-PRMP-ISPCA-006

Pursuant to Administrative Order Num. OA-586[1], Act. No. 38/2017[2], as amended, and 45 CFR 74.327-329, the Puerto Rico Medicaid Program (PRMP) issued the request for proposal 2024-PRMP-ISPCA-006 (the RFP) with the purpose of evaluating responses and selecting a vendor to conduct multiple Independent Security & Privacy Control Assessment (ISPCA) operations of existing, future or projected PRMP applications, systems functionality, and system implementations such as EDW, HIE, EVV, TPL, and AVS.

PRMP received proposals from four (4) vendors. The first evaluation focused on the technical proposals and the second on the cost proposals. Conforming with Administrative Order Num. OA-586, a Technical Committee was formed for the evaluation of the technical portion of this RFP. In accordance with sections 5.1 and 5.2 of the RFP, proposals were evaluated by the Puerto Rico Department of Health (PRDoH) appointed committee, across five aspects (evaluation categories), using a weight/score methodology with a maximum overall total of 1,400 points, since oral presentations were not held. The Evaluation Committee would then recommend to the PRMP executive director for the contract to be awarded to the highest-ranked vendor from all evaluated and eligible vendors.

Based on the Technical Committee's determinations and scores given to the proposals, the Evaluation Committee recommended to the PRMP executive director that the *Buena Pro* and subsequent contract be awarded to Netxar Cybersecurity Group, whose proposal scored a total of 910 points. Having accepted the Evaluation Committee's recommendation, the program's executive director notifies this *Award Notification* in favor of Netxar Cybersecurity Group.

The professional services to be provided will be based on a one (1) year contract, with four (4) optional one-year extensions. Prior to the formation of the contract, this *Award Notification* and Netxar's proposal must be verified by Centers for Medicare & Medicaid Services (CMS). Once approved, Netxar shall submit all required documentation, including a brief of its proposal, to the PRMP contract office. Moreover, the awarded vendor must be registered with the *Registro Único de Proveedores de Servicios Profesionales (RUP)* from the Puerto Rico General Services Administration.[3] Furthermore, it is notified that no service shall be provided by Netxar until a copy of the contract is filed with the Puerto Rico Office of the Comptroller.

[1] Issued by the Department of Health of Puerto Rico.

[2] Known as the Government of Puerto Rico Uniform Administrative Procedure Act.

[3] *See:* Reglamento 9302E Sole Registry of Professional Service Providers, available in asg.pr.gov/publicacionesreglamentos.

PROCEDURAL BACKGROUND

On September 26, 2024, PRMP published on several websites[4] the RFP seeking competitive proposals from independent security and privacy control assessment vendors to manage the program's IPSCA operations and oversee its technical services, including all technological infrastructure and related services. Through the Request for Proposals (RFP), PRMP solicited the services of a vendor to perform independent and objective assessments of its applications and systems to determine whether the security and privacy controls in the PRMP are implemented correctly, operate as intended, and produce the desired outcomes for meeting the security and privacy requirements of the applications or systems. Thus, PRMP wishes to contract with an IPSCA operator (vendor) that will provide such technical services.

Interested vendors had the opportunity to present questions and receive corresponding answers that helped clarify instances of the RFP. PRMP received a total of seventy-six (76) questions. Prior to the submittal of the proposals, PRMP issued two (2) Important Updates with the purpose of announcing events, corrections, and amendments related to the RFP.

PRMP received proposals from four (4) vendors. All proposals passed the mandatory screening stage and moved forward to the first phase, the evaluation of the technical proposals.

The Technical Committee proceeded with their analysis of the technical proposals over a period of two (2) weeks. Its members evaluated each proposal at an individual level, followed by a group session where they discussed individual scores and reached a group score consensus. This process repeated itself for each proposal. Up to this point in the process, cost proposals remained sealed. At the end of the technical proposals analysis, the Technical Committee decided which proposals were to move forward to the cost proposals analysis according to the 70% threshold indicated in section 5.1 of the RFP. In this RFP the 70% threshold represents 840 points out of 1200, since oral presentations were not held. The final stage of the evaluation process consisted of the opening, scoring, and adding of those cost proposals to determine the overall best-ranked vendor.

SUMMARIES OF EVALUATED PROPOSALS
(listed in alphabetical order)

Earthling Security, LLC

Earthling Security, LLC (from now on "Earthling"), is a for-profit limited liability company based in Reston, VA. Earthling has ten (10) years of experience and a total of five (5) full-time employees providing the type of services specified in the RFP. Moreover, Earthling is a FedRAMP/3PAO cybersecurity and compliance firm who, according to its proposal, specializes in securing cloud environments and helping healthcare organizations meet regulatory requirements. They possess knowledge of frameworks like CMS MARS-E, FedRAMP, and NIST SP 800-53A, and are experienced in securing AWS, Azure, and GCP cloud environments using Infrastructure as Code. Their technical expertise includes advanced vulnerability scanning and penetration testing aligned with industry best practices.

[4] Medicaid website, Puerto Rico Department of Health website, Puerto Rico General Services Administration website.

As conveyed in their proposal, Earthling takes a risk-based approach to assessments, prioritizing critical vulnerabilities and providing detailed reports with actionable remediation plans. With experience in the healthcare sector, they have conducted MARS-E assessments for various organizations and performed security and privacy assessments for Medicaid Enterprise Systems (MES). They offer a tailored approach to each client, emphasizing collaboration and knowledge transfer. Their focus on cloud security and automation, combined with their healthcare expertise, distinguishes them.

Earthling proposed the following key staff:

1. Lead Security Assessor
2. Penetration Testing Specialist
3. Compliance and Privacy Specialist
4. Project Manager

Earthling has the following auditing certifications:

1. CISSP
2. CISA
3. CISM
4. CCSK
5. PMP

Earthling has privacy and security experience with the following:

1. IS2P2
2. MARS-E
3. ISO 27001
4. NIST SP
5. HIPAA
6. DFARS
7. FedRAMP/3PAO

Nevertheless, Earthling's proposal failed to grab the attention of the Technical Committee across all evaluation categories. The members concluded that its responses were vague or too general and failed to provide the vendor's approach to tackle the needs specified in the request for proposals. The vendor seemed to be confused with the transition aspects of the proposal and answered as if they were transitioning in. The vendors proposal also failed to detail how they planned to comply with the SLAs. The Technical Committee could not get a clear idea of how the vendor would provide the assessments expected for all applications of the MES. The vendor did not provide a timeframe for each assessment in terms of weeks duration.

Cost Proposal: **$2,407,373.54**

Emagine IT, Inc.

Emagine IT, Inc. (from now on "EIT"), is a for-profit corporation based in North Bethesda, MD. EIT has eighteen (18) years of experience and a total of seventy-six (76) full-time employees providing the type of services specified in the RFP. Moreover, EIT specializes in cybersecurity and compliance for health and complex information systems, with a focus on Risk Management Framework (RMF) implementation and data-driven security. According to its proposal, EIT is one of only forty-five (45) global Third-Party Assessment Organization (3PAO) providers and the 7th-ranked all-time FedRAMP Assessor in the global marketplace.

As mentioned in their proposal, their team includes certified professionals with experience managing large-scale RMF processes and conducting Privacy Impact Assessments as well as facilitating strategic and cultural shifts within organizations, promoting security models through a data-driven approach. Furthermore, they have a record of transforming security postures and have managed the CMS ISPG's Cybersecurity and Risk Assessment Program. EIT's focus on proactive security, combined with their RMF experience and partnership with Cyber Unveil International, LLC for local expertise, positions them as a partner for organizations seeking to enhance their security maturity.

The vendor indicated that "the timeframe for delivering each assessment spans approximately 12 weeks, structured to address the complexity of producing four (4) integrated deliverables. The process begins with the development of the System Assessment Plan (SAP) within the first two (2) weeks, followed by a coordinated two-and-a-half-month effort to complete the Security Assessment Worksheet (SAW) and the Security Assessment Report (SAR). Through each stage, the Plan of Action and Milestones (POA&M) is continuously updated and refined to reflect findings and mitigation strategies, ensuring it remains aligned with the assessment's progression."

EIT proposed the following key staff:

1. Program Manager
2. Senior Lead Assessor
3. Penetration Tester
4. Security Assessor
5. Physical Assessor

EIT has the following auditing certifications:

1. CIPP
2. CISSP
3. CISA
4. CISM
5. PMP

EIT has privacy and security experience with the following:

1. MARS-E
2. ISO 27001
3. NIST SP
4. HIPAA
5. FISMA
6. A2LA
7. CMMI DEV
8. SVC ML3
9. ISO 20000
10. ISO 9001
11. FedRAMP/3PAO

Cost Proposal: **$6,319,894.35**

FTI Consulting, Inc.

FTI Consulting, Inc. (from now on "FTI"), is a for-profit corporation based in Washington, DC. FTI has five (5) years of experience and a total of sixteen (16) full-time employees providing the type of services specified in the RFP. Moreover, FTI is a global risk management and compliance firm with a dedicated cybersecurity practice specializing in healthcare. Their cybersecurity team comprises of experienced consultants from law enforcement, intelligence, and the private sector, proficient in conducting NIST SP 800-53, HIPAA, and ISO 27001 assessments. They offer a wide range of services, including penetration testing, dark web analysis, and compliance reviews.

FTI leverages a partnership with HealthTech Solutions LLC (from now on "HealthTech"), a for-profit limited liability company based in Frankfort, KY and healthcare technology consulting firm. With thirteen (13) years of experience and around two hundred and fifty (250) full-time employees providing the type of services specified in the RFP, they have had experience with Medicaid Enterprise System (MES) planning, procurement, and project management engagements in multiple states. In these engagements, HealthTech has worked with Gainwell Medicaid management information systems, eligibility, and enrollment (E&E) systems, analytics and data warehousing systems, electronic visit verification (EVV) systems, asset verification systems (AVS), and health information exchanges (HIEs).

Having a combined partnership with HealthTech, FTI possess experience with Medicaid enterprise systems and federal requirements. FTI's focus on risk management, merged with their global cybersecurity expertise and local knowledge in Puerto Rico, makes them a contender in the healthcare cybersecurity space.

The vendor proposed the following key staff:

1. ISPCA Engagement Director
2. ISPCA Engagement Manager
3. ISPCA Lead Methodologist

4. ISPCA Senior Advisor – Puerto Rico Information Security and Privacy Laws and Regulations
5. ISPCA Methodologist
6. ISPCA Senior Advisor – Federal Information Security and Privacy Laws and Regulations
7. ISPCA Assessment Team Lead – Team 1
8. ISPCA Assessment Team Lead – Team 2

FTI has the following auditing certifications:

1. CIPP
2. CISSP
3. CISA
4. CISM
5. CBCP

FTI has privacy and security experience with the following:

1. MARS-E
2. ISO 27001
3. NIST SP
4. HIPAA
5. FIPS
6. FISMA
7. HITECH

As in the case of Earthling, FTI's proposal did not meet the minimum required score to pass the 70% threshold and move on to the cost evaluation phase. Even though the Technical Committee recognized the amount of experience accumulated by its personnel, the members considered that the vendor did not directly address the requirements established in the request for proposals. Much of the proposal goes on to describe the vendor's experience dealing with different clients and projects, but failed to portray how those experiences would be implemented to attend PRMP's needs described in the RFP.

Regardless of the score, FTI's cost proposal puts the vendor's proposal way outside of any serious consideration.

Cost Proposal: **$24,281,765.36**

Netxar Cybersecurity Group

Netxar Cybersecurity Group (from now on "Netxar"), is a for-profit joint venture based in San Juan, PR. Netxar has twenty-four (24) years of experience and a total of seventy (70) full-time employees providing the type of services specified in the RFP. Moreover, Netxar specializes in cybersecurity, privacy compliance, and risk management, with a strong focus on serving finance, government, and healthcare sectors. They have experience conducting Independent Security and Privacy Control Assessments (ISPCAs) and are proficient in industry standards like NIST SP 800-53 and ISO 27001. Their team consists of certified professionals capable of performing technical assessments, including penetration testing and vulnerability analysis.

Netxar follows a structured methodology for ISPCAs, prioritizing stakeholder engagement and delivering detailed reports with actionable recommendations. They offer continuous monitoring and support to ensure the long-term effectiveness of security controls and tailor assessments to meet specific client needs. With a proven record of accomplishment in the healthcare sector, Netxar's focus on client-specific solutions and their commitment to continuous improvement make them a reliable partner for organizations seeking to enhance their security and privacy posture.

Netxar's proposal included an illustrated timeline summary that suggested a 20-week timeframe to ensure that PRMP's systems, applications, programs, and processes would be assessed thoroughly and aligned with regulatory requirements. As stated in their proposal, the purpose of this detailed roadmap would be achieving compliance while enabling PRMP to effectively manage resources and track progress throughout the assessment process. However, it was not clear to the committee whether the 20 weeks mentioned in the summary were for all the assessments required for the MES applications or for each application. Netxar was asked, according to section 8.1[5] of the RFP, to clarify this aspect. Nextar clarified that each individual assessment would take from 5 to 7 weeks.

Netxar proposed the following key staff:

1. Project Manager
2. Lead Security Architect
3. Compliance Specialist
4. Senior Penetration Tester
5. Quality Assurance and Report Writing

Netxar has the following auditing certifications:

1. CIPP
2. CIPP/G
3. CISSP
4. CISA
5. CISM
6. PMP

Netxar has privacy and security experience with the following:

1. IS2P2

[5] "PRMP reserves the right to award a contract based on initial responses received; therefore, each response shall contain the vendor's best terms and conditions from a technical and cost standpoint. PRMP reserves the right to conduct clarifications or negotiations with one or more vendors. All communications, clarifications, and negotiations shall be conducted in a manner that supports fairness in response improvement."

2. ARS
3. MARS-E
4. ISO 27001
5. NIST SP
6. HIPAA

Cost Proposal: **$1,279,446.67**

PROPOSAL EVALUATION

A – METHODOLOGY AND ANALYSIS OF TECHNICAL PROPOSALS

The purpose of this request for proposals was to acquire the services of a vendor to perform independent and objective assessments of PRMP's applications and systems to determine whether the security and privacy controls in the program are implemented correctly, operate as intended and produce the desired outcomes for meeting the security and privacy requirements of the applications or systems. These assessments must comply with the CMS framework.

According to OA-586, proposals were evaluated by a technical and evaluation committee, both appointed by the Secretary of the Puerto Rico Department of Health. Section 2.11.4 of the RFP instructed vendors to submit proposals in two distinct parts sealed in separate envelopes: technical proposal and cost proposal. Prior to the opening of the cost proposals, technical proposals were evaluated by each member of the Technical Committee at an individual level, followed by a group session where members discussed their personal analysis and reached a consensus score. Members of the Evaluation Committee had no access to cost proposals until all proposals were group-scored.

Technical proposals were scored by assigning a value from a scale of 1 through 5 to each criterion according to the following rubric:

5: Excellent – exceeds the specifications
4: Good – fully addresses the specifications
3: Marginal – addresses the specifications, but has some minor deficiencies
2: Deficient – partially addresses the specifications or is very limited
1: Unacceptable – fails to address the specifications

The following evaluation criteria was stated in the RFP:

Evaluation Category	Points Allocated
Criterion 1: Vendor Qualifications and Experience	200 points possible
Criterion 2: Project Organization and Staffing	300 points possible
Criterion 3: Approach to Statement of Work	550 points possible
Criterion 4: Privacy and Security Requirements	150 points possible
Criterion 5: Oral Presentations (if held)	50 points possible

Criterion 6: Cost Proposal	200 points possible
Total Points Possible	**1,450 points**

Since oral presentations were not held, the maximum number of points available was **1,400**.

To produce the *Points Allocated* in the RFP, a **weight/score formula** was implemented. Regarding each evaluation category, throughout the RFP vendors were solicited specific information. Proposals were evaluated based on their submitted responses. Each item had an assigned weight, which had to be multiplied by the consensus score given by the Technical Committee. The weights assigned to each *technical* criterion multiplied by a score of 5 would give 1,200, the maximum available points for technical proposals.

According to RFP records, technical proposals were initially evaluated and scored by the members of the Technical Committee, who provided an analysis of each proposal to the members of the Evaluation Committee. The Technical Committee was not allowed to see the cost proposals. Members of the Evaluation Committee accepted the Technical Committee's analysis in its entirety. Once the technical analysis was submitted, the Evaluation Committee proceeded to evaluate and add the costs proposals' scores.

As provided in section 5 of the RFP, only proposals that receive the minimum acceptable technical score 840 (70% of applicable technical evaluation points) would be eligible to move forward to the cost proposal evaluation phase thus not all vendors that participated and submitted their proposals for evaluation were able to reach the corresponding threshold. As stated before, Earthling and FTI failed to reach the threshold and consequently did not move forward to the cost and final consideration phase. In general, both failed to provide the level of description and detail that was expected in terms of how the vendors' experience and expertise would be applied to PRMP's needs and requirements.

The following tables portray the Technical Committee's consensus scores for each vendor's *technical* criterion and their respected allotted points. *Table 1* portrays the scores of the proposals that did not pass the 70% threshold and *Table 2* portrays the proposals that passed the 70% threshold. (Please see the attached *Addendum Scoring Area Captions*):

Table 1:

Evaluation Category	weight	**Earthling Security**		**FTI Consulting**	
		score	points	score	points
Vendor Qualifications and Experience	---	---	---	---	---
A.	10	3	30	3	30
B.	10	3	30	4	40
C.	10	4	40	3	30
D.	10	2	20	3	30

Subtotal	---	---	**120**	---	**130**
Evaluation Category	weight	**Earthling Security**		**FTI Consulting**	
		score	points	score	points
Project Organization and Staffing	---	---	---	---	---
Initial Staffing Plan	---	---	---	---	---
E.	5	3	15	3	15
Key Staff, Resumes, and References	---	---	---	---	---
F.	5	3	15	4	20
G.	5	3	15	3	15
H.	5	3	15	3	15
I.	5	3	15	3	15
J.	5	3	15	3	15
K.	5	3	15	3	15
L.	5	3	15	4	20
M.	5	3	15	4	20
N.	5	3	15	4	20
O.	5	3	15	4	20
P.	5	3	15	3	15
Subtotal	---	---	**180**	---	**205**
Approach to SOW	---	---	---	---	---
Q.	5	3	15	4	20
R.	5	3	15	4	20
S.	5	3	15	3	15
T.	5	3	15	4	20
U.	5	2	10	3	15
V.	5	3	15	3	15
W	5	3	15	3	15
X.	5	3	15	3	15
Y.	5	3	15	3	15
Z.	5	3	15	3	15
Aa.	5	3	15	3	15
Bb.	5	3	15	4	20
Cc.	5	3	15	3	15
Dd.	5	3	15	4	20
Deliverables	---	---	---	---	---
Ee.	5	3	15	3	15
Ff.	5	3	15	4	20

Gg.	5	3	15	4	20
Hh.	5	3	15	4	20
Ii.	5	3	15	3	15
Jj.	5	3	15	4	20
Kk.	5	3	15	4	20
Ll.	5	3	15	3	15
Subtotal	---	---	**325**	---	**380**
Privacy & Security Requirements	---	---	---	---	---
Mm.	4	3	12	3	12
Nn.	4	3	12	3	12
Oo.	4	3	12	3	12
Pp.	4	3	12	3	12
Qq.	4	3	12	3	12
Rr.	4	3	12	3	12
Transition Requirements	---	---	---	---	---
Ss.	2	2	4	4	8
Tt.	2	2	4	3	6
Uu.	2	2	4	4	8
Subtotal	---	---	**84**	---	**94**
Evaluation Category	weight	**Earthling Security**		**FTI Consulting**	
		score	points	score	points
Oral Presentations	---	---	---	---	---
Technical Total	---	---	**709**	---	**809**

Table 2:

Evaluation Category	weight	**Netxar**		**Emagine IT**	
		score	points	score	points
Vendor Qualifications and Experience	---	---	---	---	---
A.	10	3	30	4	40
B.	10	4	40	3	30
C.	10	3	30	4	40
D.	10	2	20	4	40
Subtotal	---	---	**120**	---	**150**

		Netxar		Emagine IT	
Evaluation Category	weight	score	points	score	points
Project Organization and Staffing	---	---	---	---	---
E.	5	4	20	4	20
Key Staff, Resumes, and References	---	---	---	---	---
F.	5	3	15	4	20
G.	5	4	20	3	15
H.	5	4	20	3	15
I.	5	4	20	3	15
J.	5	4	20	4	20
K.	5	4	20	3	15
L.	5	4	20	4	20
M.	5	4	20	4	20
N.	5	4	20	4	20
O.	5	4	20	3	15
P.	5	4	20	3	15
Subtotal	---	---	**235**	---	**210**
Approach to SOW	---	---	---	---	---
Q.	5	4	20	3	15
R.	5	4	20	3	15
S.	5	4	20	4	20
T.	5	4	20	3	15
U.	5	4	20	4	20
V.	5	4	20	3	15
W.	5	4	20	4	20
X.	5	4	20	4	15
Y.	5	3	15	3	15
Z.	5	4	20	3	15
Aa.	5	4	20	3	15
Bb.	5	4	20	3	15
Cc.	5	4	20	3	20
Dd.	5	4	20	4	15
Deliverables	---	---	---	---	---

Ee.	5	4	20	3	20
Ff.	5	4	20	4	20
Gg.	5	4	20	4	20
Hh.	5	4	20	4	20
Ii.	5	4	20	4	20
Jj.	5	4	20	4	20
Kk.	5	4	20	4	20
Ll.	5	4	20	4	20
Subtotal	---	---	**435**	---	**390**
Privacy and Security Requirements	---	---	---	---	---
Mm.	4	4	16	3	12
Nn.	4	4	16	4	16
Oo.	4	4	16	4	16
Pp.	4	4	16	3	12
Qq.	4	4	16	4	16
Rr.	4	4	16	4	16
Transition Requirements	---	---	---	---	---
Ss.	2	4	8	3	6
Tt.	2	4	8	3	6
Uu.	2	4	8	3	6
Subtotal	---	---	**120**	---	**106**
Evaluation Category	weight	**Netxar**		**Emagine IT**	
		score	points	score	points
Oral Presentations	---	---	---	---	---
Technical Total	---	---	**910**	---	**856**

The table below summarizes the technical scores obtained by each vendor and positions Netxar as the vendor with the highest overall technical score when adding all related focus areas while EIT positioned in second place. Moreover, and regarding vendors that did not pass the threshold, FIT managed to land the third position while Earthling finished in the fourth position. Furthermore, it is worth noting that in the case of Netxar and EIT the difference in overall scoring between the two is approximately six (6) percent. In addition, the difference between the highest scoring vendor (Netxar) and the lowest scoring vendor (Earthling) is approximately twenty-eight (28) percent.

Vendor	Technical Proposal Points
Netxar Cybersecurity Group	910
Emagine IT, Inc.	856
FTI Consulting, Inc.	809
Earthling Security, LLC	709

B – METHODOLOGY AND ANALYSIS OF COST PROPOSALS

After the technical evaluation phase ended, the Evaluation Committee proceeded to add the cost proposal criteria to the equation. Vendors needed to reach a score of 840 points or more in the technical evaluation phase to move onto to the following evaluation phase. Only Netxar and Emagine IT moved on to the cost evaluation phase. The highest possible score (200 points) was automatically given to the proposal with the lowest cost. The score provided to the other cost proposal was assigned using the following formula:

$$\frac{\text{lowest offeror's cost}}{\text{the offeror's cost being scored}} \quad \text{X} \quad \begin{matrix}\text{the maximum number of}\\ \text{cost points available}\end{matrix}$$

According to the vendors' cost proposals, scores are as follows:

Netxar Cybersecurity Group
$1,279,446.67/**$1,279,446.67** = 1 x 200 = **200**

Emagine IT, Inc.
$1,279,446.67/**$6,319,894.35** = .20 x 200 = **40**

The table below portraits the combined technical and cost evaluation final score results of the vendors which passed the threshold in ascending order. Netxar and EIT, which placed in first place and second place respectively, the difference in overall scoring between the two after adding cost evaluation scores is twenty-three-point nine (23.9) percent, which represents a significant margin.

Vendor	Technical	Cost	Total
Maximum Response Points	*1,200*	*200*	*1,400*
Emagine IT, Inc.	856	40	**896**
Netxar Cybersecurity Group	910	200	**1,110**

C – RECOMMENDATION

As provided by section 5.1 of the RFP, the Evaluation Committee shall make a recommendation for the contract to be awarded in favor of the vendor who receives the highest overall score of all eligible vendors, demonstrates that they meet all the mandatory specifications, reaches at least the minimum acceptable technical score, and was selected to move forward to the cost proposal evaluation phase. Having Netxar score the highest among all eligible vendors, the Evaluation Committee proceeds to recommend to the executive director that the *Buena Pro* be given to Netxar.

Both committees concluded that Netxar presented the best proposal overall. Consistently, this vendor was allocated with the highest scores across all categories of the technical evaluation except for the global criterion named *Vendor Qualifications and Experience* in its *References* subsection. In the rest of the global criterions, Netxar received the highest scores among all evaluated proposals.

The Technical Committee noted that Netxar provided more detailed information and in-depth explanations of the processes that the vendor would go through when conducting an assessment. As an example, Technical Committee members pointed to Netxar's description of the *Penetration Testing Tools and Techniques* category. Netxar's proposal described the *Proposed Tool*s, *Techniques* and *Risk Mitigations* for each instance, providing PRMP with a clear idea of how the project would be carried out and, particularly, mitigated in cases of not meeting compliance standards. Moreover, the Technical Committee members also noted how Netxar put heavy emphasis in describing *Targeted Training and Mentorship* for PRMP employees. According to their analysis, the rest of the evaluated proposals did not reach the same level of depth in their explanations or show how they would attend to PRMP's needs and requirements. Furthermore, Netxar's proposal showed to be significantly more economical than its closest competitor.

Netxar was the only vendor which addressed the continuity of responsibilities through an existing talent pool. This approach impressed the Technical Committee as it ensured the near undisrupted continuity of services in case of an employee leaving Netxar or being unavailable. Netxar was also very thorough with the explanation of SLAs monitoring and compliance and the security and privacy controls. Netxar provided a timeline which was detailed and represented the shortest viable option to complete assessments and ensure full compliance with RFP requirements.

On the other hand, according to the scoring tables provided by the Technical Committee, Emagine IT also presented a competitive proposal. This vendor was the only one with direct experience with CMS, as evidenced by the references provided. In addition, this vendor obtained enough points to move on to the cost evaluation phase and final analysis and even received the highest scores in the *Vendor Qualifications and Experience* category. It seems that the Technical Committee was highly impressed with the qualifications and experience of its personnel. Nevertheless, the Technical Committee members concluded that its proposal did not reach the level of description and detail provided by Netxar. Moreover, its cost is four hundred and ninety-four (494) percent higher than Netxar's, which arguably by itself represents a contractual hurdle.

After considering all factors, the Evaluation Committee concluded and feels confident that Netxar's proposal represents the best value and is the most advantageous for the Puerto Rico Medicaid Program (PRMP) and ISPCA needs. Accordingly, the Evaluation Committee recommends the PRMP executive director that the *Buena Pro* and subsequent contract be awarded to Netxar who received the highest overall score out of all eligible vendors and represents the lowest cost for the services to be provided.

PRMP DETERMINATION

Hereby it is notified that the Puerto Rico Medicaid Program executive director accepts the Evaluation Committee's recommendation to award the *Buena Pro* and subsequent contract in favor of Netxar Cybersecurity Group, the highest overall scoring vendor. Before the contract is awarded and signed, this Award Notification and Netxar's proposal must be verified by CMS. Once approved, Netxar shall submit all required documentation to the PRMP contract office, including a briefed proposal.

Be advised, as mentioned before, that Netxar must be registered with the *Registro Único de Proveedores de Servicios Profesionales (RUP)* from the Puerto Rico General Services Administration. Furthermore, no service shall be provided until a copy of the contract is filed with the Puerto Rico Office of the Comptroller.

On February 4, 2025 in San Juan, Puerto Rico.

Luz E. Cruz-Romero, MBA
Interim Executive Director
Puerto Rico Department of Health
Medicaid Program
T: (787) 765-2929, ext. 6700
E: luz.cruz@salud.pr.gov

RECONSIDERATION/JUDICIAL REVIEW – TERMS

According to 3 L.P.R.A. § 9655, the party adversely affected by a partial or final resolution or order may, within twenty (20) days from the date of filing in the records of the notification of the resolution or order, file a motion for reconsideration of the resolution or order. The agency must consider it within fifteen (15) days of the filing of said motion. If it rejects it outright or does not act within fifteen (15) days, the term to request judicial review will begin to count again from the date of notification of said denial or from the expiration of those fifteen (15) days, as the case may be. If a determination is made in its consideration, the term to request judicial review will begin to count from the date on which a copy of the notification of the agency's resolution definitively resolving the motion for reconsideration is filed in the records. Such resolution must be issued and filed in the records within ninety (90) days following the filing of the motion for reconsideration. If the agency grants the motion for reconsideration but fails to take any action in relation to the motion within ninety (90) days of its filing, it will lose jurisdiction over it and the term to request judicial review will begin to count from the expiration of said ninety (90) day term unless the agency, for just cause and within said ninety (90) days, extends the term to resolve for a period that will not exceed thirty (30) additional days.

If the filing date in the records of the copy of the notification of the order or resolution is different from the one submitted through ordinary mail or sent by electronic means of said notification, the term will be calculated from the date of submission through ordinary mail or by electronic means, as appropriate.

The party filing a motion for reconsideration must submit the original motion and two (2) copies either in person or by certified mail with return receipt to the Division of Administrative Hearings within the Legal Advisory Office of the Department of Health. The requesting party must also notify all other involved parties within the designated timeframe and include proof of this notification in the motion.

Submissions must be made as follows:

- **For personal delivery:** Monday through Friday (excluding holidays), between 8:00 a.m. and 4:30 p.m., at the following address:
  Department of Health, Legal Advisory Office - Division of Administrative Hearings
  1575 Avenida Ponce de León, Carr. 838, Km. 6.3,
  Bo. Monacillos, San Juan, Puerto Rico 00926.
- **Alternatively, by certified mail with return receipt, to the following postal address:**
  Legal Advisory Office - Division of Administrative Hearings
  Department of Health
  PO Box 70184
  San Juan, Puerto Rico 00936-8184.

According to 3 L.P.R.A. § 9672, a party adversely affected by an agency's final order or resolution, and who has exhausted all remedies provided by the agency or the appropriate appellate administrative body, may file a request for judicial review with the Court of Appeals within thirty (30) days. This period begins from either the date the notification of the agency's final order or resolution is filed in the records or the applicable date provided under 3 L.P.R.A. § 9655, when the time limit for requesting judicial review has been interrupted by the timely filing of a motion for reconsideration.

The party requesting judicial review must notify the agency and all other involved parties of the filing simultaneously or immediately after submitting the request to the Court of Appeals. Notification to the agency must be sent to the same addresses designated for the filing of motions for reconsideration. The notification of the filing submitted to the Court of Appeals must include all annexes.

If the filing date of the copy of the notification of the agency's final order or resolution in the records differs from the date it was deposited in the mail, the time period for requesting judicial review will be calculated from the date of deposit in the mail.

The judicial review provided herein shall be the exclusive remedy for reviewing the merits of an administrative decision, whether it is of an adjudicative nature or of an informal nature issued under 3 L.P.R.A. § 9601 *et al.*

The mere presentation of a motion for reconsideration or request for judicial review does not have the effect of preventing the Puerto Rico Medicaid Program (PRMP) from continuing with the procurement process within this request for proposals, unless otherwise determined by a court of law.

Finally, any party adversely affected by this *Award Notification* that decides to file a motion for reconsideration according to 3 L.P.R.A. § 9655 and eventually files a request for judicial review according to 3 L.P.R.A. § 9672, must comply with a *Notice Requirement* meaning that they have the obligation to inform other participating parties to ensure transparency, fairness, and due process.

I hereby certify that on February 4, 2025, copy of this *Award Notification* has been sent via electronic mail to all vendors to the addresses provided for legal notices in the submitted proposals:

Earthling Security, LLC Yusuf Ahmed 1818 Library Street, Suite 500 Reston, VA 20190 yaa@earthlingsecurity.com (202) 445-4959	**Netxar Cybersecurity Group** Jenny Feliz 954 Ponce de León Ave., Miramar Plaza, Ste. 501, San Juan, PR 00907 JENNY.FELIZ@NETXAR.COM (407) 219-1403
Emagine IT, Inc. Song Pak 909 Rose Avenue, Suite 900 North Bethesda, MD 20852 Song.Pak@eit2.com (443) 858-7906	**FTI Consulting, Inc.** Juan M. Montañez 555 12th St., Suite 700 Washington, DC 20004 juan.montanez@fticonsulting.com (202) 263-1449

Francisco moreno

Francisco Moreno Rodríguez
Acting Solicitation Coordinator
francisco.moreno@salud.pr.gov

Addendum
Scoring Area Captions

Id	Evaluation Items	Weight
	Vendor Qualifications and Experience	
A	Overview	50
B	Existing business relations with Puerto Rico	50
C	Business disputes	50
D	References	50
	Project Organization and Staffing	
	Initial Staffing Plan	
E	Describe how you will identify, recruit, and/or support any staff that may be required to perform the services of this RFP.	25
	Key Staff, Resumes, and References	
F	Provide the names of the proposed staff for the Security and Privacy Assessment services, including their qualifications, experience, and references. Describe how the proposed staff are best suited to meet the requirements of this RFP.	25
G	Describe how staffing/ resource needs or changes will be managed.	25
H	Describe how continuity of responsibilities will occur if a staff member needs to be replaced.	25
I	Describe how continuity responsibilities will occur should a staff member need to be replaced.	25
J	Describe the management structure, staff management process and how talent management support will be provided.	25
K	If a staff remediation plan is requested, describe how you will provide oversight and manage the remediation plan	25
L	Describe what you believe will be the most effective approach to managing the entire contract.	25
M	Describe how SLA will be monitored and reported.	25
N	Describe how the Communication Plan will include all stakeholders, your approach to stakeholder analysis, and how the communications will be managed.	25
O	Describe the process for change requests.	25
P	Describe your disaster recovery and business continuity plans. How quickly can you restore services?	25
	Approach to Scope of Work	
Narrative description how vendor will meet the following requirements:		
	System Functionalities and Capabilities	
Q	Describe your capabilities, knowledge, and experience performing the services described in the Statement of Work of this RFP.	25
R	Describe your capabilities, knowledge, and experience assisting state/federal agencies/organizations with the services requested in this RFP, particularly your understanding of the Medicaid program's/CMS specific security requirements, regulations, and documentation.	25
S	List your specific privacy and security experience and relevant auditing certifications, emphasizing those examples listed in the Executive Summary Section of this RFP	25
T	Describe your approach in developing an assessment strategy and procedure that will provide PRMP with a standardized approach for planning and resourcing the Security and Privacy Control Assessment (SCA) of its information systems and underlying components.	25
U	Describe your capabilities to perform security assessments that meet the CMS Framework for the Independent Assessment of Security and Privacy Controls Version 3.1 Final, dated June 16, 2022, the MARS-E (or ARCAMPE) requirements and more stringent security certifications.	25
V	Describe your capabilities, knowledge, and experience in determining whether the security and privacy controls are implemented correctly, operate as intended, and produce the desired outcomes for meeting the security and privacy requirements of the application(s) and/or system(s).	25
W	Describe how you can rapidly identify compliance gaps and support PRMP efforts to achieve MARS-E (or ARC-AMPE) compliance.	25
X	Describe the overall approach and plan for assessing, among others, PRMP's systems, applications, programs, and processes, including an illustration of the timeline with key activities, deliverables, and milestones that include the anticipated resource allocations that will support the proposed plan	25

Y	Describe how you can ensure PRMP compliance with the latest applicable regulatory guidance if any referenced standards or publications are updated (e.g., MARS-E, NIST, etc.).	25
Z	Describe your approach toward collaborating with PRDoH/PRMP staff to ensure compliance with CMS and other applicable standards.	25
Aa	Describe your approach and/or methodology to reduce the risks posed to a particular application or system and protect all sensitive information, including assigning business and system risk levels following the methodology outlined in NIST Special Publication 800-30, Rev. 1, Guide for Conducting Risk Assessments, and following CMS required levels of granularity.	25
Bb	Describe your approach to using recognized industry standard frameworks for evaluating privacy and security controls that can allow PRDoH/PRMP to demonstrate to CMS the compliance of its systems with MARS-E 2.2 requirements (for example, not limited to ISO 27001:2022 or NIST 800-53 Moderate).	25
Cc	Provide details of the penetration testing tools and techniques that will be proposed to simulate vulnerabilities. Note: The proposed tools that might pose a risk to the computing environment must be identified in the SAP	25
Dd	Describe your approach to ensure that the impartial and unbiased nature of the assessment processes will be preserved.	25
	Deliverables	
Ee	Work Plan with tasks, resources, and timeframe for completing the assessment(s) and providing all the required reports/deliverables.	25
Ff	Security and Privacy Assessment Plan (SAP).	25
Gg	Security Assessment Workbook (SAW).	25
Hh	Security Assessment Report (SAR).	25
Ii	Plan of Actions & Milestones (POA&M).	25
Jj	Annual Security and Privacy Attestation Report.	25
Kk	Security Assessment Closeout Report.	25
Ll	Preliminary and Final Reports describing the work performed or completion of tasks.	25
	Privacy and Security Requirements	
Mm	Describe how you will ensure all staff, including subcontractors, will protect the confidentiality and integrity of sensitive data.	20
Nn	Describe how compliance with the HIPAA Privacy and Security Rules will be assessed under the services and requirements of this RFP.	20
Oo	Describe how you will ensure the "valid need to know" requirement when requesting access to any information related to the security and privacy of PRDoH/PRMP's systems.	20
Pp	Please outline the risk assessment and vulnerability management approach in the context of Medicaid data.	20
Qq	How do you keep up to date with emerging threats and vulnerabilities in the healthcare sector, especially those that may impact the confidentiality, integrity, or availability of the PRMP's information?	20
Rr	Describe how you will train staff to ensure they understand and observe requirements related to any confidentiality requirement in this RFP.	20
	Transition Requirements	
Ss	Describe the activities and methodology to be included in a Transition Plan if PRMP determines this as necessary while providing the services under this RFP.	10
Tt	Describe the staff (if any) responsible for the transition.	10
Uu	Describe your approach to maintaining a Documentation Repository during the requested transition.	10