October 21, 2024

Vendor Questions and Answers

Number	Questions	Answers
1	Can you provide an inventory of all systems and applications that will require assessment (e.g., MMIS, E&E, EDW, HIE)?	This RFP currently includes MMIS, E&E (Mediti3G), and EDW with HIE coming online soon. The expectation is that this RFP will include at least annual audits of these systems plus support for any certification efforts for new releases.
2	Are there any future or planned implementations that we should include in our scope (e.g., EVV, TPL, AVS)?	There are current plans for additional systems coming online outside of the MMIS, E&E, EDW, and HIE. TPL, AVS and EVV will come online in the future and should be included in the scope. Additional systems in the future would be managed by our CR process.
3	Are there any specific system integrations or interfaces we should be aware of, particularly with federal systems (e.g., CMS Data Services Hub)?	The E&E system currently connects to the Federal (CMS) Data Services HUB and PR State Agencies via the PR State Hub. The HIE system connects with PR agencies, MCOs, labs, and other local health agencies. PR does not interact with SSN nor IRS services.
4	Are there any updates or deviations from the MARS-E 2.2 or NIST SP 800-53 controls that PRMP expects us to follow?	Currently, MARS-E 2.2 (Based on NIST SP 800-53 r4 and FedRAMP) is the Compliance Standard we use. This will be updated to the ARC-AMPE (Based on NIST 800-53 r5 and FedRAMP) as soon as it is released in the Oct/Nov 2024 timeframe. Once released, PRMP will expect future audits to conform with this standard and should be part of this RFP.
5	Does PRMP have any existing security or privacy policies and procedures that we should review as part of the assessment?	Yes, PRMP as well as our vendor partners maintain security and privacy policies which are outlined in each system SSPP. The assessments will follow CMS audit guidelines which include documentation review, interviews, and testing requirements.
6	Has PRMP undergone previous security or privacy assessments, and if so, can we review the findings and reports from these assessments?	The MMIS and E&E systems have undergone at least three (3) years of previous audits and assessments. This assessment can be shared with the selected vendor once contracts have been awarded.
7	Are there any state-specific privacy laws or standards, in addition to HIPAA, that we must comply with?	There are only minimal State-Specific Laws and/or standards in addition to HIPAA and CMS MARS-E / ARC-AMPE. These focus on eSignature and Document Retention/Destruction requirements.

Vendor Questions and Answers

8	Are there any specific tools or technologies preferred by PRMP for conducting vulnerability scanning, penetration testing, or configuration assessments?	PRMP does not mandate nor recommend specific tools. However, we do require the selected tools of the vendor to be able to cover all aspects of the Audit/Assessment requirements outlined by CMS audit requirements.
9	Will we have direct access to system environments, or will testing be conducted in a controlled environment (e.g., test accounts without access to sensitive data)?	Temporary access and credentials will be provided by the individual systems as needed to complete the assessments. The assessments will be conducted against production systems where available. Preproduction system testing will be completed against UAT environments which will mirror production systems. Once the system is in production, future assessments will be conducted against production environments. To access these environments, vendors will need to comply with PRMP access requirements including, but not limited to, HIPAA training, BAA, ISA, and/or CMAs.
10	Can PRMP provide a list of existing security controls, firewalls, routers, and configurations that will be part of the assessment?	Details, SSPP, and supporting documentation will be provided to the selected vendor after contract award. MMIS, E&E, and HIE systems are hosted in AWS or Azure Government Cloud environments and use approved technologies within those environments.
11	What documentation will be provided to the vendor (e.g., network diagrams, system security plans, user manuals, prior audit reports)?	Each system maintains aSSPP which outlines all relevant documentation. Any documentation listed within the SSPP will be provided to support the assessment. This includes the Plan of Action and Milestones, and previous audit reports as needed to complete future assessments.
12	Are there any specific deliverables formats PRMP prefers (e.g., Excel for Plan of Action & Milestones, PDF for Security Assessment Report)?	All deliverables will follow the CMS required templates including the POAM, SAP, SAR, SAW, ISRA, and Raw vulnerability and penetration testing results from the vendors tools.
13	Can we get an estimated number of stakeholders (e.g., business owners, system administrators) we should interview during the assessment?	The vendor can identify stakeholders whom they would like to interview based on their evaluation of the SSPP. Previous audits have included five to ten (5-10) individuals per system.
14	Are there any PRMP locations we need to visit beyond the Central Office, such as regional Medicaid offices or data centers?	Systems are maintained in cloud locations which are covered by FedRAMP certifications. Activities within PRMP are primarily operated from the World Plaza Offices where PRMP is located. Regional offices and partner locations within Puerto Rico can be made available to the vendor for appropriate inspection as requested.

Vendor Questions and Answers

15	Are there any logistical considerations we should be aware of regarding on-site assessments (e.g., facilities access, security protocols, COVID-19 restrictions)?	Security Protocols outlined in PRMP policies must be followed for on-site visits. This includes being chaperoned by State staff or designated authorized personnel. All individuals must be able to provide Identification (Photo), have provided HIPAA compliant training documentation, and signed appropriate BAA/NDA documentation. There are currently no COVID-19 restrictions in place at the time of this RFP. However, PR continues to follow Federal and State Health Emergency requirements if they are required.
16	What is the expected timeline for key milestones, such as the initial kick-off meeting, assessment phases, and submission of deliverables?	The vendor should work with PRMP CISO to establish a timeline for completion of the assessments. Each system has delivery milestones, but an SAP should be submitted by the awarded vendor to ensure the delivery date can be met. CMS does maintain 30- and 90-day submission requirements of key documents. SAP must be submitted at least ninety (90) days prior to delivery, and SAR must be submitted at least thirty (30) days prior to expiration of current ATC dates. These should be considered with developing an assessment schedule.
17	Are there any hard deadlines related to federal reporting (e.g., CMS compliance) that we need to meet?	The E&E system requires Authority To Connect (ATC) annual assessments to be completed by April each year. Other systems are based on release dates.
18	Can PRMP provide an overview of high-risk areas or known vulnerabilities in its current systems that the vendor should prioritize?	Currently PRMP does not have any High-Risk areas or known vulnerabilities in current systems. The POAM is tracking several medium and low priority items. This document with expected resolution dates can be provided to the selected vendor after contract award.
19	Are there any ongoing or planned remediation efforts for known security gaps that we should be aware of?	All planned remediation efforts are outlined in the POAM.
20	Separately, we have an initial question related to Section 1.1 of the RFP document. For context, the vendor is an accredited FedRAMP & StateRAMP 3PAO, meeting several of PRMP's requirements with that representation alone. The vendor is also an active contractor supporting the Center for Medicare and Medicaid Services (CMS) and frequently interacts with documentation related to MARS-E and ARC-AMPE certification for entities involved in the program. The vendor’s 3PAO assessment team and the team supporting CMS do not interact or overlap.	PRMP did not find any problems with interacting with the vendor and being able to submit a proposal for this RFP.

Vendor Questions and Answers

	The vendor would like PRMP to confirm that, given the context provided above, it can be considered an impartial & unbiased vendor that can move forward through this RFP process and maintain the independence required for this scope of work. The vendor is not aware of any active or previous contractual relationships with PRDoH-PRMP.	
21	En términos de futuras y/o proyectadas aplicaciones que PRMP y/o implementaciones de sistemas como **EDW, HIE, EVV, TPL y AVS**, podría identificar cuales de estas aplicaciones o sistemas están implementadas hoy día o cuando serían implementas? In terms of future and/or projected PRMP applications and/or implementations of systems such as EDW, HIE, EVV, TPL and AVS, could you identify which of these applications or systems are implemented today or when they would be implemented?	See question 2.
22	For level-of-effort estimation and cost proposal preparation, for systems not currently in production can you provide estimates of when these systems are expected to go into production?	
23	Have any assessments been conducted already? If so, can you provide details on the systems and sites assessed, when the assessments were completed, and the entity(ies) that conducted the assessments?	See question 6. Aside from those mentioned in question 6, no other assessments have been conducted.
24	If the firm responding to the RFP includes subcontractors in its proposal, can the experience and credentials of the firm and its subcontractors be counted towards meeting the requirements in the RFP (mandatory and other requirements)?	No, the main vendor is the one who needs to comply with RFP requirements. Moreover, the subcontractor needs to comply with its own requirements (References).
25	Are there caps on the annual budgets for these assessment services? If so, for cost proposal preparation purposes can the PRMP share details on the caps?	PRMP does not maintain CAPs on the annual budget for these assessments. However, cost is a key consideration when selecting a vendor.
26	Who is the incumbent, and can the Government please provide the contract information, including the value of the current contract?	No current incumbent.

Vendor Questions and Answers

27	Would the Government please provide the Word version of the solicitation in order for Offerors to complete each Appendix in the required format?	Yes, a word version has been posted along with the answers to this Q&A. Vendors should note that the word version should be used only for completing the document and no changes to format, document order or any other change beyond filling information is allowed.
28	Can the Government please confirm Offerors are only required to acknowledge Appendix 4: Proforma Contract Draft and are not required to submit a completed version?	Vendors are only required to acknowledge Appendix 4, and not required to submit a completed version.
29	We noted a couple of inconsistencies between the instructions provided in Table 2: Expected Proposal Sections and Content Structure and the information provided in the attachments: a. The title of Attachment B includes a “Brief Proposal Summary,” which appears to include a requirement for Offerors to include a “Brief Proposal Summary” within Attachment B: Title Page, Vendor Information, Brief Proposal Summary, Executive Summary, Subcontractor Letters, and Table of Contents. However, there is not a section titled “Brief Proposal Summary” between the “Vendor Information” and the “Executive Summary” sections. Can the Government please clarify? b. For Attachment F: Response to Statement of Work, the table shows the order of sections as: Scope and Requirements Management and Expertise Approach, Security and Privacy Assessment Knowledge and Experience, Deliverables; Staffing Approach; Management Approach; Security Approach; and Transition Approach. However, in the actual attachment, the order is Vendor Qualifications and Experience; Scope and Requirements; Staffing, Project Organization, and Management; Privacy and Security Requirements; and Transition Requirements. Can the Government please confirm whether Offerors should follow the order presented in Table 2, or only provide the information required within the actual Attachment?	A. Vendors should place the “Brief Proposal Summary” between “Vendor Information” and the “Executive Summary”. B. Vendor should only provide the information required within the actual attachment.

Vendor Questions and Answers

30	Can the Government clarify if mailing printed proposals is a requirement and considered mandatory for compliance?	Yes, mailing or otherwise delivering the proposals physically is a requirement mandatory for compliance. This applies to the printed proposals and the USBs containing the proposals and their appendices digitally.
31	Can the Government provide the number of staff and the Labor Category mix for the incumbent staff currently performing the work?	There is no current incumbent vendor for this project, as such there is no incumbent staff.
32	Can the Government please provide a breakdown of the anticipated level of effort (LOE), including anticipated labor categories and the anticipated manhours per year?	The vendor should use their experience to determine the estimated level of effort. CMS does require document evaluation, personnel interviews, and system testing to be completed as part of audits. Historically, these activities have been spread over 2-3 months to provide ample time for response and review to audit activities. While these audits do span several months, these activities are not Full-Time for the entire duration, rather the span covers PRMP and out vendors time to respond and support the audit effort while continuing to perform their daily activities with minimum impact.
33	Can the Government clarify the requirement for the number of Key Staff resumes?	Each member of the key staff should provide one resume and two references.
34	Are we correct in the understanding that in addition to providing a resume for each key person, we also need to separately submit two (2) references where they have performed similar work?	The RFP states: “The vendor should provide references for each proposed key staff member. The reference should be able to confirm that the staff has successfully demonstrated performing tasks commensurate to those they will perform for the services under this RFP. PRMP prefers two (2) different references to demonstrate experience; however, this is not a requirement.” As such the vendor should separately submit two references for each key staff the vendor proposes, utilizing the template provided.
35	Can the Government please confirm the work will be performed virtually with the exception of assessments, which are required to be performed on-site?	PRMP allows for remote / virtual work in the completion of these activities where possible. Some activities, such as site inspections, do require on-site presence. PRMP may require in person representation for high profile meetings. If such a need presents, PRMP will provide ample notification to schedule required travel to a PRMP location. This normally does not occur more than once or twice per year.
36	How many systems are in scope? How many boundaries?	Currently, PRMP has 2 production system boundaries (MEDITI3G / MMIS), 1 preproduction system boundary (HIE), and 1 planned boundary (DW). Future systems does not have a set release date at this time.

Vendor Questions and Answers

37	Please provide the number of components within the system boundary. Specifically, provide the number of: a. Servers b. Webservers c. Domain Controllers d. Workstations e. Firewalls f. Routers g. Load Balancers h. Switches i. Databases	This information will be solicited and provided in a timely manner.
38	Where is the information system located?	MMIS is hosted in AWS Government Cloud, HIE and MEDITI3G are hosted in Azure Government Cloud.
39	How many data centers are the systems housed in? Where are they located?	Currently, all systems in scope for this RFP are hosted in the Cloud.
40	Will vulnerability and compliance scan results be provided by the Puerto Rico Department of Health, or will the vendor be required to procure and install scanning software to perform the scans?	The vendor is responsible for conducting vulnerability and penetration testing as part of this RFP. CMS requires independent testing as part of the audit process. The vendor is responsible for selecting and providing software needed to conduct these tests. These tools are for vendor use only, PRMP does not anticipate procuring, installing, nor operating these tools on an ongoing basis.
41	If a cloud environment is in scope, what type of cloud service is being utilized? (IaaS, PaaS)	The Cloud environments are primarily IaaS. Some platform capabilities such as firewalls and security log audit may be used.
42	Do the application(s) reside within a cloud environment? If so, which Cloud Service Provider(s) are being utilized?	See Question 38.
43	Can testing be conducted remotely? If so, is it possible to conduct the testing from a contractor's facility?	See Question 35.
44	Section 2.2 of the RFP states that there is an initial term of two years, however, the pricing matrix shows that year 2 through 5 are all option years. Can you please clarify?	The RFP states “PRMP intends to award one (1) multi-term contract, with an initial term of two (2) years, and three (3) one-year optional extensions.” As such, vendors must fill in their cost proposals with the second year as part of the base term of the contract.

Vendor Questions and Answers

45	After the initial year, will the annual assessments consist of an assessment of all security controls, or will they be a subset of controls?	These audits follow CMS guidelines. Typically, this follows approximately 1/3 of the security controls where 100% of controls are completed every 3 years. However, this can be modified at CMS request depending on Security Impact Assessments outlining changes performed on the environment or system.
46	How many physical locations are expected to be visited as a part of this assessment, and where are they all located?	The RFP states "The PRMP Central Office is located at: 268 Luis Muñoz Rivera Ave. World Plaza – 5th Floor (Suite 501) San Juan, Puerto Rico 00918. However, the vendor shall consider within the proposal on-site visits to other locations such as OIAT (PRDoH), ASES, and Medicaid offices2 (Regionals) around the Island to perform the services requested under this RFP." The regional offices are listed in the RFP and are located as follows, "Regions - Arecibo (offices located at Barceloneta, Camuy, Florida, Hatillo, Lares, Manatí, Morovis, Orocovis, Quebradillas, and Utuado), Fajardo (offices located at Fajardo, Humacao, Naguabo, Rio Grande, Vieques, and Yabucoa), Bayamón (offices located at Cantón Mall, HURRA, Cataño, Corozal, Dorado, Naranjito, Toa Baja and Vega Alta), Mayagüez (offices located at Aguada, Aguadilla, Cabo Rojo, Isabela, Lajas, Las Marías, Maricao, Moca, Rincón, San Sebastián and Mayagüez), Caguas (offices located at Caguas, Aibonito, Aguas Buenas, Cayey, Cidra, Comerio, Gurabo, Las Piedras, and San Lorenzo), Metropolitana (offices located at Canóvanas, Carolina, Guaynabo, Loíza, Santurce, Rio Piedras and Trujillo Alto), and Ponce (offices located at Coamo, Arroyo, Adjuntas, Guánica, Guayama, Guayanilla, Jayuya, Patillas, Peñuelas, Salinas, Santa Isabel, Villalba, Yauco and Ponce)."
47	May offerors remove the instructional information from each of the Attachments in their proposal response (i.e. "The vendor should include a title page stating the vendor's intent to bid for this RFP. The vendor's response should include…")?	The vendors may remove the instructional information; however, vendors may not remove the attachment identifiers.
48	Can you provide more details on the specific goals and priorities of the Independent Security and Privacy Control Assessment, for example, are there particular areas of concern or high-risk systems you would like us to focus on?	The primary goal of this RFP is to maintain compliance with security objectives outlined in the PRMP security program and CMS oversight requirements. There are not specific high-risk areas of concern.
49	Are there any legacy systems or specific applications that have been challenging to secure in the past that we should be aware of?	No, all systems have been in compliance with requirements. While every audit usually finds areas of improvement, there have been no key security concerns at this point.

Vendor Questions and Answers

50	What is the current status of compliance with MARS-E and other relevant standards like NIST SP 800-53A for your existing systems?	All production systems are in compliance with CMS MARS-E 2.2 expectations. There are open medium and low priority items on the Plan of Action and Milestones. This document can be shared with the selected vendor after contract.
51	Are there any recent audits or assessments that identified vulnerabilities or gaps in your security and privacy controls? If so, can you share the findings or areas for improvement?	See Question 6.
52	Beyond CMS and NIST requirements, are there any specific federal or local regulations that we need to consider during our assessment?	See Question 7.
53	Are there any upcoming changes in regulatory requirements that you anticipate could impact the scope of the assessment or the systems we will be evaluating?	See Question 4.
54	What level of risk (low, medium, high) is considered acceptable for the systems under review, and how do you define the criteria for each risk level?	PRMP follows CMS audit requirements outlined in CMS's Minimum Acceptable Risk and Safeguards for Exchanges version 2.2. Please note this will be updated to the CMS Acceptable Risk Controls for ACA, Medicaid, and Provider Entities (ARC-AMPE) when released later this year.
55	What security tools or technologies (e.g., SIEM systems, firewalls, vulnerability scanners) are currently in place for monitoring and protecting your IT environment?	See Question 37.
56	Are there specific tools or solutions that you prefer us to use during vulnerability scanning and penetration testing?	See Question 8.
57	What is your current incident response process, and how are cybersecurity incidents typically handled within your organization?	PRMP maintains an Enterprise Incident Response plan which will be provided to the selected vendor. During the initial kick-off meeting after contract, we will provide specific details on reporting suspected and/or confirmed incidents. This includes collecting and preserving supporting evidence.
58	How would you like our team to communicate and coordinate with your incident response team in case a critical vulnerability or breach is detected during the assessment?	See Question 57.
59	Are there particular data sensitivity concerns (e.g., Personally Identifiable Information (PII), Protected Health Information (PHI), Federal Tax Information (FTI)) that we should be aware of during testing?	PRMP maintains PII and PHI within the system boundaries of the systems outlined by this RFP scope.

Vendor Questions and Answers

60	What are the specific data handling and privacy policies we need to follow to ensure compliance with HIPAA and other relevant privacy regulations?	PRMP will provide a Computer Matching Agreement, Data Use Agreement, and/or Business Associate Agreement along with the contract for this RFP. At a minimum, these agreements will outline: • Access Control requirements for connecting testing tools to PRMP environments • Training requirements for HIPAA data handling and privacy expectations • Configuration requirements for encryption between environments • Media Protection requirements for collection, storage, and destruction of PRMP data • Identity Requirements for accessing PRMP systems Relevant Policies and Procedures will be provided upon contract.
61	What level of access will be provided to our team for conducting the assessment (e.g., network-level access, administrator-level access)?	PRMP and our partner vendors will work with the selected vendor to establish connection and access requirements outlined by the selected vendors Security Audit Plan (SAP). Historically, PRMP has provided System and Network level access. The Selected vendor will have access to PRMP administrators for advanced access needs. However, this level of access is typically restricted.
62	Are there specific physical locations or data centers where on-site visits are required, and what are the protocols for gaining access to these facilities?	See Question 46. All on-site visits are to operational locations, all data centers are cloud based
63	Who are the primary stakeholders within your organization that we will be collaborating with during this assessment, and what are their roles?	The Primary Stakeholder is the PRMP Director and CISO. Other key resources will be available as needed based on the system being audited.
64	How frequently would you like to receive status updates or progress reports, and in what format (e.g., weekly meetings, written reports)?	This should be outlined in the SAP provided by the selected vendor. However, historically, we have meet weekly during the audit window.
65	Are there any specific deadlines or project milestones that we need to align with, such as upcoming audits or compliance reviews?	See Question 17.
66	Will your internal teams (e.g., IT, security, compliance) be available to support our assessment activities, or are there any resource constraints we should be aware of?	Yes, PRMP will ensure all resources required to participate in the audit process are available to the selected vendor as needed to complete the audit in alignment with the provided SAP.
67	What are your expectations regarding the remediation of identified vulnerabilities? Should we provide detailed guidance and support for remediation efforts?	All identified vulnerabilities should follow the CMS Security Audit Workbook and Security Audit Report templates. This does include providing recommended guidance on remediation. System Implementation and Support teams will be responsible for Remediation efforts.

Vendor Questions and Answers

68	Would you prefer a phased approach for implementing security improvements, or do you expect all vulnerabilities to be addressed immediately?	This RFP is for the audit and reporting of vulnerabilities. These should include recommendations for remediation. However, PRMP maintains contracts with system vendors who will be responsible for implementation and resolutions of vulnerability fixes.
69	How would you like the final assessment results to be presented (e.g., executive summaries, detailed technical reports, risk matrices)?	See Question 12.
70	Are there any specific formats or templates you require for the Security Assessment Plan (SAP), Security Assessment Report (SAR), and other deliverables?	See Question 12.
71	Are you looking for a long-term partnership to support continuous monitoring and updates to the security posture, or is this engagement intended to be a one-time assessment? Document implies initial 2yr term with potential 1yr extensions.	This RFP is for the Annual Audit requirements for each system outlined.
72	How do you envision our role in supporting future compliance efforts and maintaining the security of your evolving IT environment?	CMS mandates independent 3rd party audits. These audits should identify potential vulnerabilities and/or compliance risks outlined by CMS based on the system SSPP and supporting documentation on an annual basis. This RFP does not involve remediation nor enhancement of the PRMP Security Program nor its environments. Involvement in the enhancement would negate the independent status of the selected vendor.
73	What have been the biggest challenges in achieving and maintaining compliance with CMS and other security standards in the past?	PRMP has achieved compliance with CMS sense adopting the MARS-E 2.2 standard.
74	Are there specific pain points or areas where previous assessments have fallen short, and how can we ensure our approach addresses these issues effectively?	None at this time.
75	How do you handle changes or updates to your IT infrastructure, and how would you like us to accommodate any changes that occur during the assessment process?	PRMP has documented Change Request Process that is followed for any IT Infrastructure and/or system updates. While PRMP does not anticipate any changes to the infrastructure in support of this RFP, we do recognize that some support activities such as execution of scripts against network or database resources may be required. These activities should be outlined in the SAP. The SAP will be presented to the Chance Control board for review and approval following this process.

Vendor Questions and Answers

76	Is there a preferred method for communicating changes that may impact the scope of our assessment or the risk landscape?	The SAP should outline all aspects for the system audit being conducted. This should include any required support activities. If there is a change to this SAP, then this should be discussed with the CISO and documented in an updated SAP document.