PA Compact Data System RFP Vendor Questions & Responses

Accessibility

1. Accessibility Standards: Is WCAG 2.1 AA compliance sufficient, or will Section 508 requirements also apply?

   1.1. *If not specified in the RFP, then it will be determined through the agile process.*

2. Are there specific accessibility testing tools preferred by the Commission to ensure WCAG 2.1 AA compliance (e.g., Pa11y, Axe)?

   2.1. *No*.

Administrative & Submission

3. Can you confirm whether proposals must be submitted in a single PDF file or if technical and price proposals may be submitted as separate attachments?

   3.1. *Proposals must be submitted as one PDF, plus an Excel workbook with the vendor's price proposal. See RFP section 6.2* – Price Submissions.

4. Are vendors required to submit a completed W-9 or other registration forms with the proposal?

   4.1. *No.*

5. Is there any page limit for resumes included in the staffing plan beyond the one-page limit for key personnel?

   5.1. *No.*

6. Will answers to vendor questions be posted publicly on the PA Compact website, or shared only with participating offerors?

   6.1. *Answers will be posted publicly on the PA Compact website, www.pacompact.org*.

Authentication & Authorization

7. Social Logins: Are social logins (e.g., Google, Facebook) explicitly out of scope?

   7.1. *No.*

Budget, Contract, & Funding

8. The ceiling price is $270,000. Is the Commission open to phased proposals that outline base and optional feature sets within that ceiling?

8.1. *Yes.*

9. Will travel expenses (if needed) be reimbursed separately or must they be included in the loaded hourly rate? Does the $270,000 ceiling include travel expenses, or are those covered separately?

9.1. *Travel is not required nor anticipated. If travel is necessary, then it will be reimbursed. Expenses for travel should not be included in the loaded hourly rate.*

10. Are payment milestones tied to deliverables (e.g., sprints completed, code accepted) or billed monthly based on hours worked?

10.1. *Payments will be billed monthly based on hours worked.*

11. If the project is extended or additional funding is secured (per the Appendix), will there be a new solicitation or modification of this contract?

11.1. *It is anticipated that the existing contract will be modified.*

12. Is there funding available for enhancements beyond the initial scope during the base year or future phases?

12.1. *Depending on the commission's finances and needs, funding would be pursued for additional system needs. At least maintenance services will be needed.*

13. Contract Structure: Would the Commission consider a phased fixed-fee MVP (with options) instead of time-and-materials for better budget and scope control?

13.1. *No.*

14. Future Roadmap: Should proposals include an optional roadmap for features beyond the MVP?

14.1. *No.*

15. Scope vs. Budget: Given the $270,000 NTE and a team of 4–9, what scope would be considered successful?

15.1. *A system that enables the commission to issue compact privileges, and other features as developed through the agile process.*

Hosting & Environment

16. Existing Infrastructure: Does the Commission already have a cloud environment, or will the contractor need to provision and configure one?

16.1. *The contractor must provision and configure a cloud environment.*

17. Will the commission require cloud hosting? Who will be responsible for managing it? Paying for it?

17.1. *Yes, the commission would require and pay for cloud hosting, as section 5.1 of RFP specifies the need for a cloud environment. There may be a need for the data system vendor to manage the cloud environment on short term basis, which would be compensated for as part of the contract.*

18. Can the Commission clarify whether the contractor will be responsible for initial hosting and deployment of the data system or if hosting will be managed by the Commission or a third-party provider?

18.1. *The contractor will be responsible for deployment and initial hosting of the data system.*

19. What technologies will be used to host the environment?

19.1. *The vendor should propose the solution*.

20. Cloud Compliance: Must production run in a FedRAMP-authorized environment (e.g., AWS GovCloud, Azure Government), or is a commercial cloud acceptable? Are there any state-specific data residency constraints?

20.1. *Standard, commercial grade is acceptable. Data residency constraints will be determined through the agile process.*

21. Environment Setup: What environments are expected (development, test, staging, production)? What are the required RTO/RPO targets and disaster recovery expectations?

21.1. *At least development, test, and production environments are expected to be needed. The commission has not yet established required RTO/RPO targets or disaster recovery expectations.*

22. Is the contractor expected to develop APIs for external state systems or only for internal Commission use?

22.1. *There is no expectation for external state system development. There will likely be a need for API capability for internal commission use and ensuring ease of interface between the commission data system and external state systems.*

Integrations & Data Exchange

23. Jurisprudence Exams: What data signals (e.g., pass/fail, score, timestamp) and APIs exist for exam verification?

23.1. *This will be determined through the agile process, but it will likely be an attestation.*

24. Standards & Protocols: Are there preferred data exchange standards (e.g., REST/JSON, XML, SFTP batch, FHIR-like resources)?

24.1. *The commission does not have preferred data exchange standards. They will be determined through the agile process.*

Legal & Policy Nuances

25. Foreign Government Interests: Are there specific certifications or attestations required at proposal time regarding foreign government interests?

25.1. *Disclosures will be needed at time of proposal pursuant to RFP section 5.3 –* Disclosure of Foreign Government Interests.

26. Records Management: Are there state or federal requirements for retention, FOIA/public records, or legal hold that the solution must support?

26.1. *None currently unless further developed by commission by rule.*

Open Source & Licensing

27. SBOM & License Policy: Will the Commission accept a third-party Software Bill of Materials (SBOM) (e.g., SPDX, CycloneDX) and a defined license policy (allow/deny/exception)?

27.1. *These must be disclosed, and the commission may decide to include.*

28. Data Ownership & Reuse: Data is Commission-owned—can we confirm that generic components (excluding data) may be reused in other open-source projects?

28.1. *Yes, per the open-source license that is assigned.*

29. Repository Operating Model: Can you clarify expectations for repository management (e.g., GitHub organization, branch protection rules, pull request review process, issue tracking conventions)?

29.1. *This should be proposed by the vendor*.

30. Preferred Licenses: Are there preferred open-source licenses (e.g., MIT, Apache-2.0) and any restrictions on copyleft licenses?

30.1. *There are currently no preferred open-source licenses. This will be determined later through the agile process*.

31. Front-End Guide Links: The RFP references broken links to the 18F Front-End Guide—would https://designsystem.digital.gov/ be an acceptable replacement?

31.1. *The archived 18F Front-End Guide can be found here*.

32. Is the entire code expected to be open source? Or some parts (specify please) only? What are the reasons for having open-source code? How does this affect a vendor's existing libraries, if they were to be used in development?

32.1. *Yes, it is the commission's preference that the code by open source, but a vendor may disclose in its proposal and later obtain permission from the PA Compact Commission to deliver software under this task order that incorporates software that is not free and open source. The commission has elected to require open source because it assists with state onboarding, provides greater autonomy and ownership as compared to proprietary systems, and avoids licensing fees. The Compact Commission retains the right to choose a vendor based on all available information and any contracts issued would be between the Commission and the vendor. Though the commission cannot speak to any vendor's existing libraries, any proprietary code approved for use in the data system would remain proprietary*.

33. The RFP specifies an open-source release requirement. Can you clarify if the Commission has a preferred GitHub organization or repository structure for the project?

33.1. *The commission does not have a preferred Github repository or repository structure*.

34. Can you please confirm whether the open-source requirement is mandatory? If so, would the Commission allow the source code to be shared exclusively with the PA Compact Commission under a Non-Disclosure Agreement (NDA), rather than being made publicly available?

34.1. *The commission's preference is open source; however, if vendors choose to include code that is not open source in their project proposal, they must disclose it in the proposal*.

35. Are there any restrictions on the use of existing open-source frameworks or libraries (e.g., Angular, React, Django, Node.js) if they comply with the Open-Source Definition?

35.1. *No*.

Operations & Support

36. On-Call & SLAs: Who is responsible for on-call coverage, uptime SLOs, support hours, and bug resolution SLAs during the contract and after its completion?

36.1. *This will be determined later in a maintenance contract*.

37. Observability Requirements: What level of observability is expected (e.g., logs, metrics, traces)? Are error budgets and runbooks required?

37.1. *The commission has not yet established these requirements*.

Quality & Testing

38. Security Tooling: The RFP lists tools like Snyk, npm audit, and OWASP ZAP, which are JavaScript-oriented. Can tooling be aligned to the chosen technology stack (e.g., Bandit, Trivy, Semgrep)?

38.1. *Yes*.

39. Test Coverage: Does the 90% coverage requirement refer to line, branch, or function coverage? Should generated code, database migrations, and infrastructure scripts be excluded?

39.1. *The commission will discuss this with the chosen vendor*.

40. Performance Testing: Are performance tests required? If so, are there specific targets for throughput, latency, or scalability (e.g., public search performance, peak renewal periods)?

40.1. *The commission has not yet established requirements for performance testing.*

41. Error Tolerance: The target is WCAG 2.1 AA with zero automated and manual errors—can you clarify what constitutes a "manual error" and whether minor deviations are acceptable during iterative development?

41.1. *WCAG 2.1 AA specifies strict guidelines for accessibility, some of which can be verified automatically, but others require manual testing because they cannot be automated. The QASP standard refers to errors reported in manual testing. Deviations would not be acceptable.*

Scope, Phasing, Technical Approach, Deliverables, & MVP

42. Will individual States require customer support post development? Would the PA Compact Commission require from the vendor maintenance/customer support post development? What's the budget for it?

42.1. *The current budget is for the development of the system. Customer support and maintenance are envisioned to be needed as part of either a new or continued contract. The budget has not been determined at this time*.

43. Will APIs be needed? How many? What kind?

43.1. *API functionality is an anticipated need but will be defined further through the agile development process. How many and what kind will also be determined through the development process*.

44. Will the vendor need to integrate with a payment processor? Who will create and manage the payment processing solution within the PA Compact?

44.1. *Yes, this is an anticipated need. The vendor will be responsible for integrating the payment processor into the data system. The vendor will discuss payment processor options with the commission. The commission will ultimately select the payment processor.*

45. Will there be a dedicated technical resource available during working hours?

45.1. *Yes, the commission has staffing to help.*

46. 72-Hour Issuance Requirement: Is the 72-hour issuance requirement a system-level SLA or an operational goal dependent on state response times? If dependencies exist, what service-level objectives (SLOs) apply?

46.1. *The 72-hour issuance requirement is an operational goal. This would be further developed through the agile process.*

47. Is there an expectation for the contractor to provide a production-ready system at the end of the one-year performance period, or primarily an MVP with core workflows implemented?

47.1. *The goal is for MVP. Timeline will be influenced by the commission's input of user stories that would ultimately encompass the MVP.*

48. Will the Commission provide design artifacts or data samples from member states to guide initial user story development?

48.1. *The commission is comprised of members states and will work with the developer on user story development. Through the agile process the commission will work with vendor to provide relevant information.*

Security, Compliance, & Privacy

49. Data Classification & Compliance: Will the system store PII, disciplinary/investigatory data, or PHI? Is HIPAA compliance required?

49.1. *This will be determined through the agile process, but PII is expected. The commission does not anticipate a need for HIPAA compliance.*

50. Incident Response: Should the proposal include a formal security incident response plan?

50.1. *No.*

51. Security Standards: Beyond OWASP ASVS 3.0, are other standards required (e.g., NIST, SOC 2)?

51.1. *No.*

52. Network & Monitoring: Are IP allow-listing, SOC integration, and SIEM monitoring expected? What incident response SLAs apply?

52.1. *As this is not a contract for hosting services, these standards are not applicable. The commission may need the data system vendor to provide short-term hosting, which could be accommodated through a contract modification. These standards would then be determined through the agile process*.

53. The RFP references QWASP Application Security Verification Standard 3.0. Can you confirm whether the Commission requires third-party penetration testing prior to system acceptance or a penetration testing report using the standard tool will suffice?

53.1. *This has not been determined at this time*.

54. Will the Commission provide its own security assessment or vulnerability scanning tools, or should the contractor procure and operate these independently?

54.1. *The vendor should provide this*.

Staffing & Project Management

55. Should the contractor plan for quarterly stakeholder demonstrations in addition to sprint demos?

55.1. *Quarterly stakeholder demonstrations are not required, but sprint reviews will be expected*.

56. Are remote-only project teams acceptable, provided they are available during 9 a.m. – 5 p.m. ET?

56.1. *Yes*.

57. Does the Commission have a preferred agile methodology (Scrum, Kanban, or hybrid) or expect the vendor to propose one?

57.1. *The vendor is expected to propose an agile methodology*.

58. Will the Commission's Product Owner participate in daily stand-ups or only sprint reviews?

58.1. *The product owner will participate in both planned stand ups and sprint reviews*.

User Experience & Functionality

59. Will the Commission provide end users for usability testing, or is the contractor expected to recruit representative users (e.g., from member states)?

59.1. *The commission will assist with providing end users for usability testing*.

60. The RFP outlines several user stories. Does the Commission have a prioritized product backlog or will prioritization occur collaboratively during sprint planning?

60.1. *Prioritization will occur during sprint planning*.

61. Participant Profiles: Are there specific user groups that must be prioritized for testing?

61.1. *This will be determined through the agile process, but likely physician assistants and licensing boards*.

Agile Process

The following questions cannot be answered at this time as they will be determined through the agile process.

1. Public Directory: Which fields should be publicly visible versus restricted? Are there requirements for rate limiting, bulk export, or API access for directory data?
2. Usability Testing: What is the expected cadence for usability testing?
3. Can the Commission identify which state systems or data sources (e.g., FSMB, NCCPA) must be integrated during Phase 1?
4. Should the system include real-time license verification capabilities, or batch updates during the initial release?
5. Are there any defined data standards or formats (e.g., HL7, JSON schemas) that must be followed for cross-state data exchange?
6. Reporting & Analytics: What reporting and analytics capabilities are expected? Please provide examples of key performance indicators (e.g., privileges issued by state/month, processing times, revocations, renewal rates). Is there a preference for self-service BI tools or dashboards?
7. MVP Definition: What is the minimum viable product (MVP) expected for the initial release? Which user stories are mandatory for MVP versus later phases?
8. Persona Coverage: Must MVP include all personas (e.g., Physician Assistant, State Administrator, Commission staff, public users, insurers, employers, regulators), or can public-facing features and insurer/employer integrations wait for Phase 2?
9. Encryption Requirements: What level of encryption is required for data at rest and in transit?
10. Identity Assurance: Do applicants require NIST IAL2/AAL2 or equivalent? What is the minimum identity proofing standard?
11. Audit & Retention: What are the requirements for audit logging, tamper evidence, retention, and expungement/sealing of disciplinary records?

12. External Interfaces: For AAPA, NCCPA, FSMB, DEA/credentialing systems, and insurers— which are authoritative sources versus reference sources?
13. SSO Integration: Should the system support single sign-on (SSO) using SAML or OIDC with state identity providers and/or Commission staff accounts?
14. Access Control Model: What is the expected authorization approach, RBAC, ABAC, or a hybrid? Please confirm required roles (e.g., Physician Assistant, State Administrator, Investigator, Commission Staff, Read-only Public, Insurer, Employer, Regulator).
15. Military Affiliation Verification: How should military affiliation be verified? What authoritative source and protocol should be used?
16. State Licensing Systems: Which state licensing systems are in scope for Phase 1 integrations?
17. Update Mechanism: Will states push updates via webhooks/event notifications, or should the system poll? What notification channels are required (email, SMS, webhooks)?
18. Payments & Financial Flows: Which payment service provider should be used? What are the PCI-DSS requirements? How should fees be distributed between states and the Commission? What invoicing and reconciliation processes are expected?
19. Canonical Entities: What are the core entities the system must support (e.g., Practitioner, License, State of Qualifying License, Privilege, Discipline/Complaint, Exam, Payment, Status/History)? Are there any additional entities we should plan for?
20. Credentialing Artifacts: For “supports credentialing and DEA registration,” what artifacts or attestations must the system produce (e.g., verifiable credential, digitally signed PDF)?
21. Reminder Rules: What is the expected cadence and escalation process for expiration/renewal reminders, and are opt-out options required?
22. Digital Wallet Scope: Is a verifiable credential/digital wallet approach (e.g., W3C VC, HL7 VC) in scope, or is a static attestation acceptable?
23. Channels & Standards: Which channels are permitted (email, SMS, in-app) and what requirements apply for templates, localization, and brand standards?