Cloud Vendor Security Questionnaire and Assessment

Audience

IT manufacturers, vendors, and third-party organizations that are being considered as potential business partners, or those that are currently contracted with the NYC Health Department.

Purpose

To more easily assess the cybersecurity posture of a vendor-hosted / cloud solution, the manufacturer should provide requested information below. When completing the form, please attach or provide links to supporting documentation such as policies and procedures.

Item No.	Description	Response
0.0	NYC Health Department Project Name and ID	<Filled out by NYC Health Department>
0.1	NYC Health Department contract PIN or purchase order number if applicable.	<Filled out by NYC Health Department>
Vendor		
1.0	Vendor/Company Name	**Nava PBC**
1.1	Product Name including Version Number and Edition/Level (e.g. Standard, Pro, Enterprise) If multiple products are included in the proposal, please list them all.	Government Services Navigator, v1.0 (Custom SaaS, developed for this engagement).
1.2	Company web site	https://navapbc.com
1.3	Company main office address	601 13th St NW, Floor 12, Washington DC 20005
1.4	Primary contact info (Name, email, phone)	Meg Ingram, Director of Contracts, contracts-team@navapbc.com, (703) 829 0243
1.5	Primary technical contact info (Name, email, phone)	Mike Moran, Director of Information Technology, mikemoran@navapbc.com
1.6	Please provide list of security certifications that your company holds such as but not limited to FedRAMP, HIPAA, PCI, SOC1, SOC2, ISO27001, SOC1/SSAE16/ISAE3402 Security Assessment Document (SAD), etc.	Nava's Beam benefits platform holds SOC 2 Type II certification. The Government Services Navigator is deployed on the same underlying AWS and Strata infrastructure architecture. Nava is committed to achieving SOC 2 Type II for this environment. Additionally, Nava's Government Services Navigator infrastructure complies with NIST SP 800-53 Rev. 5 FISMA

	Please provide and/or attach supporting documentation.	Moderate controls via Nava Strata infrastructure-as-code templates. Information about Nava Strata NIST compliance is available at https://www.navapbc.com/strata
Solution		
2.0	Please describe the solution service offering including if it is Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or Software as a Service (SaaS).	The solution is delivered as Software as a Service (SaaS). Government Services Navigator is an AI-powered, agentic benefit enrollment tool that helps NYC residents identify eligibility for and apply to public benefit programs in a single guided session. The system combines a conversational AI interface with structured form-based data entry, document parsing and auto-population, and agentic application submission via robotic process automation (RPA) and pre-filled forms where direct API integration is unavailable. Residents do not create accounts or store personal information; all session data is ephemeral. Nava hosts and operates the fully managed, cloud-hosted application on AWS. DOHMH client access the service via a publicly accessible URL. Nava is responsible for all infrastructure provisioning, maintenance, patching, monitoring, and operations.
2.1	If this is a Software as a Service (SaaS), please classify your product under the below category and explain: a. **Off-the-Shelf (SaaS) product:** A prebuilt solution designed for general use and requires minimal configurations to function. These products are essentially ready to use "as-is" and cater to a wide range of industries and users with standard features and functionality. b. **Configurable (SaaS) product:** A solution that allows users to configure the system for different use cases through configuration and/or no-code and low-code development. These adjustments are typically achieved through user-friendly interfaces or built-in configuration tools.	Customized SaaS product. The Government Services Navigator will be developed specifically to meet DOHMH's requirements for NYC benefit enrollment, including program-specific eligibility logic for approved NYC benefits programs, custom UX, non-API integration pathways, and document parsing tailored to program-specific document types.

	c. **Customized (SaaS) product:** A solution modified or developed specifically to meet the unique requirements of an organization. These customizations often involve changes to the platform's code, integrations with other systems, or the development of entirely new features.	
2.2	Please describe the general solution category (e.g., Health Care, Case Management System, Surveillance, Inspection, Storage, Survey, Collaboration, Security)	Digital Government Benefits Enrollment. Government Services Navigator is a resident-facing web application that guides NYC residents through eligibility screening and application submission for non-gated public benefit programs.
2.3	Please indicate the cloud service provider the solution hosted on. (e.g., Azure, GCP, AWS, self-hosted)	Amazon Web Services
2.4	Please indicate the country and region the cloud solution hosted on. If outside of the U.S.A., please describe if the solution can be hosted in the U.S.A. and if any terms and conditions apply to it.	Amazon Web Services (AWS), primary region: US-East-2 (Ohio). Disaster recovery region to be confirmed during implementation. Current architecture supports multi-region deployment and all infrastructure is defined as code (Terraform/Strata templates) enabling rapid deployment to any U.S. AWS region.
2.5	Please provide a copy of dependency topology and data flow diagram.	See attached architecture diagram.
2.6	Please indicate if the solution includes a mobile app (iOS, Android) and describe how it works with the overall solution.	The Government Services Navigator is a responsive web application, not a mobile application.
2.7	Please indicate if your company provides a staging environment to customers for the following purposes: a. User acceptance testing of customed or configured functionality. b. Testing of new platform features or seasonal upgrades. c. Application scanning / penetration testing. d. Other, please describe.	Yes. Nava will provide a dedicated staging environment for: (a) User acceptance testing of configured functionality; (b) Testing of new features prior to production deployment; (c) Application scanning / penetration testing by NYC Cyber Command (separate from UAT environment). Staging environments are included at no additional cost within the contract price.

	Please indicate if there an additional cost to separate environments for staging and application scanning. Please note that scanning cannot be conducted in the same environment as user acceptance testing due to possible corruption of data.	
2.8	Please indicate if the access to the cloud solution is directly via a publicly accessible URL. If the solution must be access through a private endpoint utilizing VPN Tunnel, Circuit, and/or SDWAN with the city's network, please also fill out the appropriate sections in the On-Premises Vendor Security Questionnaire and Assessment document.	Yes. The solution is accessed via a publicly accessible URL over HTTPS (TLS 1.3). No VPN, private endpoint, or SDWAN connection to the City's network is required.
2.9	Please describe if the cloud solution is built on another vendor cloud platform. If so, describe the expectation of NYC Health to support the solution post Go-Live. If the solution is built on a low-code platform, at this time, the agency is not accepting new solutions built using Microsoft Dynamics or Service Now. The agency is currently leveraging Salesforce.	Government Services Navigator is built on AWS, a widely used commercial cloud platform. Nava manages the full application stack. The solution does not use Microsoft Dynamics or ServiceNow. Nava will provide post-go-live support for the solution as described in the contract; DOHMH is not expected to maintain AWS infrastructure independently.
2.10	Please describe any required 3rd party solutions that are required to work with this system. For example, if the system requires a document management system to be integrated, please indicate that and which products and where it would be hosted.	Government Services Navigator integrates with the following third-party components: 1. AWS Bedrock or OpenAI API, large language model (LLM) for conversational eligibility screening and document parsing. All data processed via LLM API is transmitted over encrypted channels; no PII is retained by the LLM provider. 2. AWS services (CloudFront, WAF, ECS, Lambda, S3, CloudWatch, Security Hub) are all managed within Nava's AWS account. No additional customer-managed infrastructure is required.

2.11	Please describe the required specifications for peripheral technology such as printers, label printers, scanners, instruments, RF Guns, etc. Please indicate if any peripherals will be connected to the NYC Health network or only to the user's workstation. If the solution requires networked peripherals: a. Please describe the communication/network protocols/network ports required? b. Please indicate if all communication is encrypted in transit.	None. Government Services Navigator is a web-based application with no peripheral hardware requirements.
Security and Availability		
3.0	Please describe if the solution encrypts data at rest and if so at what encryption level (e.g., AES256).	Yes. All data stored in AWS services is encrypted at rest using AES-256 via AWS KMS Customer Managed Keys (CMK). This includes: Aurora PostgreSQL 16 database (storage encrypted with KMS CMK); DynamoDB session store (KMS CMK); ECR container image repositories (KMS CMK); Amazon Cognito user pool (KMS CMK); AWS Secrets Manager (KMS CMK); SSM Parameter Store (KMS CMK). KMS key rotation is enabled. No data is stored in unencrypted form at rest.
3.1	Please describe if the solution encrypts data in transit and if so at what encryption level (e.g. TLS 1.2). Encryption must be at the message level not at the transport layer (e.g., VPN encryption). The solution must support approved modern ciphers: • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_128_GCM_SHA256	Yes. All data in transit is encrypted using TLS. The solution uses AWS Application Load Balancers configured with security policy ELBSecurityPolicy-TLS13-1-2-2021-06, which enforces a minimum of TLS 1.2 and supports TLS 1.3. TLS 1.0 and TLS 1.1 are disabled. HTTP requests are redirected to HTTPS via HTTP 301. All communication between application services and AWS managed services (Amazon Bedrock, DynamoDB, Secrets Manager, SSM Parameter Store, ECR) uses HTTPS via AWS PrivateLink VPC endpoints, keeping traffic within the AWS network. Database connections to Aurora PostgreSQL use TLS enforced by IAM database authentication. No unencrypted protocols are permitted across any external or inter-service boundary.

	It may support older ciphers for compatibility purposes only: • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-CHACHA20-POLY1305 • ECDHE-RSA-CHACHA20-POLY1305 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256	
3.2	Please describe the Data Loss Prevention (DLP) program for this solution.	The solution's primary DLP measure is architectural and data-minimization-by-design: (1) No resident PII is transmitted to or retained by the LLM (Amazon Bedrock) beyond the active inference request. (2) Session data in DynamoDB is scoped to the active session and expired automatically. (3) The Aurora PostgreSQL database stores application operational data; access is restricted to authorized services via IAM database authentication over TLS, with no public endpoint. (4) All data egress to external non-AWS services is routed through a dedicated task-executor service with restricted egress Security Group (HTTPS/443 only from private subnet). (5) CloudWatch and New Relic provide monitoring for anomalous data access patterns. (6) All storage is encrypted with KMS CMK; key access is logged and auditable via AWS CloudTrail.
3.3	Please describe the data retention policy and plan for this solution.	(1) Resident session data (DynamoDB): session records expire automatically at session end; TTL is configured on all session records. (2) Application database (Aurora PostgreSQL): operational data retained for the contract period; no resident PII stored by design. (3) Uploaded documents: documents are processed in-memory and not persisted to storage. No uploaded

		document is retained by the system after processing. Where required, processed documents or extracted data can be forwarded directly to the relevant agency; Nava does not retain a copy. (4) Audit/system logs (CloudWatch): retained for 90 days in active storage, then archived for 1 year. (5) New Relic APM data: retained per New Relic's data retention policy for the account tier. Aurora automated backups: retained for 30 days consistent with the NYC Cloud Services Agreement requirement. Point-in-time recovery (PITR) is enabled for DynamoDB.
3.4	Please indicate the country and region the where the data resides.	All data is stored and processed exclusively within the United States. Primary: AWS US-East-2 (Ohio). All AWS services (Aurora PostgreSQL, DynamoDB, Secrets Manager, SSM Parameter Store, ECR, CloudWatch) are provisioned in U.S. AWS regions. Amazon Bedrock uses cross-region inference profiles; all inference endpoints are within the U.S. No data is transmitted to or stored in non-U.S. locations.
3.5	Please describe the data backup plan, schedule, and location.	(1) Aurora PostgreSQL 16: automated daily backups with 30-day retention; point-in-time recovery (PITR) enabled. Backups stored in AWS US-East-2 (Ohio). (2) DynamoDB (session store): point-in-time recovery (PITR) enabled; on-demand backup available. (3) Infrastructure configuration (Terraform state): versioned in S3 with versioning enabled; daily snapshots retained for 30 days. (4) Application code: version-controlled in GitHub; continuous versioning. (5) CloudWatch logs: retained 90 days active, 1 year archived. (6) All backups encrypted with KMS CMK. (7) DR site maintains consistent backup state. RTO: 6 hours; RPO: 2 hours.
3.6	Please describe how the solution implements network segmentation and firewalls to protect the data and application.	Multi-layer network security architecture: (1) WAFv2 Web ACL (REGIONAL): edge-level application firewall with AWS managed rule sets (AWSManagedRulesCommonRuleSet, SQLi protection, body size limits) and rate limiting.

	Please include if any special rules are applied for data that is considered Restricted and/or HIPAA/PCI.	(2) VPC segmentation: public subnets host only Application Load Balancers; all ECS Fargate services, Aurora PostgreSQL, DynamoDB access, and inter-service communication run in private subnets with no direct internet exposure. (3) Security Groups: ALBs accept HTTPS (443) from internet; Fargate services accept traffic from ALB Security Groups only (ports 3000, 8080, 8086 internally); Aurora PostgreSQL accessible from private SG only on port 5432; no public endpoint. (4) VPC PrivateLink endpoints: all AWS service communication (Bedrock, DynamoDB, Secrets Manager, SSM, ECR, CloudWatch) uses private VPC endpoints, bypassing the internet entirely. (5) External egress: only the task-executor service has egress to external non-AWS services, restricted to HTTPS/443 from a private Security Group. The solution does not handle HIPAA or PCI data; NIST SP 800-53 SC controls are applied throughout.
3.7	Please describe the solution password policy and standards assuming SSO integration is not applied. ● Complexity/length ○ At least 24 characters without MFA ○ At least 15 characters with MFA ○ Must have upper case character, Lower case character, numbers and special character. ○ Expiration Every 90 days ● Auto Lock out and deactivation ○ After 5 consecutive failed login attempts within 15-minute period, the account must require a delay of at least 15 minutes before retrying.	The resident-facing application does not have a native login. Residents interact without creating accounts or passwords. For Nava infrastructure administrative access (AWS Console, CLI): (1) MFA is required for all access (authenticator app). (2) IAM password policy: minimum 14 characters, requiring uppercase, lowercase, numbers, and special characters. (3) Passwords expire every 90 days. (4) Account lockout after 5 consecutive failed login attempts within a 15-minute window (15-minute delay before retry); locked until reset after 10 failed attempts. (5) All credentials managed via AWS Secrets Manager and SSM Parameter Store, encrypted with KMS CMK, consistent with the NYC Citywide Encryption Standard. No long-lived static credentials are used; CI/CD uses GitHub Actions with OIDC (no static AWS keys).

	○ After 10 failed login attempts, the account must be locked until the user successfully resets the password. • Other ○ Passwords must be encrypted at rest and in transit using protocols compliant with the Citywide Encryption Standard.	
3.8	Please describe the solution's SSO ability to integrate with Azure Entra and SAML 2.0. NYC Department of Health uses: • Azure Entra for NYC Health employees • NYC.ID (SAML 2.0) for public users, partners, and city agencies. Please also describe if the solution can integrate with both within the same solution. Please also indicate if the solution can leverage the solution's native login alongside integrated SSO.	The resident-facing application is public-access and requires no login. SSO integration with Azure Entra or SAML 2.0 providers is not in scope for the initial build. Administrative and CSP user access uses Amazon Cognito with Google IdP (OAuth 2.0/OIDC) and inviteonly provisioning for this engagement. However, Cognito natively supports SAML 2.0 and OIDC/OAuth 2.0 identity providers, including Azure Entra and NYC.ID, which would enable SSO integration to be supported in a future iteration without architectural changes.
3.9	Please describe if the solution has its own native multi-factor authentication (MFA) separate from SSO integration. For example, if the native login was used does it natively have MFA? Please describe what type of MFA is used (e.g., SMS, Authenticator App, Voice, Email)	Yes. Amazon Cognito (the identity provider for admin/CSP users) has MFA enabled natively. MFA is required for all authenticated administrative users. Supported MFA types: TOTP (authenticator app) and SMS. The resident-facing application has no login interface and therefore does not require MFA for residents.
3.10	Please describe the solutions audit logging process and retention policy. • Successful and unsuccessful login • Major events • Other Please describe the process in which NYC Health Department can access the audit logs via API to integrate to our SIEM.	Comprehensive audit logging via AWS CloudWatch and New Relic APM: (1) All Fargate service logs, ALB access logs, WAF logs, and VPC flow logs are captured in CloudWatch. (2) Successful and unsuccessful Cognito authentication events (login, MFA, sign-up) are logged. (3) All AWS API calls are captured via CloudTrail. (4) KMS key usage is logged.

		(5) Database query logging and slow query logging are enabled on Aurora PostgreSQL. (6) New Relic APM captures application-level events and performance metrics. Log retention: 90 days in active CloudWatch storage; archived for 1 year. NYC Health Department can access audit logs via the CloudWatch API (pull-based) or via Kinesis Data Firehose integration to a SIEM endpoint. Nava will configure SIEM integration during implementation in coordination with DOHMH.
3.11	Please describe the solution's Disaster Recovery plan. Please ensure to include the following information: • Location and distance from primary data center. • Recovery Time Objective (RTO) • Recovery Point Objective (RPO) • Testing frequency • Other	Government Services Navigator disaster recovery plan: (1) DR site: infrastructure-as-code (Terraform/Strata templates) enables rapid redeployment to an alternate U.S. AWS region. DR region to be confirmed during implementation. Current architecture supports multi-region deployment. Distance from primary (US-East-2, Ohio) to alternate U.S. region exceeds 500-mile requirement. (2) RTO: 6 hours. (3) RPO: 2 hours. (4) Aurora PostgreSQL automated backups (30-day retention, PITR enabled) support rapid DB restoration. DynamoDB PITR enabled. (5) ECS Fargate services are stateless and redeployable from ECR images within minutes. (6) Terraform state and application configuration backed up and available for DR deployment. (7) DR testing: annually, documented. (8) Uptime SLA: 99.9% monthly availability.
3.12	Please describe the internal Access Control Plan (ACP) to the elevated permissions to the solution including ability to view customer data and administrative rights. Please include: • Personnel responsible for and process for account provisioning, approval process for account provisioning and changes • Documentation process / management • Frequency of reviewing accounts • Other	Nava's access control plan for Government Services Navigator: (1) Personnel: access provisioning is managed by Nava's Engineering Lead and reviewed by the Project Lead. All access requests require written approval from the Project Lead. (2) Provisioning process: access is provisioned only upon signed approval, with assignments following least-privilege RBAC. (3) Documentation: all access grants and changes are documented in an access control log maintained in Nava's project management system.

		(4) Review frequency: access is reviewed quarterly. Personnel departures trigger immediate access revocation. (5) Elevated access (production): requires MFA + manager approval; time-limited where possible. (6) Nava's US-based staff only have access to production systems relevant to their role.
3.13	Please indicate the country and region of implementation and support staff who have access to customer production data. If outside of the U.S.A., please describe if the solution can be supported by only staff located in the U.S.A.	All Nava implementation and support staff are located in the United States.
3.14	Please describe the organization's Incident Response Policy and Protocol when a security incident occurs. Please also include notification protocols.	Nava's Incident Response Policy is aligned with NIST SP 800-61: (1) Detection: automated alerting via AWS Security Hub and CloudWatch alarms triggers immediate notification to Nava's on-call engineering staff. (2) Triage: initial triage within 1 hour of detection. (3) Containment: impacted systems isolated; access revoked if compromise is suspected. (4) DOHMH notification: within 24 hours of confirmed incident identification. (5) Investigation and remediation: documented root cause analysis; remediation deployed and verified. (6) Written incident report: delivered to DOHMH within 5 business days of incident resolution. (7) For incidents involving potential PII exposure: Nava follows applicable breach notification requirements and will notify DOHMH immediately.
3.15	NYC Cyber Command requires that a DAST scan be directly performed by NYC Cyber Command for any system that stores or transmits Sensitive or Restricted data. The submission / attestation from a third party is not acceptable. Please describe your organizations policy to allow NYC Cyber Command to conduct the DAST scan. Please also provide a copy of the most recent penetration testing and vulnerability scanning report and results	Nava fully supports and welcomes NYC Cyber Command conducting a direct DAST scan of the Government Services Navigator staging environment prior to production deployment. We understand that third-party attestations are not acceptable and that NYC Cyber Command must conduct the scan directly. Nava will: (1) Provide NYC Cyber Command with direct access to the staging environment on a mutually agreed schedule. (2) Coordinate a dedicated DAST environment separate from the UAT environment, as required. (3) Remediate all critical and high findings prior to production deployment.

	conducted by an independent 3rd party cybersecurity firm.	(4) Provide scan scheduling coordination via the DOHMH project team.
3.16	Please describe the solution's email capabilities for receiving and sending emails including sending emails to public users, registered users, and admin users. Please describe if the solution includes this natively and/or third-party integration with an email provider is required. Please name any preferred email providers. For sending emails, please indicate the solutions capabilities to support DKIM/DMARC to securely use NYC Health Department email domain.	Government Services Navigator does not send or receive email on behalf of residents. Optionally, session summary or submission confirmation can be delivered via email if DOHMH chooses to implement this feature. If enabled: email would be sent via a transactional email provider (e.g., Amazon SES or SendGrid), with DKIM/DMARC configured to support use of the NYC Health Department email domain if required. This would be scoped and configured during the implementation phase. Currently, no email functionality is included in the initial build scope.
3.17	Please describe the solution's SMS capabilities for receiving and sending SMS messages including sending emails to public users, registered users, and admin users. Please describe if the solution includes this natively and/or third-party integration with an SMS provider is required. Please name any preferred SMS providers. For sending SMS messages, please indicate the solutions capabilities to dedicated short codes specific to NYC Health Department.	Government Services Navigator does not currently include native SMS capabilities. If DOHMH requires SMS notifications (e.g., submission confirmation), this can be added via a third-party SMS provider (e.g., Amazon SNS or Twilio). Short code configuration specific to NYC Health Department would be coordinated with the chosen provider. Currently, no SMS functionality is included in the initial build scope.
Physical Security		
4.0	Please describe the physical and environmental safety plan for your company.	Government Services Navigator is hosted on Amazon Web Services (AWS). Physical security for all data center facilities is managed by AWS. AWS maintains comprehensive physical security including 24/7 security staff, biometric and badge-based access controls, CCTV surveillance, and environmental controls (fire suppression, power redundancy, HVAC). AWS physical security documentation is available at https://aws.amazon.com/compliance/data-center/controls/.

		Nava staff do not have physical access to AWS data centers. Nava's office environments follow standard commercial office security practices.
4.1	Please describe if staff are required to electronically swipe their ID to physical gain access to sensitive locations such as a server room or data center.	AWS data centers (where Government Services Navigator is hosted) require electronic badge swipe access for all entry to secure areas, including server rooms. Access is restricted to authorized AWS personnel only. Nava staff do not have physical access to AWS data center facilities. For Nava's own office environments, access control varies by office location but includes standard commercial building security.
4.2	Please describe your organizations ability to audit and track physical entry into sensitive locations including non-staff guest entry for temps, contractor, inspectors, and visitors.	AWS data centers provide comprehensive physical entry audit logging for all personnel, including staff, contractors, and visitors, with electronic access records. Nava staff do not access AWS data center facilities. AWS compliance reports (SOC 2 Type II) document physical access controls and are available under NDA upon request.
4.3	Please describe your organizations surveillance system to monitor sensitive locations.	AWS data centers are equipped with comprehensive CCTV surveillance systems monitoring all secure areas. AWS's SOC 2 Type II report documents surveillance controls. Nava staff do not have access to AWS physical facilities.
Support and Upgrades		
5.0	Please describe the organization's support structure for clients. Describe what is included as part of the maintenance/subscription cost, and what requires professional services add-ons. Please also describe who can contact support and during what hours of the week. For professional services add-ons, please indicate if the hours are billed only when used, or they are packaged support hours that expire. Indicate if all staff are U.S. based? Non-U.S. based staff require a waiver from the city and is not guaranteed to be approved. All proposals should assume U.S. based staff unless it is not possible.	Nava provides dedicated support included in the contract price: (1) Primary support channel: shared Slack channel and email with DOHMH project team. (2) P1 (critical — system unavailable): response within 1 hour, 24/7. (3) P2 (major feature impaired): response within 4 business hours. (4) P3 (standard): response within 1 business day. Support hours: standard business hours (9am–6pm ET, Monday–Friday) for P2/P3; 24/7 on-call for P1 critical issues. All Nava employees are U.S.-based. No professional services add-ons are included within the scope of this contract period.

5.1	During the implementation phase of the initial project, please describe the costs incurred by the client. Indicate if the client will be billed for entirety of all licenses prior to Go-Live, or if license costs will ramp up as the project enters Execution, User Acceptance Testing, and Go-Live.	All costs are included in the $100,000 firm fixed price. There are no separate licensing costs that ramp up during implementation. Payment milestones are tied to project deliverables rather than license activation. DOHMH will not be billed for licenses prior to go-live. The payment schedule is milestone-based as described in the Price Proposal section of the proposal response.
Confirmation		
	Today's Date (yyyy-mm-dd): Name and Title	2026-06-19 Signed by: Megan Ingram 4F3806103419487... Megan Ingram, Director of Contracts Nava PBC

Template Information

Version:	1.1
Date:	1/20/2026
Data Classification:	NON-RESTRICTED - Available for public disclosure.