CALIFORNIA STATE LOTTERY

REQUEST FOR INFORMATION

Lottery Public Website (PWS) and Cloud Infrastructure: Maintenance, Support, and New Development

ISSUED BY:
California State Lottery
PROCUREMENT SERVICES AND SUPPORT UNIT

Table of Contents

California State Lottery 1
Request for Information (RFI) 1
Invitation 5
1. Introduction 6
2. Background 7
2.1. Overview 7
2.2. Site Audience and Content 7
2.3. Digital Services Environment 8
2.4. Development 11
2.5. PWS Data Flow 11
2.6. Transactions 12
2.7. Content Administration 13
3. Key Action Dates 13
4. RFI Format 13
5. Services 13
6. Current PWS Tools and Supporting Systems 18
7. Exhibit A-1 Questionnaire 21
EXHIBIT A-2 – California Lottery Information Security Standards 22
1. Information Security 22
2. Data Confidentiality, Integrity, Availability and Management 22
3. Contractor Responsibilities 22
4. Information Security Incident 23
5. Information Security Incident Contact Information: 23
6. Information Security Audit 24
7. Physical Security 24
8. Security Plan 24
9. Security Plan Requirements 25
10. Business Continuity and Disaster Recovery Planning 26
11. Rights to Lottery Data 27
12. Data Location 27
13. Remote Access 27
EXHIBIT A-3 – IT Provisions 28
1. Deliverable Review, Accpetance, and Rejection: 28
2. Definitions 28
3. Deliverable Expectations 28
4. General Requirements 28

5. Samples:.....29
6. Future Releases: 29
7. Encryption/CPU ID Authorization Codes: 29
EXHIBIT A-4 – Current Network and Infrastructure Administration 31
1. Network/Security Administration:.....31
2. Infrastructure Administration:.....31

This page is intentionally left blank.

Invitation

Attention: All Interested Parties

RE: RFI for the California Lottery's Public Website (PWS) and Cloud Infrastructure for Maintenance, Support, and new Development

This Request for Information (RFI) is being issued to companies who specialize in cloud hosted website, infrastructure support, and website development.

This RFI seeks industry feedback and information on standard requirements for PWS' management, maintenance, and support including its infrastructure and future development.

Built on the Sitecore platform and cloud-hosted in Azure, PWS requires Contractor website development expertise and support for PWS infrastructure and databases. Upon contract award, the Contractor will begin a transition period to assume 24/7/365 monitoring and support of site operations along with new development requests for PWS enhancements.

The RFI responses will assist the Lottery in finalizing their solicitation effort and provide a better understanding of the commercial support models for websites with multiple third-party integrations.

This RFI is intended to help the Lottery ensure that it has done its due diligence to prevent the requirements from being overly restrictive, so as not to inadvertently dissuade a viable business provider from submitting a proposal.

The Lottery requests that vendors provide feedback regarding errors, omissions, inconsistencies, contradictions, or clarity. The Lottery will use information provided through this RFI to ensure that the deliverables and qualifications outlined in the resulting PWS Request for Proposal (RFP) provide prospective vendors with a sufficient basis for understanding the Lottery's needs.

The Lottery will also use this information to determine that the services and deliverables in the solicitation are reasonable within the scope and to provide the vendor community with an opportunity to identify additional services that would assist the Lottery to achieve desired performance and outcomes. This document provides questions to be answered by prospective bidders in Questionnaire (Exhibit A-1).

1. Introduction

The Lottery is releasing this RFI to gather information from companies that provide website support and development. Responses to this RFI will help the Lottery gain a better understanding of market trends as they apply to the Lottery's needs.

The information received from Respondents will be used as follows:

- To compile information regarding experience, methods, capability, and tools.
- To assist the Lottery in identifying products and methods that can meet business needs.
- To offer respondents a chance to provide additional information, not specifically requested, but which the responder deems important and/or relevant may also be submitted. **Note**: Although Responder comments are strongly encouraged and deemed important, the Lottery makes no commitment to change the PWS Support requirements based on input received.

PLEASE READ THE FOLLOWING IMPORTANT INFORMATION BEFORE RESPONDING TO THIS RFI:

1. The Lottery will not reimburse vendors for costs associated with responding to this RFI.
2. The Lottery has no obligation to issue a solicitation or make a purchase as a result of this RFI.
3. Information provided in response to this RFI will not be considered when evaluating bidders who respond to any future procurement.
4. Though not required for response to this RFI, future procurement solicitations will require that vendors agree to the Lottery's Information Security Standards (Exhibit A-2) and Lottery's IT Provisions (Exhibit A-3)
5. Although all comments received will be carefully reviewed and may be considered for inclusion in possible later action, the Lottery makes no commitment to include any recommendations. Further, respondents will not be notified of the result of this process.
6. While not required for response to this RFI, organizations and corporations responding to solicitations from the Lottery must be properly licensed to do business within the State of California.
7. Since this RFI is not a request for bids and no commitment is required of either party, protests will not be considered by the Lottery.
8. All material submitted in response to this RFI will become the property of the Lottery and will be returned only at the Lottery's discretion and at the respondent's expense.

2. Background

2.1. Overview

The Lottery is a public agency created to provide supplemental funding for public education in California. Since its creation in 1984, Lottery has given more than $37 billion in supplemental funding to education. As the Lottery strives to increase supplemental funding for California's public schools, PWS plays a vital role.

The Lottery operates as a consumer products enterprise providing two products – Scratchers® and draw games – sold at more than 23,000 retail establishments. Generally, the Lottery releases 52 individual Scratchers games per year, with four (4) to five (5) new games released each month. The Lottery currently offers eight draw games: two (2) are drawn twice a week, one (1) is drawn three (3) times a week, one (1) is drawn twice a day, three (3) are drawn daily, and one game is drawn every four (4) minutes.

PWS supports Lottery marketing activities by providing product information and services such as account registration. This digital service environment is integrated with a complex, dynamic gaming infrastructure, where peak traffic increases rapidly as jackpots rise.

PWS support requires expertise in website development, maintenance and operations in an Azure cloud environment that includes multiple third-party integrations, network and database management. In addition to maintenance and operations the Lottery seeks the knowledge, skills, and capacity to design and develop PWS features and functionality that improve PWS performance, grow sales and boost customer engagement.

2.2. Site Audience and Content

PWS provides information and digital services to Lottery retailers, players, and the public. Digital services refer to the electronic delivery of information including data and content across multiple platforms and devices, presented in easy-to-use way that enhances the player experience. These digital services include transactional services such as user registration and accessing winner claim forms. Digital services also include features built to increase brand appeal and awareness based on data and analysis of customer interactions with the Lottery brand across digital platforms.

The Lottery's Mobile Apps rely on data from PWS and prospective vendors would be responsible for ensuring the exchange of information between the Mobile Apps and PWS, but not for the maintenance, operations and development of the Mobile Apps themselves. Examples of Mobile App functionality that relies on PWS include:

- APIs (Application Programming Interface) used by the Mobile Apps to capture

and post draw game data and to provide images used within the apps.

- Player 2nd Chance access allowing users to submit ticket codes for additional play opportunities, register for an account, and perform account management functions.

2.3. Digital Services Environment

Built on the Sitecore Experience Platform, PWS is entirely cloud-based, hosted in Microsoft Azure. As a high-availability (99.99% uptime) site for a public agency, PWS must be accessible 24/7/365. Normal PWS traffic volume averages 10,000 calls per minute and is subject to significant traffic increases during high jackpot periods where the average increases to 18,000 calls per minute with peaks approaching 80,000 calls per minute. To meet performance and availability standards, the Lottery currently uses a number of tools and applications to actively monitor PWS uptime, traffic, performance, data interfaces, and site security. The list of current tools and applications that support PWS can be found in the PWS Tools and Supporting Systems table. The Lottery seeks information on additional tools and technologies used in the industry that support the same types of activities needed to maintain and operate PWS.

PWS consumes and produces information in a two-way exchange with the Gaming System, managed by International Game Technology (IGT) Global Solutions Corporation; PWS pushes registration and submission data to IGT, while it pulls player and 2nd Chance draw data from IGT. Additionally, PWS pulls HotSpot® draw results and receives Scratchers©, winning number, jackpot, retailer data, etc. from IGT. Data exchanged between these systems relies on Application Program Interfaces (APIs) and file transfers. These interfaces with the IGT Gaming System fall within the scope of the work described in this document, while Gaming System maintenance, operations and development are out of scope.

In addition to the IGT Systems' integrations, PWS also includes integrations with Experian products to comply with Lottery business rules and State regulations: Address Verification, Email Verification, NameSearch, and PreciseID. Address Verification prevents non-California residents from creating accounts by verifying the physical address entered during the registration process. Email Verification confirms a valid, active email address. PreciseID ensures that no one under 18 years-old registers for a Lottery account and along with NameSearch, prevents the creation of duplicate accounts for a single individual. These tools and integrations serve a critical role in maintaining Lottery compliance with State regulations and are included in the monitoring and maintenance of the PWS. Additionally, under Design Development and Implementation (DDI) work, PWS may need additional integrations with third party applications for promotional events.

The PWS also plays a part in managing the Lottery's social media presence by providing APIs to 3rd Party Applications to provide automated game results and key information such as draw numbers for posts on Facebook and Twitter.

Recently PWS also developed a blog tool to create posts in one place to propagate across social media channels.

To ensure continuity of operations and limit disaster recovery impacts, PWS leverages cloud back-ups and redundancies built into Azure platform.

Figure 1 provides a high-level, generalized view of the Lottery PWS using three tiers: Presentation, System, and Data. The Presentation Tier shows the PWS has three access points: mobile devices, a web portal, and phone (IVR system integration for draw results). The Lottery develops and manages mobile device apps independently but relies on PWS APIs for data. Maintenance and support of the APIs are included in the work described in this document.

The System Tier is composed of Sitecore platform and related components, including databases and custom programs (2nd Chance) with integrations to external, vendor-managed systems. These integrations include the Email and Address Validation, NameSearch and PreciseID managed by Experian and the Gaming Systems (several interdependent systems), managed by IGT.

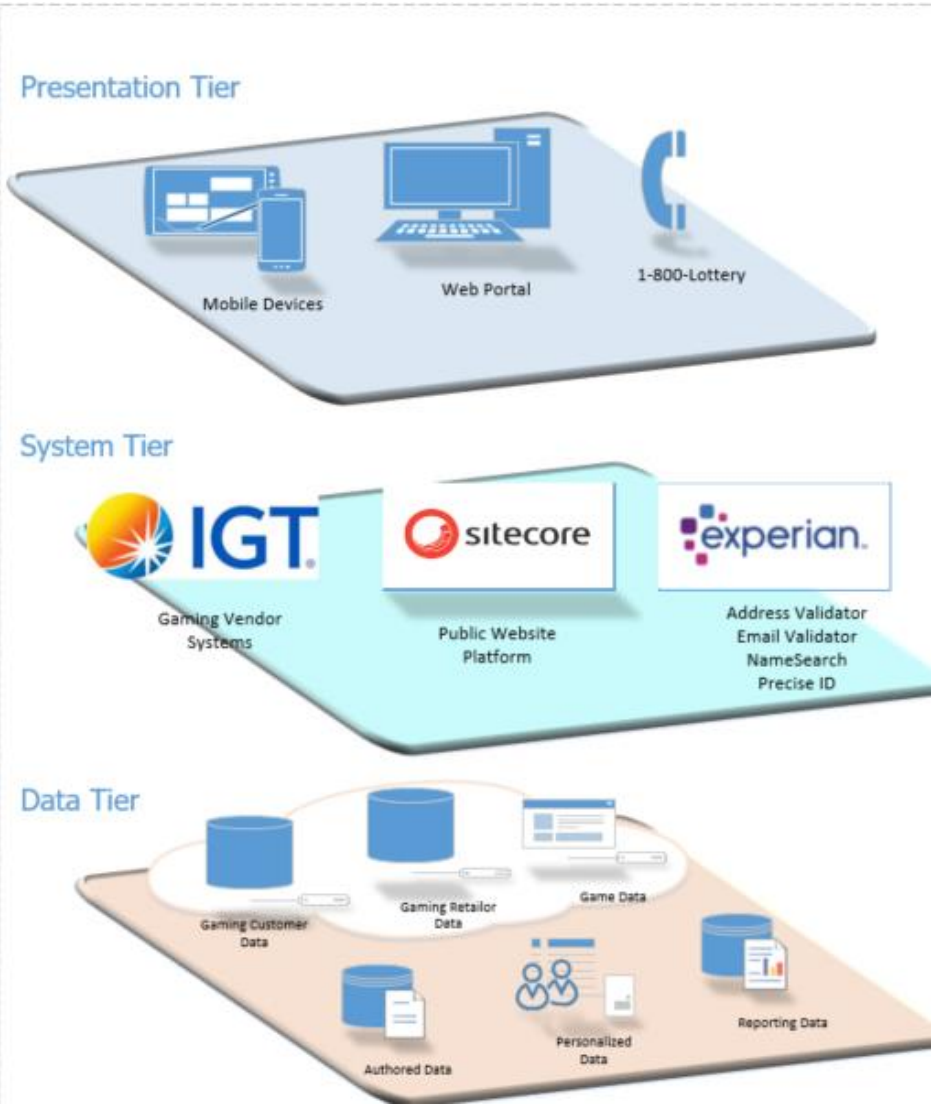

Figure 1

The Data Tier comprises five sets of databases in scope for PWS: Gaming/Retailer Data, Game Data, Authored Data, Personalized Data, and Reporting Data. The PWS maintenance and operations (M&O) includes ensuring availability and recoverability by managing and maintaining these databases, their underlying infrastructure, and data quality. This includes management of the Gaming Customer data connections between the Gaming System and PWS.

M&O includes system monitoring, incident response, patch management, software management, ongoing Website Content Accessibility Guidelines (WCAG) compliance and infrastructure management. M&O also includes security operations, monitoring and incident response. Efforts to enhance PWS in support of Marketing activities to improve system operations and to add new features are performed as DDI work.

2.4. Development

Working in tandem with Lottery business units, ITSD continually develops new features and functions to enhance the user experience. Using the Azure DevOps tool and SAFe Agile methodology PWS delivers several releases each year following standard SDLC best practices. All development is completed in compliance with relevant security standards and meets all applicable governing accessibility requirements including WCAG. The scope described in this document, represents the activities needed to develop the PWS (front end and back end), including work with business partners and stakeholders to deliver new digital products and features. Past projects include the implementation of Experian's tools for Player verification upon new account creation, "animated" HotSpot® drawing display, updating Scratchers® section for improved display, integration of interactive elements from the Lottery's Scratchers' Contractors and Mega Millions® and Powerball® page updates to accommodate changes to the national draw games.

2.5. PWS Data Flow

The diagram provided in Figure 2 illustrates how data flows through the PWS environment. The following narrative describes how data moves through PWS for user select transactions, content, network/security, and infrastructure administration.

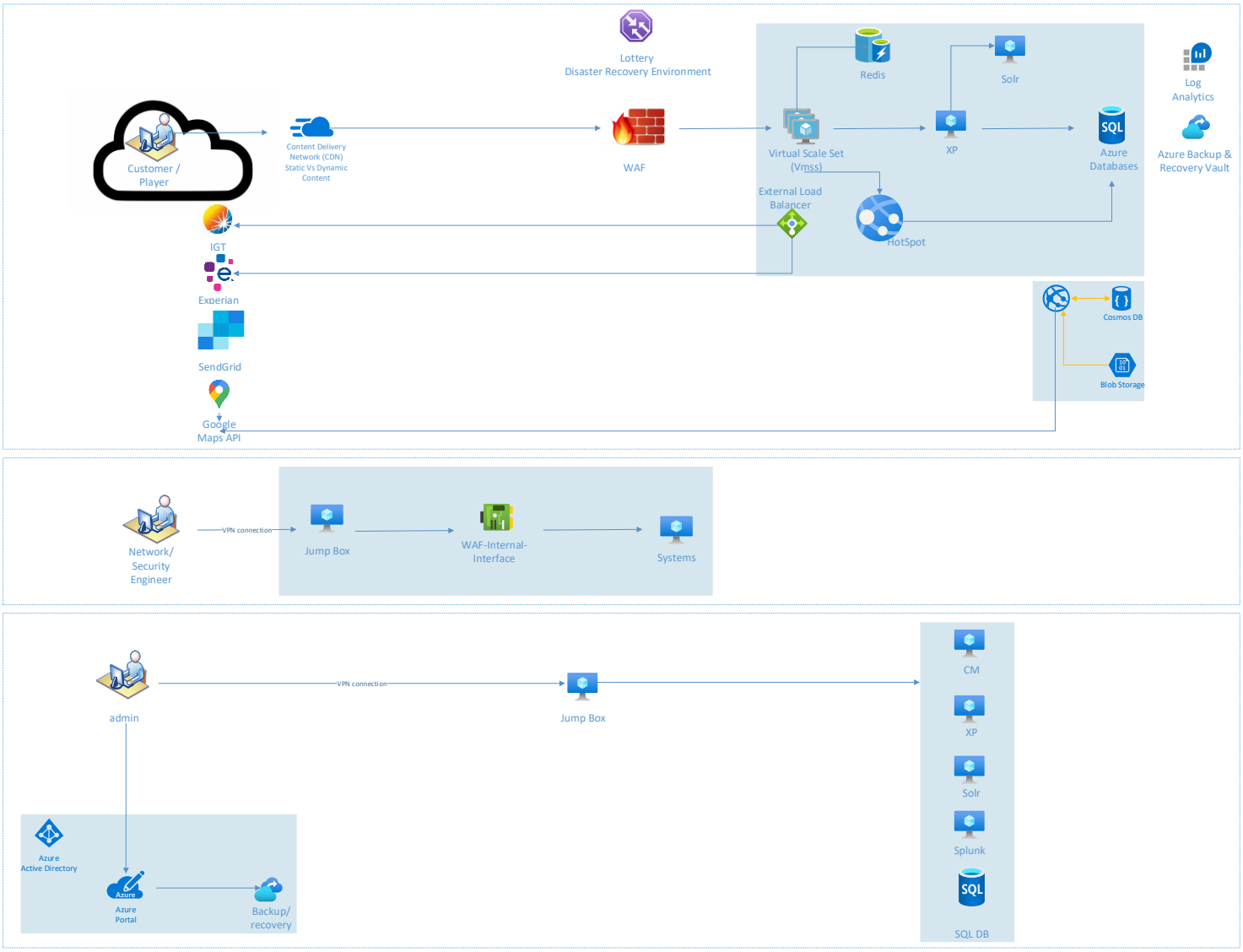

Figure 2

2.6. Transactions

- **2nd Chance Entry:** Using the Lottery's 2nd Chance system, players can enter ticket codes into a 2nd Chance draw where they have another opportunity to win a prize with the same ticket. PWS then passes valid entry information to the IGT Gaming System to determine whether or not the ticket code can be entered into the draw. The Gaming System responds via an API indicating successful/unsuccessful entry.

- **Transaction: 2nd Chance Registration**: If a user wishes to participate in 2nd Chance but does not have an account the system provides the opportunity to register for one. Registration requires the user to enter personal information which invokes an API call to identity verification and management services provided by Experian. Using these results, eligible users can register for an account and submit their ticket codes for 2nd Chance drawings.

2.7. Content Administration

- **Static Content**: PWS environment uses a content delivery network (CDN) to store images and files. When viewing static content, users are redirected to the cloud-hosted vendor-managed CDN. This reduces traffic on the PWS infrastructure thereby enhancing performance for the user.

- **Cached Content**: Content subject to frequent update is cached. When a user accesses a page with cached content, the content is provided from Sitecore cache.

3. Key Action Dates

Activity	Projected Date
Release of RFI	***August 19, 2021***
Due Date to Submit Questions Related to the RFI	***September 8, 2021***
Lottery Responds to Questions	***September 16, 2021***
Last Day to Submit RFI Responses	***October 1, 2021***

All RFI questions and responses must be submitted via email to the Procurement Services Support (PSS) unit at sclements@calottery.com. Questions must be submitted in Microsoft Word or PDF format.

4. RFI Format

Responses must include a cover page that identifies the following:

1. Company Name
2. Company Mailing Address
3. Company Representative's Name
4. Company Representative's Telephone Number
5. Company Representative's E-mail Address

5. Proposed Solicitation Requirements

The requirements provided in the table below provide a high-level basis for understanding what the Lottery needs for the maintenance, operation, support and development of PWS. Respondents are invited to comment on whether the requirements are clear, valid and provide an understanding of Lottery needs; respondents do not need to indicate in their response whether or not they currently meet them. In presenting these requirements in the RFI, the Lottery seeks input to understand where additional clarification or detail may be needed and to ensure that

these requirements represent reasonable scope and are not overly restrictive so as to inadvertently prevent qualified organizations from responding to future PWS service procurement solicitations.

Category	Business Area	ID No.	Type	Requirement
Transition	Staffing	1.1	Business	Contractor will meet qualifications and skills to ensure operational continuity, and support planned and unplanned activity throughout the contract's life.
Transition	Maintenance	1.1	Technical	Contractor, in consultation with Lottery and the current PWS support Contractor, will develop and execute a transition plan to ensure uninterrupted PWS operations and readiness to assume complete contract scope within three months of contract execution.
M&O	Maintenance	2.1	Technical	Contractor will provide 24/7/365 PWS' environment monitoring for health, performance, and security, triggering appropriate incident response protocol based on severity and impact.
M&O	Availability	2.2	Non-Functional	Contractor must ensure continued PWS High Availability, defined as 99.99% uptime. (please refer to Exhibit A-1, question 9)
M&O	Maintenance	2.3	Technical	Contractor will oversee and implement upgrades, patches, and fixes needed to ensure all hardware, software and products supporting the PWS environment are up-to-date and supported by their respective vendors.
M&O	Maintenance	2.4	Technical	Contractor will manage and maintain PWS API's and data transfers.
M&O	Support	2.5	Business	Contractor must manage/support the SiteCore platform for technical and non-technical users, including but not limited to product configuration, user account maintenance, end-user support, security compliance, network management, architecture, patches, template support and creation, product upgrades, incident response, performance tuning, and integrations.

Category	Business Area	ID No.	Type	Requirement
M&O	Maintenance	2.6	Technical	Contractor must manage/support the Azure cloud environment and all associated cloud environment components including but not limited to security monitoring, incident response, network connection management, site architecture, system patching, product upgrades, major incident response, infrastructure performance tuning, and integrations.
M&O	Maintenance	2.7	Technical	Contractor must manage/support the Azure Security Center and Application Insights to meet target score.
M&O	Maintenance	2.8	Technical	Contractor must provide support for and oversee PWS maintenance Web Application Firewalls (F5), including product upgrades, patching, performance tuning, and configuration management.
M&O	Maintenance	2.9	Technical	Contractor must provide support for and oversee PWS database maintenance and external data connections including but not limited to database configuration, security monitoring, incident response, database architecture, SQL upgrades and maintenance, integrations, and performance tuning.
M&O	Maintenance	2.10	Non-Functional	Contractor must regularly review performance to define tools, technologies, and practices to meet current and future performance needs including Azure Cloud Pools' possible use.

Category	Business Area	ID No.	Type	Requirement
M&O	Security	2.11	Technical	Contractor must oversee and ensure PWS environment security by applying security measures and configurations that follow recommended industry best-practice, such as: • *Approved network traffic enforcement* • *Local application logging* • *Transport encryption* • *Infrastructure-level DDoS protection* • *Malware protection* • *Access Key Management* • *Azure Security Center review and remediation* • *On-going WAF management and support* • *Vulnerability Scanning on PWS* • *Incident response support*
M&O	Capacity	2.12	Business	Contractor must conduct ongoing PWS capacity planning to ensure database and infrastructure resources meet or exceed current and future capacity needs.
M&O	Capacity	2.13	Business	Contractor will conduct PWS environment performance assessments and develop performance tuning plans to identify and address bottlenecks or other performance issues.
M&O	Support	2.14	Business	Contractor will create an incident management/response plan to be tested and revised in coordination with Lottery staff at least annually; with test results and recommendations provided to the Lottery.
M&O	Support	2.15	Business	Contractor will be responsible for PWS Disaster Recovery Plan's management and yearly updates, ensuring it meets Recovery Time (RTO) and Recovery Point Objectives (RPO), conducting periodic coordinated tests (annually) with Lottery staff to ensure its viability and effectiveness with results, and providing recommendations to the Lottery.

Category	Business Area	ID No.	Type	Requirement
M&O	Capacity	2.16	Business	Contractor will ensure PWS environment scalability and maintain plans to increase or reduce PWS resources as needed to support higher-than-normal traffic that occurs during high jackpots.
M&O	Support	2.17	Business	Contractor will provide real-time afterhours PWS performance monitoring and reporting during periods of higher-than-normal traffic during high jackpots.
M&O	Support	2.18	Technical	Contractor must manage, maintain, and conduct periodic recovery tests on environment backups at least annually to ensure they can be used to restore PWS in the event of a system failure; test results and provide recommendations to the Lottery.
DDI	Development	3.1	Business	Contractor must coordinate with Lottery technical and business stakeholders to plan and develop new integrations/ interfaces to support new features and business needs.
DDI	Development	3.2	Technical	Contractor will develop and deploy secure, custom code within SiteCore Platform following established work authorization and change management procedures.
DDI	Development	3.3	Business	Contractor will develop PWS code only as authorized and will not bill the Lottery for any work not specifically approved by the Contract Manager through established work authorization procedures.
DDI	Development	3.4	Business	Contractor will provide DDI ability to support all front-end and back-end development efforts, including unit testing and peer-based code review. DDI's scope can range from simple web page display modifications to new site functionality (ranging from ADA compliant new promotional displays to new interactive website experiences) and/or 3rd party system integrations.

Category	Business Area	ID No.	Type	Requirement
DDI	Testing	3.5	Technical	Contractor will develop automated test suite capabilities to conduct automated regression testing for all releases, features, and functions.
DDI	User Experience	3.6	Business	With design direction from Lottery and their Marketing Agencies, the Contractor to provide documented recommendations that enhance user experience through best practice design, development, and deployment methods.
DDI	Accessibility	3.7	Business	Contractor must monitor PWS to ensure continued PWS accessibility in accordance with State of California public agency website certification requirements (AB 434) and to maintain WCAG compliance, providing compliance certification and remediation plans as required.
DDI	Project Management	3.8	Business	Contractor must manage and track all M&O, Transition, DDI development efforts, including scope, schedule, cost, and resource hours in accordance with accepted Project Management Methodology.
DDI	Maintenance	3.9	Technical	Contractor must have the ability and tools to simulate normal production traffic and high load traffic in non-production environments for testing the performance impact of new features and releases.

6. Current PWS Tools and Supporting Systems

Name	Purpose
AppDynamics	Application Performance Management (APM) tool, monitors application infrastructure and gives code level visibility. Used for 3rd party API calls to see performance and verify everything is running in a healthy state
Azure Backup	Cloud environment backup
Azure Baston	Allows remote access
Azure Cosmos DB	Database for retailer related data for display on PWS
Azure DevOps	User Stories/ Code versioning/Release Management.
Azure Monitor	Aggregate and stores monitoring telemetry in log data store

Name	Purpose
Azure App Insight	Feature of Azure Monitor and is currently used to view code logs to determine errors on PWS. The Lottery has different levels of logging from informational to error logs and the tool is used to figure out where in code errors are occurring.
Azure Security Center	Infrastructure security management
CDN	Content delivery network or content distribution network. PWS leverages a primary and backup content delivery network to cache heavyweight content objects, such as videos, graphics, and downloadable assets in order to meet the high-performance requirements of the PWS. This content is referred to as the static PWS content.
Experian Address Validation	Address verification of Players input
Experian Email Validation	Email validation of Players input
Experian Name Search	Prevent Players from creating multiple accounts
Experian Precise ID	Verification of real person to meet player account requirements
F5's	Firewall: Manages all publishing of information feeding into CDN
Google Static Maps API	Online mapping functionality (GEO) within PWS. Mapping is used for the Retailer Search functionality on PWS. Google Static Maps API V2 is used to provide this functionality.
Pingdom	Monitoring of APIs
Send Grid	Email and auto responses to the Lottery's VCC system using SMTP relay server
Sensu	Virtual machine and other service monitoring Sensu is a telemetry and service health checking solution for multi-cloud monitoring at scale. It provides visibility into servers, services, and other connected services. All alerts generated in Sensu are displayed on the Lottery's front-end management tool, Uchiwa.
Sitecore CMS	PWS' CMS
Solr	Search Engine used to provide site-wide search functionality for the PWS
OpsGenie	Critical alerts monitoring checks are tied in via webhooks to the Lottery's "Incident Response" tool, OpsGenie. This tool ensures that Managed Services 24/7 on-call support team is notified when a critical alert is triggered. OpsGenie also handles the Managed Services team call routing to ensure that any calls which are placed to the Lottery's 24/7 support line are directed to the appropriate person. Escalation policies help to ensure that any missed alerts or calls are forwarded to management.

Name	Purpose
SQL DB	Databases to store game, player, and retailer data
Uchiwa	Dashboard for Sensu data
WinWatcher	Automated file transfer monitor. This tool processes files received from the Gaming System (for winning numbers, jackpots, retailers, etc.).

7. Exhibit A-1 Questionnaire

Please provide answers to the following questions, if you choose not to respond to a question, please indicate your lack of response.

1. Based on the information provided in this RFI, is there anything that would prevent you from bidding on an upcoming solicitation?
2. What details not provided in this RFI are needed for you to develop staffing and support plans that include Service Level Agreement (SLA), Level of Effort (LOE) and costs?
3. What methods/tools or best practices would you use or recommend in order to monitor and manage performance, security, backup status and scaling for a website and Azure hosted environment? (List of Current PWS Tools and Supporting Systems)
4. After reviewing the Lottery's requirements, and environment, what changes if any would you recommend and why? What changes would you recommend to effectively manage and assume operations from existing resources?
5. What are your recommendations and requirements to ensure an accessible, consistent user experience across all digital channels? Based on the information provided in the RFI would you recommend any changes?
6. After reviewing the Requirements please provide any feedback that you have on the stated services. Any additional information you provide may be used in future solicitations.
7. What skills and/or knowledge would you recommend including in the solicitation to ensure coverage of all support, maintenance and development needs described in this RFI?
8. After reviewing the Current PWS Tools and Supporting Systems table please provide any feedback you have on the current list and any suggestions you have for alternative tools or applications keeping in mind the dollar and time cost to transition and train staff.
9. Per Services ID 2.2 the Lottery seeks your input on the uptime requirement (9?.??%) with your response considering a balanced cost approach against business needs.
10. What information would you recommend the Lottery include in an upcoming solicitation that would ensure a well-rounded application security program to mitigate threat vectors like injection attacks, cross-site scripting, and other vulnerabilities as outlined in the OWASP Top 10 Web Application Security Risks? See Exhibit A-4 for access configuration.

EXHIBIT A-2 – California Lottery Information Security Standards

1. Information Security

The Contractor acknowledges and agrees that it may, in its performance of the Contract, collect, generate, and/or have access to information and data pertaining to or provided by the Lottery and/or its customers (collectively, "Lottery Data"). The Contractor also acknowledges and agrees that proper information security requires protecting the integrity, availability, and confidentiality of confidential, sensitive, and personal information and the resources used to enter, store, process and communicate such information.

To this end, in performing the Contract, the Contractor must establish and maintain adequate security controls, policies, standards, and procedures to prevent unauthorized access to, and protect the confidentiality, integrity, and availability of, Lottery Data, assets and services.

The Contractor must operate in accordance with California state and federal laws, and all other applicable laws, regulations and rules, as well as best industry practices, related to the protection of information assets and the timely and efficient management of security incidents, including corrective action.

2. Data Confidentiality, Integrity, Availability and Management

Lottery Data will be collected and retained by the Contractor only for legitimate business purposes associated with the Contract. All electronic Lottery Data, whether at rest or in transit, must comply with Lottery's Encryption Policy. The Contractor's data handling processes must, throughout the term of the Contract, comply with the Lottery's Information Security policies and Information Security Program Manual and meet or exceed the required level of protection. Copies of the applicable policies will be provided by the Lottery.

Upon Contract expiration or termination, or as directed by the Lottery during the term of the Contract, all Lottery Data in the Contractor's possession must be returned to Lottery or destroyed beyond recovery, at the Lottery's option. Such data destruction or return must be completed, at Contractor's cost and expense, within a mutually agreed upon timeframe, but in no case later 90 days after Contract expiration/termination.

3. Contractor Responsibilities

Information security must be ensured by the Contractor, as the Contractor may have physical or electronic access to the Lottery's confidential, sensitive, or personal information. This information may be contained in systems that directly support the Lottery's business operations. This includes IT hardware and software, and the services associated with the management, operations, maintenance, programming and system administration of computer systems, networks, telecommunications

systems, and social media. This also includes access to printed materials and other paper records.

The Contractor and all Contractor personnel must not use or redistribute any Lottery Data processed, stored, or transmitted by the Contractor, except as specified in the Contract or upon written Lottery approval.

4. Information Security Incident

The Contractor must disclose to the Lottery any Information Security Incident. An Information Security Incident is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits associated with the Lottery Contract.

The Contractor must notify the Lottery Contract Manager, the Lottery Deputy Director of Security/Law Enforcement (SLED), and the Lottery Information Security Office within two hours after discovery of the incident.

To the extent that the Information Security Incident includes or is reasonably believed to include the acquisition of personal information, as defined in California Civil Code section 1798.29, by an unauthorized person, Contractor must notify the Lottery Contract Manager, the Lottery Deputy Director of Security and Law Enforcement Division (SLED), and the Lottery Information Security and Privacy Office immediately following discovery.

If the Lottery determines that disclosure of an information security breach is required under section 1798.29, or any other applicable law or regulation, Contractor will diligently assist the Lottery in gathering all necessary information for the Lottery to comply with the disclosure requirements set forth therein. In addition, if the information security breach arises from the negligence or willful misconduct of the Contractor, or its agents, employees, or subcontractors, Contractor will reimburse the Lottery for any costs incurred in connection with the breach; such costs may include, but will not be limited to, the cost of preparing and delivering required notifications and up to 12 months of identity theft prevention and mitigation services for any California residents whose personal information may have been compromised, if the Lottery determines that such notifications and/or services are required by applicable law, consistent with industry standards or otherwise reasonably necessary to safeguard the Lottery's business standing or reputation.

5. Information Security Incident Contact Information:

Lottery Contract Manager
Lottery Deputy Director, Security and Law Enforcement Division (SLED)
Lottery Information Security and Privacy Office

6. Information Security Audit

The Contractor must keep audit logs of any access or other activities associated with Lottery information. Refer to the Information Security Program Manual, Security Audit Log (Event Log) Section for specific requirements.

The Lottery has the right to audit the Contractor's information security controls and associated plans and processes to verify compliance with the Contract.

7. Physical Security

The Contractor must take appropriate measures, including without limitation those set forth below, to prevent the loss, theft, damage, and misuse of all equipment associated with the Lottery Contract.

The Contractor must take reasonable measures to minimize the possibility of equipment damage or other disruptions to service from any line voltage fluctuation or power loss and to ensure the continued operation of all Lottery systems and operations in the event of a failure of a public electric distribution system providing service to the Contractor.

The Contractor must safeguard all information systems equipment and data facilities used in the performance of the Contract against fire or water and will maintain and monitor fire and moisture detection systems. Alarms will be monitored on site and by a 3rd party alarm service on a 7-day-per-week, 24-hour-per-day basis. The alarm company will perform regularly scheduled maintenance and testing of all monitoring and alerting equipment.

The Contractor must safeguard all information systems and data center facilities against high temperatures and inappropriate humidity. Temperature and humidity must be maintained within the range specified by the manufacturer.

8. Security Plan

The Contractor must provide, within 10 days after the execution of the Contract, and shall maintain and follow throughout the term of the Contract, a Security Plan that identifies implemented administrative, physical and technical security controls that will properly protect information at a level that is proportionate to the criticality and sensitivity of the information. The Lottery uses the following most current standards and guidelines for identifying the sensitivity, classification, and the recommended security controls necessary to protect the information:

Federal Information Processing Standards (FIPS) 199
National Institute of Standards and Technology (NIST) Special Publication 800-53
Publications of the ISO/IEC 27001, ISO/IEC27002
The Contractor's handling of Lottery Information Assets must be consistent with the foregoing standards and guidelines and with all the Lottery's obligations thereunder. After the Contractor has submitted its initial Security Plan, the Contractor will be

responsible for submitting updated Security Plans on an annual basis, within 30 days after the anniversary of the Contract start date. The Security Plan must be submitted to the Lottery for approval, identifying the security considerations and controls, and naming a designated Information Security Officer (ISO) for the operations of the Contractor under the Contract. For the duration of the Contract term, the Lottery may also require the Contractor to update the Security Plan at any time and submit it to the Lottery for approval, if the Lottery determines that a significant change to the deliverables necessitates an update to Contractor's security controls.

If the Contractor has engaged services from a subcontractor or uses the services of a subsidiary as part of the Contract, it is the Contractors responsibility to ensure that these parties also provide to the Lottery a Security Plan consistent with the Lottery's Information Security requirements and comply with such plan.

9. Security Plan Requirements

The Security Plan must designate Contractor personnel and staffing profiles to ensure that there is a clear "separation of duties" throughout the Contract Term. Separation of duties is the principle of not allowing one person to be responsible for completing or controlling a task, or set of tasks, from beginning to end when the potential for fraud, abuse or other harm exists.

The Security Plan must also demonstrate how the Contractor complies with the concepts of "least privilege" and "need to know;" an individual Contractor or Contractor group must only have access to the systems and information required for their tasks, access must be limited to only the information required to perform their role, and broad system privileges that may put Lottery information at undue risk must not be granted.

Contractor supervisors and management must ensure adherence to the approved Security Plan.

The Security Plan must include, at a minimum, security measures and program safeguards to ensure that the information and systems developed, acquired, operated, maintained and/or used by the Contractor and Contractor personnel provide the following:

1. Protection from unauthorized access, alteration, disclosure, misuse of information processed, stored, or transmitted, and misuse of administrative privileges.
2. A Business Continuity and Disaster Recovery plan (See "Business Continuity and Disaster Recovery Planning" below) in the event of a major system failure, information security incident or disaster.
3. Appropriate management, administrative, operational, technical, and environmental controls sufficient to provide cost-effective assurance of the information's confidentiality, integrity, and availability.
4. Hardening and secure configurations of network devices, servers, applications,

operating systems, services, and other information technology resources.

5. An Antivirus protection program, operating system patching program, and application patching program for all information systems and resources under their control.
6. A network intrusion detection and prevention program as well as a continuous vulnerability management and remediation program for all information technology resources under their control.
7. A security incident response plan for handling suspected information security incidents and breaches, including incident escalation and corrective actions.
8. A fully implemented information security training and privacy awareness program.
9. Maintenance, monitoring and analysis of access rights, as well as security and audit logs.
10. An independent review of the management, administrative, operational, and technical controls to provide assurance that these controls are in place and are effective.
11. The Contractor must ensure adherence to the approved Security Plan at all times.

10. Business Continuity and Disaster Recovery Planning

The Contractor must maintain data backup and recovery processes for all critical Lottery Data as defined by the Lottery, according to the specifications provided by the Lottery. The specifications will include, without limitation, the applicable Recovery Time Objectives (RTO) for the Contractor to meet when restoring a service, application, or system. The specifications will also include the applicable Recovery Point Objectives (RPO) that define the amount of information or data loss the Lottery will accept due to service disruptions such as data corruption or system outages. Backed up data or copies of data must be stored securely and geographically separated from the original data. All copies must be verified to be accurate and operational. Restoration systems must be tested at least once per month, and all backup and restoration exceptions must be corrected as soon as possible. Tests and all exceptions will be logged for 30 days and made available to the Lottery for review when requested. Major backup exceptions spanning more than five days, or restoration test failures, must be reported to the Lottery Contract Manager when they occur.

The Business Continuity and Disaster Recovery Plan must cover a minimum of four topic areas: (1) summarization of strategy for managing disaster situations; (2) distinct management and staff assignment of responsibilities immediately following a disaster and continuing through the period of re-establishment of normal operations; (3) prioritization for the recovery of critical systems; and (4) operational procedures documented in a systematic fashion that will allow recovery to be achieved in a timely and orderly way. The plan must be adapted to suit the Lottery's needs.

11. Rights to Lottery Data

The parties agree that as between them, all rights, including all intellectual property rights, in and to Lottery Data (including but not limited to any information, formulae, algorithms, or other content uploaded, created, collected, provided, transmitted or modified by the Lottery, its employees, agents, or end users, or by the Contractor on behalf of the Lottery, in connection with the Contract) shall remain the exclusive property of the Lottery; Contractor has a limited, non-exclusive license to access and use the Lottery Data as provided to Contractor solely for performing its obligations under the Contract. Nothing herein shall be construed to confer any license or right to the data, including user tracking and exception data within the system, by implication, estoppel or otherwise, under copyright or other intellectual property rights, to any third party. Unauthorized use of data by Contractor or third parties is prohibited. For the purposes of this requirement, the phrase “unauthorized use” includes the data mining or processing of data stored or transmitted by the Contractor for unrelated commercial purposes, advertising, or advertising-related purposes, or for any other purpose that is not explicitly authorized by the Lottery.

12. Data Location

All Lottery Data maintained by the Contractor or its subcontractors, and any Contractor or subcontractor data center where Lottery Data is stored, must be physically located within the continental United States.

13. Remote Access

Remote access to Lottery Data from outside the United States is prohibited, unless approved in advance in writing by the Lottery.

EXHIBIT A-3 – IT PROVISIONS

1. DELIVERABLE REVIEW, ACCEPTANCE, AND REJECTION:

Unless otherwise specified or defined in the Contract or Statement of Work, the Lottery's requirements for deliverable acceptance and quality assurance, is set forth below:

2. Definitions

Deliverable – Tangible or intangible Contractor requirement to be produced during the term of the Contract. Deliverables may be either an outcome to be achieved or an output to be provided.

Quality Assurance System – Any systematic process of determining whether services and deliverables meet specified Lottery requirements, standards, procedures, and industry best practices.

Contractor will complete each Deliverable in accordance with the terms of this Contract. In each instance, the Lottery will determine whether the Deliverable is acceptable according to this provision or as specified in the Statement of Work (SOW). In the event of a conflict, the SOW's requirements prevail over this provision and other terms and conditions in the Contract. The Lottery will notify Contractor of any deliverable deficiencies found during the performance of this Contract, and Contractor will have the opportunity to cure such deficiency or errors in accordance with the process described under this provision or the SOW.

3. Deliverable Expectations

Prior to starting work on each Deliverable, the parties will mutually agree on the acceptance criteria that will be used for each Deliverable. The criteria will be incorporated into the SOW's requirements for acceptance of each Deliverable. However, if the acceptance criteria cannot be established upon approval of the SOW, acceptance criteria will be agreed to by both parties via email before the completion of the final Deliverable.

4. General Requirements

a. Contractor will provide and maintain a Quality Assurance System acceptable to the Lottery covering all Deliverables under this Contract or SOW and will only provide Deliverables that have been reviewed and found to conform to this Contract's or SOW's requirements. Contractor will keep records evidencing its reviews and their results and will make these records available to the Lottery during the Contract term and for four years thereafter. Contractor shall allow the Lottery to review procedures, practices, processes, and related documents to determine the acceptability of Contractor's Quality Assurance System or other similar business practices related to performance of the Contract.

b. All Deliverables may be subject to review and testing by the Lottery or its authorized representatives.

c. Contractor shall provide all reasonable facilities for the safety and convenience of the Lottery during record reviews at no additional cost to the Lottery. Contractor shall provide the Lottery with all information and data as may be required to perform their record reviews.

d. All Deliverables may be subject to final review, testing and acceptance by the Lottery at destination, notwithstanding any payment or inspection at source.

e. The Lottery shall give written notice of rejection of any Deliverables or services performed hereunder within a reasonable time after receipt of such Deliverable or performance of such service. The rejection notice will state why the Deliverable does not substantially conform to the acceptance criteria. If the Lottery does not provide such notice of rejection within a reasonable time after delivery, such Deliverable or service will be deemed to have been accepted. Acceptance is final, except as it relates to latent defects, fraud, and gross mistakes amounting to fraud. Acceptance shall not be construed to waive any warranty rights that the Lottery might have at law or by express reservation in this Contract with respect to any nonconformity.

5. SAMPLES:

a. Samples of deliverables, including, but not limited to, wire frames, may be required by the Lottery for inspection and specification testing and must be furnished free of expense to the Lottery. The samples furnished must be identical in all respects to the Deliverables specified in the Contract.

b. Samples, if not destroyed by tests, may, upon request made at the time the sample is furnished, be returned at the Contractor's expense.

6. FUTURE RELEASES:

Unless otherwise specifically provided in this Contract, or the SOW, if improved versions, e.g., patches, bug fixes, updates or releases, of any Deliverable are developed by Contractor, and are available to other agencies or clients, they will be made available to the Lottery at no additional cost during the term of the Contract. If Contractor offers new versions or upgrades to its Deliverables, they shall be made available to the Lottery, at the Lottery's option, at a price no greater than the current Contract hourly billing.

7. ENCRYPTION/CPU ID AUTHORIZATION CODES:

a. When Encryption/CPU Identification (ID) authorization codes are required to operate the deliverables, Contractor will provide all codes to the Lottery with delivery of the deliverables.

b. In case of inoperative CPU, Contractor will provide a temporary encryption/CPU ID authorization code to the Lottery for use on a temporarily authorized CPU until the designated CPU is returned to operation.

c. When changes in designated CPUs occur, the Lottery will notify Contractor via telephone and/or email of such change. Upon receipt of such notice, Contractor will issue via telephone and/or email to the Lottery within 24 hours, a temporary encryption ID authorization code for use on the newly designated CPU until such time as permanent code is assigned.

EXHIBIT A-4 – Current Network and Infrastructure Administration Configuration

1. **Network/Security Administration:**

   The Lottery provides all PWS Security and Network Administrative staff with Lottery Active Directory accounts. Using their Lottery account credentials Network/Security Administrators connect to the Lottery Jump Box via VPN. From the Jump Box, Administrators can access the internal WAF configuration management interface where they can monitor and view connections to PWS component systems.

2. **Infrastructure Administration:**

   Using their Lottery account credentials Infrastructure Administrators connect to the Lottery Jump Box, which allows authorized access to the VM Ware infrastructure, including database, content management, and security monitoring tools.