Request for Proposal: Web Application Firewall Services

February 12, 2020

1. Introduction

The **Department of the Lottery,** www.illinoislottery.com, awarded the Private Management Agreement ("PMA") to Camelot Illinois LLC ("Camelot Illinois") on September 22, 2017 following a bid submission. Following the Notice of Award, the PMA was executed on October 13, 2017.

Camelot Illinois, as part of an overall business strategy, plans to implement a new web-based application firewall and inherent security measures system. As such, the goal of this Request for Proposal: Web Application Firewall Services ("RFP") is to enter into one or more contracts with a vendor who will provide Camelot with web-based firewall services (collectively, the "Services") to alert, detect, monitor and mitigate application layer cyber-attacks on Camelot Illinois publicly accessible websites.

2. Instructions

This RFP invites interested organizations to submit a response to this RFP ("Proposal").

The requirements for the Proposal are set forth in Section 7 of this RFP.

2.1 Timetable

Proposals must be submitted by March 20, 2020 to the attention of: procurement-services@camelotillinois.com

The RFP milestones are as follows:

Issue RFP	February 12, 2020
Last Date for Vendor Questions	Mar 2, 2020@5:00 pm CT
Answers to Vendor questions posted	Mar. 9, 2020
Vendor intends to submit a Proposal	Mar. 13,2020 @5:00 pm CT
RFP submission date	Mar. 20,2020 @5:00 pm CT

Request for Proposal: Web Application Firewall Services

Estimated Date of Award *(subject to contract)*	April 3, 2020

Camelot Illinois reserves the right to make any necessary amendments to the above timetable. Any such changes will be posted on the Illinois Lottery website and Camelot Illinois's website. Companies that submit Proposals ("Vendors") will be notified in writing of any changes to these dates. **Please note that Proposals submitted late will not be considered**.

2.2 Contacts

Please submit any questions via email to procurement-services@camelotillinois.com. Questions regarding this RFP must be emailed before March 2, 2020 at 5:00 pm CT. A consolidated response to any questions received will be posted on the both the Illinois Lottery website and Camelot Illinois's website under the Business Opportunities tab[1] and will be made available to all Vendors without identifying the Vendor that asked the question. Camelot Illinois reserves the right to decline to answer specific questions.

2.3 Vendor Intends to Submit a Proposal

Vendors are required to notify Camelot Illinois that they intend to submit a Proposal via email to procurement-services@camelotillinois.com by March 13, 2020 at 5:00 pm CT.

2.4 Response Format

Please provide the following information on the cover page of Vendor's Proposal and ensure that Vendor's name appears on each subsequent page of the document:

   A. Vendor's Name;
   B. Vendor's Address;
   C. Contact Name;
   D. Contact Job Title;
   E. E-mail Address; and
   F. Telephone Number.

Ensure that Vendor's Proposal follows Camelot Illinois's format (e.g., numbering answers in the format of this document). Failure to do so may result in the Proposal being misinterpreted or missed. Please answer all questions fully. Proposals should be delivered in electronic format via email to procurement-services@camelotillinois.com

The Proposal should explain how the Vendor could support Camelot Illinois in the achievement of its objectives.

---

[1] http://www.illinoislottery.com/en-us/Business_Procurement_Opportunities.html

Request for Proposal: Web Application Firewall Services

Where possible, the Proposal should also include the following:

A. Innovative ideas on meeting Camelot Illinois requirements;
B. Why Camelot Illinois should choose you as a Supplier; and
C. How your space / design differs from the competition.

3. Conditions of the RFP

3.1 General Considerations

The issuance of this RFP does not constitute a legal offer capable of acceptance.

Camelot Illinois reserves the right to reject any or all of the Proposals submitted, or to withdraw this RFP at any time. Camelot Illinois also reserves the right to accept a Proposal from Vendors in part only.

Camelot Illinois will not be liable for any costs incurred by any Vendor in connection with the preparation of a response to this RFP, or for any costs incurred for attendance at meetings, presentations, clarifications or demonstrations.

The numbering of this RFP is an important aid in the evaluation process. Please utilize it within Vendor's Proposal, as this may affect Camelot Illinois's evaluation of it.

Vendors may not take advantage of any apparent error or omission in this RFP. In the event that any errors or omissions are discovered, a Vendor shall notify Camelot Illinois immediately.

Please provide complete and accurate information against the specifications contained within this RFP. If Vendor is unable to meet any requirements, then this should be clearly noted in the appropriate response section(s). Any assumptions within Vendor's Proposal should be clearly stated.

Any commitment made in a Proposal will be binding on the applicable Vendor. A commitment includes any guarantee or representation made in the Proposal, accompanying documentation or subsequent negotiation.

3.2 Confidentiality

Subject to Appendix A - Private Manager Agreement Incorporated Terms ("Incorporated Terms"), of this RFP, any information disclosed in, or in connection with this RFP becomes the property of Camelot Illinois, subject to the Vendor's redaction of confidential, proprietary, or other sensitive material in accordance with the PMA and State Policies and Rules (defined in the Incorporated Terms). Such information will be available to the public in accordance with State Policies and Rules. The failure to designate any materials as "proprietary and confidential" at the time of delivery of such information to Camelot Illinois does not prohibit the Vendor from subsequently designating any information as proprietary and confidential. However, this designation does not necessarily exempt such information from disclosure under the Freedom of Information Act, 5 ILCS 140/1 *et seq*.

Request for Proposal: Web Application Firewall Services

3.3 Employment

From the time this RFP is issued until either (i) six (6) months after the award of a contract pursuant to this RFP or (ii) the rejection of all Proposals received by Camelot Illinois, Vendors are prohibited from officially or unofficially making any employment offer or proposing any business arrangement with Camelot Illinois' employees.

3.4 Compliance

Failure to comply with any specific instructions detailed in this RFP may, at Camelot Illinois's discretion, exclude the Vendor from further consideration in the process.

3.5 Selection of Supplier

Any Proposal that fails to meet the requirements set forth in this RFP will be disqualified.

The table below defines the evaluation criteria and the relative importance of each criteria that will be used to evaluate the Proposals. The requirements are identified in Section 7 of this RFP.

Proposal Elements	Relates to requirements	Maximum # of Points Possible
Company Information	C1 – C5	15
Deployment Mode, Connection Handling & Traffic Processing	R1 – R14	25
Detection and Protection Techniques	R15 - R34	30
Logging and Reporting	R35 – R48	30
Management, Performance and Support	R49 – R64	20
Pricing Schedule	P1- P6	30
TOTAL		**150**

Camelot Illinois reserves the right to adjust selection criteria until March 4,2020. Any such changes will be posted on the Illinois Lottery website, no later than March 6,2020 to permit any necessary refinement of Proposals prior to submission. Camelot Illinois will notify all Vendors who have submitted an intent to submit a Proposal of all changes via notice posted on both the Illinois Lottery and Camelot Illinois' websites.

Camelot Illinois' selection of a winning Vendor ("Supplier") will be determined by the highest overall score achieved based on the above criteria and, if appropriate, updated following any presentations. Camelot Illinois's decision will be final.

Request for Proposal: Web Application Firewall Services

3.6 Terms and Conditions

Vendors should note that any contract award will also be subject to Camelot Illinois' terms and conditions.

Camelot Illinois operates within a regulated environment, and it is a requirement of the PMA that Suppliers be vetted or approved by the State regulator in advance. Accordingly, the prospective Supplier must complete State disclosure and certification documents, located at https://ipg.vendorreg.com/. For further information about this requirement, please email procurement-services@camelotillinois.com.

The PMA requires Camelot Illinois to pass through various non-negotiable provisions to all Suppliers. Camelot Illinois will achieve this by including a separate exhibit of the Incorporated Terms in the Supplier's contract. The Incorporated Terms will take priority over any conflicting term in the rest of the contract. Refer to Appendix A of this RFP for the Incorporated Terms.

From the time this RFP is issued until the end of the contract term, the Supplier represents and warrants that it shall neither   (i) be debarred or prohibited from doing business with the State of Illinois for any reason; nor (ii) likely to have a material and/or adverse effect on the interests of the Illinois Lottery.

Camelot Illinois is looking to establish a contract for an initial term of five (5) years, subject to the Supplier's performance and Camelot Illinois's evolving requirements and strategy.

3.7 Validity of Proposal

Proposals shall be binding offers, binding for a period of ninety (90) days from the date the Proposal is submitted.

Request for Proposal: Web Application Firewall Services

4. Estimated Timings

4.1 Web Application Firewall Services

This RFP seeks the implementation, launch and ongoing operation of a web application firewall. The Supplier should be able to provide services around the list of capabilities identified under requirements Section 7 listed below.

The Supplier will be required to (1) remain engaged with Camelot Illinois during the implementation period and (2) ensure that required security monitoring services and measures are at an operational capacity at an agreed upon date, prior to the go-live date.

5. Response Approach and Format

Vendors are requested to provide the following:
- A. A completed version of the Company Information section, with brief responses;
- B. A completed version of the Requirements section with full responses against each requirement (where applicable); and
- C. A completed pricing schedule with any variation included at the end.

Where necessary, Vendors may supplement responses with additional material but should ensure that the material focuses on the information requested and references the section for which it applies. (Camelot Illinois may be unable to search through generic material in an attempt to find relevant information).

If the Vendor must exclude some requirements from its Proposal, this should be accompanied by a clear statement of which items are excluded and the rationale.

If the Vendor wishes to propose additional services, not mentioned in the requirements, in order to supply a full-service solution, please provide a clear statement regarding the additional services and the rationale.

Request for Proposal: Web Application Firewall Services

6. Vendor Information

Please provide the following information about the Vendor:

#	COMPANY INFORMATION	Response
C-1	Vendor's Name.	Answer in Full
C-2	Vendor's background, including details of ownership.	Answer in Full
C-3	Summarize Vendor's experience relevant to the requirements.	Answer in Full
C-4	Highlight strengths and points of difference between Vendor and its competitors.	Answer in Full
C-5	Describe the resources that will be allocated to support Camelot Illinois and Vendor's overall organizational structure. (If Vendor is selected to make a presentation, the people who would have day-to-day involvement with Camelot Illinois should make up a significant part of the presentation team).	Answer in Full

7. Requirements

Vendor should answer the following requirements in full by describing how Vendor would address and/or resolve each requirement.

If Vendor is unable or unwilling to address and/or resolve a requirement, then respond with a "Reject" for the requirement. The Vendor may also offer any mitigating circumstances or alternative approaches; however, such responses may not be accepted as compliant.

#	DEPLOYMENT ARCHITECTURE & MODE OF OPERATION	Response
R-1	Describe the product architecture and how it is deployed to customer environments from start to finish.	Answer in Full
R-2	Explain the SSL/TLS traffic processed and offloading activities. Provide information on whether the web-application firewall terminates SSL connections, passively decrypts traffic etc.	Answer in Full
R-3	Describe the authentication method used to validate users/customers and whether multi-factor authentication is available.	Answer in Full
R-4	Discuss the capability to integrate with current DDOS protection through Radware.	Answer in Full

Request for Proposal: Web Application Firewall Services

R-5	Describe the company's ability to protect multiple websites by domain IP addresses.	Answer in Full
R-6	Describe the company's capability to store data solely in the United States.	Answer in Full
R-7	Reserved	
R-8	Reserved	

#	CONNECTION HANDLING & TRAFFIC PROCESSING	Response
R-9	Describe how traffic is blocked (e.g., Drop Packet or TCP Reset) and the company's ability to silently drop traffic without sending back TCP RESET to the traffic request origin.	Answer in Full
R-10	Describe how a customer turns off information they do not want to log or masks potentially sensitive information or PII. (e.g., response filtering).	Answer in Full
R-12	Describe how the product decrypts and re-encrypts SSL/TLS traffic.	Answer in Full
R-13	List any additional products required to operate Vendor's product (e.g., new hardware or software).	Answer in Full
R-13	Reserved	
R-14	Reserved	

#	DETECTION TECHNIQUES	Response
R-15	Describe the normalization techniques used.	Answer in Full
R-16	Describe how false positives are minimized.	Answer in Full
R-17	Describe any machine learning algorithms or AI Vendor's product uses that may detect signatures and vulnerabilities outside of typical signature-based threat detection techniques.	Answer in Full
R-18	Describe whether the product allows custom rule creation by the customer. For example, will it alert customers of events with regular expressions or other coding techniques or scripts.	Answer in Full

Request for Proposal: Web Application Firewall Services

R-19	Discuss the frequency of the database updates of signatures and customized rules/zero days, etc.	Answer in Full
R-20	Describe the availability of APIs to customize or extend Vendor's detection functionality.	Answer in Full
R-21	Describe how Vendor's product performs geographic blocking.	Answer in Full
R-22	Describe whether Vendor's product allows customization rules per webpage. If so, is the customer able to block all non-US traffic to only the "payments/login" pages of a website?	Answer in Full
R-23	Reserved	
R-24	Reserved	

#	PROTECTION TECHNIQUES	Response
R-25	List and describe any protection techniques used against brute force attacks.	Answer in Full
R-26	List and describe any protection techniques used against cookie-based attacks.	Answer in Full
R-27	List and describe any protection techniques used against session or denial of service attacks.	Answer in Full
R-28	List and describe any techniques used against hidden form field protection.	Answer in Full
R-29	Describe how Vendor's product receives threat intelligence from other industry threat databases or intelligence feeds.	Answer in Full
R-30	List and describe any protection techniques used for protection against application layer DDoS attacks? Does the product have any out of the box layer 7 DDOS protection through the typical web app firewall offering or is an additional purchase/subscription required?	Answer in Full
R-31	List and describe any protection techniques used for DNS Tampering protections.	Answer in Full
R-32	List and describe any protection techniques used for protection against OWASP Top 10.	Answer in Full
R-33	Reserved	
R-34	Reserved	

Request for Proposal: Web Application Firewall Services

#	LOGGING	Response
R-35	Discuss whether Vendor's product allows log forwarding Alert Logic.	Answer in Full
R-36	Describe any unique transaction IDs included with every log message.	Answer in Full
R-37	Can Vendor's product provide critical notification via email?	Answer in Full
R-38	Discuss whether long logs are retained. If so, how long are they retained?	Answer in Full
R-39	Describe how the product provides audit logging of administrator events.	Answer in Full
R-40	Reserved	
R-41	Reserved	

#	REPORTING	Response
R-42	Provide a brief description of the different types of report formats available.	Answer in Full
R-43	Describe on-demand report generation, automation, and scheduling.	Answer in Full
R-44	Describe the report distribution methods.	Answer in Full
R-45	Discuss whether Vendor's product provides a customized block page or maintenance display message.	Answer in Full
R-46	Describe Vendor's compliance reports (e.g., PCI DSS compliance checks).	Answer in Full
R-47	Reserved	
R-48	Reserved	

Request for Proposal: Web Application Firewall Services

#	MANAGEMENT	Response
R-49	Describe the product's graphical user interface dashboards.	Answer in Full
R-50	Describe how Vendor's product supports external APIs.	Answer in Full
R-51	Describe the product's configuration management & backup procedures.	Answer in Full
R-52	Describe whether the product provides automatic signature updates.	Answer in Full
R-53	Describe the functionality of the product's policy management, export/import, and roll back mechanism.	Answer in Full
R-54	Describe the product's ticketing system integration capability and indicate whether it integrates with JIRA .	Answer in Full
R-55	Reserved	
R-56	Reserved	

#	PERFORMANCE	Response
R-57	Describe if any expected latency from the web application firewall could affect Camelot's website and/or impact throughput.	Answer in Full
R-58	Provide information on the maximum number of concurrent connections the product supports.	Answer in Full
R-59	Describe the product's fail-safe and pass through when the device/system fails.	Answer in Full
R-60	Reserved	
R-61	Reserved	

#	SUPPORT	Response
R-62	Describe the quality and availability of technical support,	Answer in Full

Request for Proposal: Web Application Firewall Services

R-63	Describe where Vendor's support originates.	Answer in Full
R-64	Does Vendor provide direct support or utilize partners?	Answer in Full

8. Pricing

8.1 Pricing assumptions

All prices should be quoted in USD.

Please provide as much background as possible on the pricing, including any explicit assumptions related to these requirements and any factors outside of this RFP. Itemization of prices is encouraged where applicable.

It is anticipated that requirements may change to meet service needs over time, so any limits, constraints, or areas where flexibility is included in the pricing schedule should be highlighted.

8.2 Pricing Table:

Vendors should format their pricing response as follows:

Section	Description	Assumptions / basis of pricings	Price (USD)
P-1	Initial Costs		
P-2	Support Costs		
P-3	Setup & Implementation Fees		
P-4	Recurring Subscription Costs		
P-5	Patch Update & Upgrade Costs		
P-6	Any other fees or costs		

Request for Proposal: Web Application Firewall Services

9. Business Enterprise Program ("BEP")

Camelot Illinois encourages BEP Vendors (i.e., minority-owned, women-owned, and persons with disabilities-owned businesses) to submit Proposals for participation in this procurement. To learn more about this program, please visit the Illinois Department of Central Management Services website at https://www2.illinois.gov/cms/business/sell2/bep/Pages/Default.aspx to learn more about this program and/or register as a BEP vendor, if you have not done so already.

Request for Proposal: Web Application Firewall Services

Private Manager Agreement Incorporated Terms

See the Incorporated Terms (Appendix A), available as a separate pdf file on the Illinois Lottery website (https://www.illinoislottery.com/illinois-lottery/major-procurement-opportunities).

Vendor should review these terms and be certain that they are willing to submit to the terms as written, as they will be included as an exhibit to the Supplier's contract.

Request for Proposal: Web Application Firewall Services