

**REQUEST FOR PROPOSAL
FOR
INFORMATION SECURITY AUDIT
SERVICES**



**RHODE ISLAND LOTTERY
1425 PONTIAC AVENUE
CRANSTON, R.I. 02920
401-463-6500**

SECTION A - GENERAL INFORMATION

1. LOCATION

- A. The Division of Lotteries of the Rhode Island Department of Revenue (hereinafter "RIL") is located at 1425 Pontiac Avenue, Cranston, Rhode Island 02920.

2. BACKGROUND

- A. The purpose of this Request for Proposal (RFP) is to obtain proposals from vendors experienced in information security controls to perform an information security audit concentrating on external and internal network risk assessment.
- B. The RIL was constitutionally created on November 6, 1973. Legislation to start the RIL was passed in March of 1974, and the RIL began in May of 1974.
- C. The RIL has approximately 81 employees, organized under the following divisions: Office of the Director, Finance, Marketing, Security, Video RIL and Table Games. The RIL has approximately 1,200 retailers throughout the State selling RIL products.
- D. The RIL currently operates four types of games – instant tickets, several online games (Powerball, Numbers, etc.) Video Lottery Terminals (VLT), and Table Games. The processing for the instant ticket games, online games and VLT gaming facilities is managed and operated by IGT Corporation, whose headquarters are located in Providence, Rhode Island. IGT has a data processing center located in the RIL Headquarters Building in Cranston, Rhode Island. The VLT gaming facilities that interface with IGT are located in Lincoln (Twin River Casino) and Newport (Newport Grand), Rhode Island. Casino style table games are only available at Twin River Casino. Systems that support table game operations are owned and operated by Twin River Casino.
- E. The RIL maintains a 10/100 Ethernet local area Windows 2012 network. IGT maintains a 10/100 Ethernet local area Windows 2008 network for supporting the gaming system. The online host systems are running AIX and the video host systems are using LINUX. All of the game processing is performed by the IGT online/video systems. The RIL and IGT networks are Cisco based networks. The RIL and the IGT data center are located within the same building. It is important to distinguish that the RIL maintains a separate internal network from the IGT gaming system network.

- F. The RIL is subject to one annual external audit by the Rhode Island Auditor General's Office.

3. LENGTH AND TYPE OF CONTRACT

- A. The terms of this contract shall commence on the execution date of the contract. The maximum term of the engagement will be up to three (3) years, and the RIL reserves the right to terminate the contract within the engagement period.
- B. The RIL reserves the right to accept proposal(s) in whole or in part and to negotiate terms, conditions, and provisions in addition to those stipulated in this RFP.
- C. The RIL reserves the right to award this contract on price alone.
- D. The laws of the State of Rhode Island, including the State's General Conditions of Purchase, shall govern any contract(s) resulting from this RFP.
- E. Prior to final award, if successful vendor is out of state, the vendor will be required to file an "Application for Certificate of Authority as a Business Corporation/Foreign Business Corporation" with the Rhode Island Secretary of State's Office; website address www.sos.ri.gov.
- F. It is the policy of the RIL to make every effort possible to assure the participation of small, minority, and female-owned businesses pursuant the General Laws of the State of Rhode Island.
- G. The purpose of this agreed upon procedures engagement will focus primarily on IGT's compliance with policies, standards, and practices adopted by the RIL to safeguard all computerized aspects of the RIL games. This engagement must also evaluate the security posture of IGT's systems and the associated networks they communicate on.
- H. IGT's policies and procedures must be reviewed and compared to the RIL existing policies, standards and procedures to ensure that IGT is in compliance with these published standards. Further, the winning vendor is to review all IGT and RIL security policies, standards and procedures to identify any additional areas where information systems security controls could be improved or enhanced. The RIL will provide all external audit reports to the vendor selected to perform this security audit.
- I. The RIL plans to conduct a pre-bid conference to answer questions relating to the specific and technical details of the engagement.

SECTION B – WORK TO BE PERFORMED

1. INFORMATION SECURITY STANDARDS

- A. The RIL has listed below the *Information Security Standards* included in the scope of this engagement. The RIL requests that each standard be priced separately in submitted bids to offer some flexibility in the priority and scheduling of their evaluation, as well as a total cost for performing the entire evaluation.
1. *System and Application Development Resources* must be protected accordingly to ensure only authorized personnel may access such resources. Change management, version and distribution controls should be in place for all implemented systems and applications. All system and application development or modifications must be supported by a thorough, documented test plan; and only applications completing the test plan and approved by the RIL Information Security Administrator should be implemented into production. Program directories and files must be secured with appropriate file access permissions granting the least required privileges, rights, and attributes.
 2. *Local Area Network Administration* by IGT should adhere to the following standards:
 - a. All nodes should be registered on the network.
 - b. All remote users must be properly and securely authenticated by the accessed network.
 - c. Verify if remote sessions are properly logged, reported, and reviewed.
 - d. IGT employee exiting procedures, whether terminated or voluntary, are to be followed to disable user account access.
 - e. All dial-up/remote passwords must be periodically changed.
 - f. A list of persons issued dial-up/remote passwords should be maintained.
 - g. Gateway accounts permitting remote access must be disabled until access is needed.
 - h. Policies for the management of routing and bridging should be operational.

- i. Configurations defined on firewalls, routers, switches, and other hardware should be operational to ensure that no individual can gain unauthorized access to these devices.
 - j. IGT network configurations cannot be taken offsite and must be reviewed onsite.
 - k. Procedures to enforce network security policies should be operational.
3. *User Account Management and Administration* should adhere to the following guidelines:
- a. Each user must have a personal account with a unique login name, password, and user identification code.
 - b. Accounts with System Administration privileges should only be used when these duties are required to be performed. System Administrators should utilize their personal account for normal user activities.
 - c. All “Guest” type accounts should be deactivated.
 - d. Accounts not used for thirty (30) days must be disabled for login and removed from the system when it is determined that the user no longer needs access.
 - e. After a predetermined number of logon attempts, the user ID being utilized must be automatically disabled by the system, and the System Administrator should be notified.
 - f. Identify system accounts that are needed for the system to operate.
 - g. Each system using passwords to protect an account should have an acceptable password policy. The policy should have a set number of days till expiration, length requirement of at least 8 characters, and requirement of special characters, spaces, and numbers. The character set used should not be a limiting factor.
 - h. Test accounts should be limited and controls should be in place to describe purpose of test account, who requires the test account, and how long the test account will be active. There should also be details describing the test accounts access to systems, how the account is monitored, and who has access to the test account.

4. Detail the effectiveness of the central system provider's current process of performing *Information Security Responsibilities*. Responsibilities include, but are not limited to:
 - a. Ensuring that RIL security standards, guidelines, and policies have been implemented and are being adhered to.
 - b. Ensuring IGT performs a gap analysis on a scheduled basis or when IGT makes policy changes that were previously compliant with the RIL Policies & Procedures to ensure a policy conflict is not occurring.
 - c. Perform a GAP analysis against the RIL and IGT IT security policies. The review of these policies must be done on site.
 - d. Assigning ownership responsibilities for all data, including databases, files, operating system, and application software. This includes indication of those individuals who have been granted the authority to originate, modify, and remove classes of information.
 - e. Management of system accounts, user profiles, and user access privileges; creating and granting access privileges to user accounts in accordance with resource owner specifications; and ensuring access privileges are revoked and resources transferred to authorized employees when an employee's status changes.
 - f. Monitoring compliance of the employees, vendors, consultants, contractors, etc. to the security requirements.
 - g. Ensuring a response to security violations and concerns by reviewing existing incident response handling procedures.
 - h. Serving as a mechanism for the on-going review of data information protection considerations, in the light of technical, environmental, or statutory changes that may arise.
 - i. Conducting reviews of computing security, including network access, on a regular basis.
 - j. Ensuring IGT provides annual employee IT security re-certification and meet industry best practices for all data center employees.

5. Each operational unit should have established procedures that will protect the unit from *Computer Viruses and Malicious Program Logic*. These procedures should provide the framework for procedures on prevention, detection, and eradication of viruses. These procedures include:
 - a. Automated protection via constant updating of virus detection master files.
 - b. Virus “scanning” is performed upon all systems on a scheduled basis.
 - c. All users know what is expected of them regarding virus protection policies.
 - d. Confirm there exist procedures for the official reporting of any detected viruses.
 - e. Ensuring that the IT security related events escalation policy is in place at the data center.

6. *Data Back-up, Storage, and Recovery*. Confirm the existence of policies and procedures that have been developed and implemented regarding the various RIL central system data back-up, storage, and required recovery. These shall be reviewed to determine if:
 - a. Data is being backed-up on a regularly scheduled basis.
 - b. Review encryption practices being utilized during system backups and to review secure storage of backup media.
 - c. There are copies of this data being stored on-site as well as off-site.
 - d. The back-up and retention schedule is able to supply all needed data for any given recovery procedure.
 - e. All pertinent personal computer (non-network) files are backed-up on a scheduled basis.
 - f. Determine that there is a formal disaster recovery plan.
 - g. Verify that the plan has been reviewed and updated within the past twelve (12) months.
 - h. Verify that there is effective monitoring of the plan’s state of readiness.

- i. Verify that the central system provider's backup data center has all the components to function as a primary data center to process transactions.
7. *Network Vulnerability and Intrusion Testing.* Inspect, identify, and test all points of access that currently exists on the online and video system. This includes:
 - a. Reviewing the access levels (internal and external) defined on all systems. Once all required information has been gathered, review all systems for any type of vulnerabilities. Report on all appropriate security features available to each system. Make note of all appropriate features that have not been 'enabled'.
 - b. Review configurations defined on firewalls, routers, switches, and all other miscellaneous network hardware located within the IGT data center to ensure that controls have been established that would block unauthorized individuals from gaining access to any of these devices.
 - c. Ensuring that all devices such as firewalls, routers, switches, and all other miscellaneous network hardware connected to the online and video systems meet EOL and EOS requirements.
 - d. Perform the following vulnerability scanning:
 - No unauthorized ports are open
 - Latest device patches/updates have been applied
 - Vulnerabilities within utilized version of software
 - Penetration Testing of IGT online/video systems (where possible)
 - Network scan of the IGT networks
 - e. Report on all areas where known vulnerabilities exist.
8. *Wireless Networking.* Perform a scan of all wireless devices located within the RIL building.
9. *Retailer Website Vulnerability Scan.* Perform a vulnerability scan of the Rhode Island Lottery's retailer website.
10. *RILOT.com Vulnerability Scan.* Perform a vulnerability scan of the Rhode Island Lottery's RILOT.COM website.

11. *Test System Connectivity with Production System.* Perform a review of how the IGT online and video test systems are interconnected with the live production systems on the IGT network to ensure controls exist to restrict and prevent production data from being copied to the test system, manipulated, and placed back onto the production system. Also, note any high risk areas with regards to how and where the test systems are placed and accessed within the IGT network.
12. *ISO/IEC 27001:2013* standards must be utilized and enforced. Compliance with current industry standards is of top priority, thus the vendor should be familiar with the ISO standards and should review if IGT is familiar with and following the standards.
13. While performing the review of the selected standards, the successful vendor is to meet with the RIL on a scheduled basis to discuss all of the findings up to that point in time. For each meeting, the vendor will produce a detailed narrative of all the findings that require discussion.
14. Once the audit of the selected standard(s) is completed, the successful vendor is to provide the RIL with all its findings in a formal written report, which highlights the risk level (low, medium, high), and recommended solution to each finding.
15. Any written reports pertaining to this audit must remain confidential.

SECTION C – REQUIREMENTS OF RESPONDENTS

1. BID RESPONSE REQUIREMENTS

- A. Vendor shall provide a description of its expertise, including, but not limited to:
 1. A brief history of its organization, including the number of years it has been in business, major clients, organizational structure, trade affiliations, and any parent/subsidiary affiliation with other entities.
 2. The names and/or positions of those individuals who will work on the RIL account, and their levels of expertise.
 3. An outline of the organization's expertise in providing information security services similar to those listed in this RFP.
 4. Any unique qualities vendor has that will enhance the services supplied pursuant to this RFP.

- B. The bidder shall provide the names and functions of the specific individuals who would be assigned to work on this project for the RIL. The RIL has the right to reject any personnel, and the successful vendor will have the obligation to immediately replace said personnel. The RIL has no obligation to disclose the reason said personnel was rejected.
- C. To allow for a complete evaluation of the integrity, background, and character of potential vendor, each bidding vendor, and parent corporation, if the vendor is a subsidiary corporation, shall disclose the following:
 - 1. The details of any conviction, judgment, and the nature of any investigations by local, state, or federal law enforcement authority in a state or federal court against the bidder or any allegation related directly or indirectly to any business activity,
 - 2. The details of any litigation during the past three (3) years that is completed, in progress, or pending between the bidding vendor and any party, private or governmental,
 - 3. The details of any bankruptcy, insolvency, reorganization, or any pending litigation involving fraud or deceit against the bidder, and
 - 4. Who, if anyone, will get a commission or other value from vendor, if vendor is selected.
- D. Failure to provide the detailed information required by the RFP may result in disqualification of a bidding vendor from the evaluation process. Award of contract shall be at the sole discretion of the RIL.
- E. The RIL may refuse to award a contract to a vendor, or any affiliated entity, if any of the following apply:
 - 1. False statements have been made in any information provided in the above-required disclosures, and/or
 - 2. Any of the entities, or principals of entities, have been convicted of an offense involving dishonesty, fraud, or any gambling-related offense.
- F. The bidding vendor shall state whether or not any of the following have occurred:
 - 1. During the last two (2) years, the bidding vendor was assessed any penalties under any of its existing or past contracts, and if so, indicate the public jurisdiction, the reason for the penalty, and the penalty amount of each incident,

2. During the last two (2) years, the bidding vendor has had to delay or nullify any contract, and
3. During the last two (2) years, the bidding vendor, subsidiary, or intermediary company, parent company, or holding company was the subject of any order, judgment, or decree of any state or federal authority barring, suspending, or otherwise limiting the right of the bidding vendor to engage in any business, practice, or activity.

2. FINANCIAL INFORMATION

A. Financial disclosure shall include either:

1. Vendor's complete financial statements (including, but not limited to, income statement and balance sheet) for each of the two (2) most recently completed fiscal years audited by a certified public accountant verifying that the audit was conducted; or
2. In the event that the vendor's income statements and balance sheet are not independently audited, the vendor's income statement and balance sheet for each of the two (2) most recently completed fiscal years and copies of vendor's income tax returns for those same years.

3. INTERESTED PERSONS

A. Vendor's proposal must disclose, to the best of vendor's knowledge and belief, any and all persons who meet all of the following criteria:

1. Are directly or indirectly related to IGT;
2. Are directly or indirectly related to the RIL;
3. Have or will have an economic interest in any contract by and between vendor and the RIL ("Interested Persons"); and/or
4. Have any existing or prior working relationships with IGT Corporation.

B. Failure of vendor to identify and disclose any and all Interested Persons to the RIL will render the contract void at the sole option of the RIL.

C. If at any time subsequent to the execution of a contract any person meets the above criteria and thus becomes an Interested Person, vendor must notify the RIL in writing of the existence of such Interested Person(s) within two (2) business days of vendor's knowledge thereof. The existence of such Interested Person(s) may be grounds for the termination of the contract at the sole option of the RIL.

4. REFERENCES

- A. Vendor shall provide the names of three (3) clients who have contracted with the vendor within the last three (3) years for information security services similar to those being requested in this RFP. The list shall include the following information:
- Contact Name
 - Company Name
 - Address
 - Telephone Number
 - Detailed Description of the Type of Service(s) Performed
- B. In addition, if vendor has provided services to other Lotteries, vendor shall list those Lotteries. The RIL may contact any company or references listed and inquire about the quality of services supplied by the vendor.

SECTION D – ADDITIONAL REQUIREMENTS OF SUCCESSFUL VENDOR

1. NON-DISCLOSURE

- A. Vendor understands that during the term of this contract, vendor may have access to information, data, and concepts that are of a highly confidential or sensitive nature. Due to the sensitive nature of the data that may be provided to the vendor, vendor expressly agrees that it shall maintain this data in confidence and that it shall not use this data for any purpose other than its performance for the RIL under this contract.

2. RIL PRIZES

- A. No officer or employee, or any blood relative living in the same household with any officer or employee, of the successful vendor shall be entitled to a RIL prize during the term of this contract.

3. SUBCONTRACTING

- A. If any part of the contract between the RIL and the vendor is to be subcontracted, the vendor shall state in writing in the proposal a description of the subcontractor's organization and the proposed subcontractual arrangements. The subcontractor must comply with all security and insurance requirements. The vendor is prohibited from subletting, conveying, assigning, or otherwise disposing of any contract resulting from the RFP, its rights, title, or interest therein, or its power to execute such agreement to any other company, corporation, or entity without the previous written consent and approval of the RIL. In the event the RIL approves the use of subcontractors in performance of this contract, the vendor is not relieved of its responsibility and obligation to meet all the requirements of this RFP.

4. PERFORMANCE GUARANTEE

- A. If the vendor is a subsidiary corporation, its parent corporation shall also be required to enter into agreement and unconditionally guarantee the performance of the vendor under the agreement.

SECTION E – BONDS AND INSURANCE

1. LITIGATION/PERFORMANCE BONDING

- A. Each vendor shall submit with its bid a litigation bond in the amount of twenty-five thousand dollars (\$25,000.00). A claim upon the bond may be made by the RIL if:
 1. The vendor brings any legal action or protest against the State of Rhode Island, RIL, or any individual member thereof, or any employees of the RIL, over the award of the information security audit contract and the RIL is the prevailing party at the conclusion of the litigation.
 2. The bond shall remain in effect two (2) years from the bid submission date. Vendors may request, and the RIL may grant, a release of the bond after six (6) months from the bid submission date in return for a release and covenant not to sue in a form acceptable to the RIL. The successful vendor may request such a release, and the release may be granted at the time of the contract execution.
 3. The successful vendor will be required to submit, at the time of the contract execution, a performance bond in amounts to be specified by the RIL based on the amount of the contract. The bond must be executed by a company authorized to do business in the State of Rhode Island and must meet the approval of the RIL. The bond shall be maintained in full force for the term of the contract.
 4. The successful vendor will also be required to submit, at the time of the contract execution, a payment bond (if subcontractors are to be used).

SECTION F – EVALUATION AND SELECTION

1. EVALUATION

- A. The RIL intends to conduct a comprehensive, fair, and impartial evaluation of proposals received in response to this RFP. All responses will be reviewed and scored by an Evaluation Committee. The Committee will evaluate each proposal that is properly submitted and provide its findings to the RIL Director, who will make the final selection.
- B. All proposals submitted must meet a minimum evaluation score of twenty-five (25) points in order to have the pricing component evaluated. Any proposals scoring less than twenty-five (25) points will be dropped from further consideration.

Quality	10 Points
Experience	15 Points
Financial Stability	15 Points
Price	<u>60 Points</u>
	100 Points

- C. An award will be made to the highest evaluated vendor who, in the sole judgment of the RIL, meets all of the requirements of the specifications, terms, and conditions contained herein.
- D. Bidders are to understand that the criteria used in the selection process are both objective and subjective and that price is not the only determining factor. Experience, financial resources, and capabilities of the vendor, and other relative matters will also be taken into consideration.
- E. The RIL reserves the right to determine which vendors have met the requirements of this RFP and to determine whether any deviation of the requirements of the specifications, terms, and conditions contained herein is merely minor or technical in nature.
- F. The RIL also reserves the right to accept bids which deviate in a minor or technical manner.
- G. The RIL reserves the right to accept or reject any, or all, bids, proposals, award on cost alone, cancel the solicitation, waive any technicality, and conduct additional negotiations as necessary in order to act in the best interests of the RIL.

2. SELECTION

- A. The Evaluation Committee will submit written findings, including the results of the evaluations, to the RIL Director, who will make the final selection for this solicitation.
- B. Upon receipt of the Committee's report, the Director is free to engage in dialogue with members of the Committee. The Director may take as much time as necessary to review the report and query the Committee.

SECTION G – RESPONSES

1. COMPLIANCE WITH FORMAT

- A. All responses must conform to the RIL's request. Bidders, in their responses, must refer to the specific sections in this RFP.
- B. Responses must be submitted in a manner that will enable the RIL Evaluation Committee to analyze each bidder's response fairly and arrive at a meaningful comparison of proposals.
- C. Except for preprinted attachments or similar material, all pages of the proposals must be clearly numbered in sequential order.

2. RESPONSE REQUIREMENTS

- A. Responses not conforming to the requirements of the RFP will not be considered.
- B. All responses must be valid for one hundred twenty (120) days.

3. PREPARATION COSTS

- A. All proposals are submitted at the vendor's sole risk and expense. Under no circumstances shall the RIL be responsible for any cost or expense incurred in submitting response to this solicitation, including travel.

4. REJECTION RIGHTS

- A. The RIL reserves the right to reject any or all proposals.
- B. Any proposal not containing sufficient information to permit a thorough analysis may be rejected, as will any response that fails to meet the minimum requirements detailed in the RFP.

SECTION H - COMMUNICATIONS

1. RESTRICTIONS ON COMMUNICATIONS

- A. Contact with RIL personnel is limited to written questions sent to the attention of the Evaluation Committee either by e-mail (tkiernan@rilot.ri.gov) or faxed to 401-463-5669 by the date stipulated herein.
- B. Contact with any RIL personnel or officials elected or appointed in the State of Rhode Island in an effort to influence the awarding of this contract shall be grounds for rejection of bidder.
- C. Prior to the approval of a contract, bidders shall not represent themselves to any party, including RIL staff, retailers, or vendors as having the endorsement of the RIL.
- D. Extraordinary requests for exceptions to these restrictions may be directed, in writing, to the RIL Director.
- E. Any bidders causing or attempting to cause a violation or circumvention of this ethical standard may, in the sole discretion of the RIL, be disqualified from further consideration.

SECTION I - SCHEDULE OF EVENTS

1. SCHEDULE OF EVENTS

- A. The RIL reserves the right to change the dates listed below. If changes are made, all known vendors receiving the original RFP will be contacted directly.

RFP Release	Wednesday, August 17, 2016
Written Questions Due	Wednesday, August 31, 2016*
Responses to Questions	Wednesday, September 7, 2016
Pre-Bid Conference	Monday, September 12, 2016
Proposals Due	Monday, September 26, 2016*
Technical Proposals Opening	Tuesday, September 27, 2016
Contract Award	Tuesday, October 4, 2016

*Written questions and Proposals must be received by 4:00 p.m. on the dates specified above.

SECTION J – SUBMITTAL AND FORMAT

1. INSTRUCTIONS FOR RESPONSE SUBMITTAL

- A. The original and five (5) copies of the bidder’s proposal, including all attachments, in the same order as the specific sections of the RFP, as well as the original and five (5) copies of the bidder pricing, must be received by the RIL no later than 4:00 p.m., Eastern Time, on Monday, September 26, 2016. Public opening of the technical proposals (not pricing) will be held on Tuesday, September 27, 2016.
- B. Any proposals received after 4:00 p.m. Eastern Time on Monday, September 26, 2016, will not be accepted.
- C. Proposals and pricing sheets must be submitted in separate envelopes addressed to:

Gerald S. Aubin
Director
Rhode Island Lottery
1425 Pontiac Avenue
Cranston, RI 02920

- D. Each envelope should be clearly marked to indicate its contents as follows:

“Sealed Bid – Pricing Proposal”
“Sealed Bid – Technical Proposal”