

**THE
RHODE ISLAND TURNPIKE
AND BRIDGE AUTHORITY
REQUEST FOR PROPOSALS**

**PCI PENETRATION TESTING
SERVICES**

CONTRACT #14-6

May, 2014

Earl J. Croft III, Executive Director
Rhode Island Turnpike and Bridge Authority
1 East Shore Road (P.O. Box 437)
Jamestown, Rhode Island 02835
Telephone (401) 423-0800 – Fax (401) 423-0830

REQUEST FOR PROPOSALS

**PCI PENETRATION TESTING
SERVICES**

CONTRACT #14-6

1. General

1.1 Summary

- A. The Rhode Island Turnpike and Bridge Authority (Authority) is soliciting proposals from PCI Standards Council qualified Security Assessors (QSA) companies to provide services related specific to testing of the Authority's current information technology network as it relates to PCI DSS version 3.0.
- B. The Authority is a small state-quasi agency that is currently responsibility for the tolling of several bridges in Rhode Island. As part of this responsibility, the Authority provides services for customers that have a Rhode Island E-ZPass account. Since credit card data is handled as part of this service the Authority needs to meet PCI compliant.
- C. The Authority is seeking a vendor that will perform external and internal penetration testing to certain aspects of its information technology (IT) network as part of it meeting PCI compliance.

2. Requirements

2.1 Vendor Requirements

- A. The bidder will be an approved PCI Standards Council Qualified Security Assessors (QSA) company.
- B. The bidder will be required to perform both external and internal penetration testing as it relates to PCI Security Standards Council (SSC) Data Security Standards (DSS) version 3.0 on select potions of the Authority IT network.
- C. Internal Penetration Testing
 - 1.) Intent of the engagement will be compliance with standard 11.3 of the PCI DSS.
 - 2.) There will be one testing perspective that from a user on the RITBA domain – a specific IP address.
 - 3.) Target scope will be five specific IP addresses one of which is an application DMZ.
 - 4.) Perform work on two (2) unique internal web applications in the

application DMZ. There is one (1) unique role of authentication per application.

- 5.) Testing can either be conducted remotely over an established VPN tunnel between the bidder and piece of provided hardware (netbook) placed in the Authority IT Domain network segment or conducted with an analyst physically being onsite with the appropriate hardware.
- 6.) Authentication credentials will be provided for each of the internal web applications.
- 7.) As part of this proposal, four (4) hours are to be included that can be used for retesting of any identified vulnerabilities and/or consultation time between the analyst and RI Turnpike and Bridge Authority.

D. External Penetration Testing

- 1.) Intent of the engagement will be compliance with standard 11.3 of the PCI DSS.
- 2.) There will be one (1) unique web application in scope.
- 3.) There will be one (1) unique role of authentication in scope.
- 4.) There will be three (3) expected network layer services: FTP, HTTP and HTTPS.
- 5.) The scope will be five (5) public IP addresses assigned to the Authority.
- 6.) One set of end user authentication credentials will be provided for one (1) public IP addresses.
- 7.) As part of this proposal, four (4) hours are to be included that can be used for retesting of any identified vulnerabilities and/or consultation time between the analyst and RI Turnpike and Bridge Authority

E. The testing will follow OWASP (Open Web Application Security Project) top ten guidelines.

F. Provide a hourly rate for any additional hours that may be required upon request.

3. General Terms and Conditions

3.1 Receipt and Opening of Proposals

A. Sealed Bids (Proposals) will be accepted and time stamped upon receipt in the office of the Executive Director at One East Shore Road, Jamestown, Rhode Island, 02835 until 2:00 p.m., Monday June 2, 2014. Two (2) copies of the proposal must be submitted in a sealed envelope marked "PCI Penetration Testing Services – Contract #14-6". Bids will be opened publicly and read at the Authority's office on Monday, June 2, 2014 at 2:00 p.m..

3.2 Form of Bid

A. Bidders shall submit two (2) copies of their bid, on the form provided, with supplemental information, and other required documentation, literature and material to be provided with the bid, on the bidders own form.

3.3 Submission of Bids

- A. Envelopes containing bids must be sealed and must be plainly marked with the name and address of the bidder and plainly marked as “PCI Penetration Testing Services, Contract #14-6”. Bids shall be delivered or mailed to:

Office of the Executive Director
RI Turnpike and Bridge Authority
1 East Shore Road
PO Box 437
Jamestown, RI 02835-0437

- B. Any bidder may withdraw his bid by written request at any time prior to the advertised time for opening. Telephone and or fax bids, amendments, or withdrawals will not be accepted.
- C. Unless otherwise specified, no bid may be withdrawn for a period of sixty (60) days from time of bid opening without the permission of the Executive Director.
- D. Negligence on the part of the bidder in preparing the bid confers no rights for the withdrawal of the bid after it has been opened.
- E. Proposals received prior to the time of opening will be securely kept, unopened. No responsibility will be attached to an officer or person for the premature opening of a proposal not properly addressed and identified.
- F. Any deviation from the specifications must be noted in writing and attached as part of the bid proposal. The bidder shall indicate the item or part with the deviation and indicate how the bid will deviate from specifications.
- G. Include in the bid paperwork a completed W-9 Form which is attached.

3.4 Rhode Island Sales Tax:

- A. The authority is exempt from the payment of the Rhode Island Sales Tax under the 1956 General Laws of the State of Rhode Island, 44-18-30, Paragraph I, as amended.

3.5 Federal Excise Taxes:

- A. The authority is exempt from the payment of any excise tax or federal transportation taxes. The price bid must be exclusive of taxes and will be so construed.

3.6 Qualification of Bidders:

A. The Authority may make such investigations as it deems necessary to determine the ability of the bidder to perform the work. The bidder shall furnish the Authority with all such information and data for the purpose as may be requested.

B. The bidder shall provide three (3) references on Attachment.

3.7 Addenda and Interpretations:

A. All questions pertaining to the specifications or proposal procedure should be directed to James Swanberg, Director of Plaza Operations, Safety and Security at (401) 423-1953 or jswanberg@ritba.org. The Authority is not responsible for information obtained from any other source.

3.8 Award of Bids:

A. The Authority reserves the right to award in whole or in part.

3.9 Contract Term:

A. This is a one year contract with two additional one year options to renew.

3.10 Hold Harmless:

A. The contractor shall be responsible for his work and every part thereof, and for all materials, tools, appliances, and property of every description used in connection therewith. The contractor agrees to indemnify and hold harmless the Rhode Island Turnpike and Bridge Authority, its employees and agents, against loss or expense by reason of the liability imposed by law upon the contractor, all sub-contractors, or owner for damage because of bodily injuries, including person or persons or on account of damage to property arising out of or in consequence of the performance of this work whether such injuries to persons or damage to property are due or claimed to be due to any negligence, including gross negligence, of a sub-contractor, the owner, the general contractor, his or their employees or agents, or any other person.

3.11. Deadline for Submissions of Proposals

A. The sealed bids will be accepted until 2:00 p.m., Monday, June 2, 2014 at the office of the Authority, One East Shore Road, Jamestown, Rhode Island. Two (2) copies of the proposal must be submitted in a sealed envelope marked "PCI Penetration Testing Services – Contract #14-6" and may be mailed to the Authority or hand carried and delivered to the Authority prior by the time and date noted above. Bids will be opened publicly and read at the Authority's office on Monday, June 2, 2014 at p.m..

B. The authority reserves the right to reject any or all bids, waive any informalities in the bidding, or accept the bid deemed to be in the best interest of the Authority.

PROPOSAL

TO: The Rhode Island Turnpike and Bridge Authority
PO Box 437
Jamestown, RI 02835

We the undersigned propose to furnish to the Rhode Island Turnpike and Bridge Authority, **“PCI PENETRATION TESTING SERVICES**, per attached specifications dated _____ 2014 for the prices stated below.

Price of the External Penetration Test:

Price in figures: \$ _____

Price of the Internal Penetration Test:

Price in figures: \$ _____

Hourly rate for any additional hours if required: \$ _____

Please supply any additional pertinent information about your proposal that is relevant to this contract.

By: _____
Authorized Signature Date

Company name

Print Name & Title

Address

Telephone Fax

Authority State Zip Code

Please include three (3) references with bid.

REFERENCES:

Name: _____

Firm: _____

Contact Number: _____

Address: _____

Name: _____

Firm: _____

Contact Number: _____

Address: _____

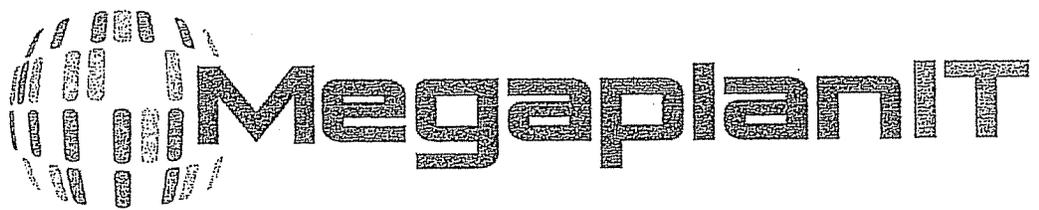
Name: _____

Firm: _____

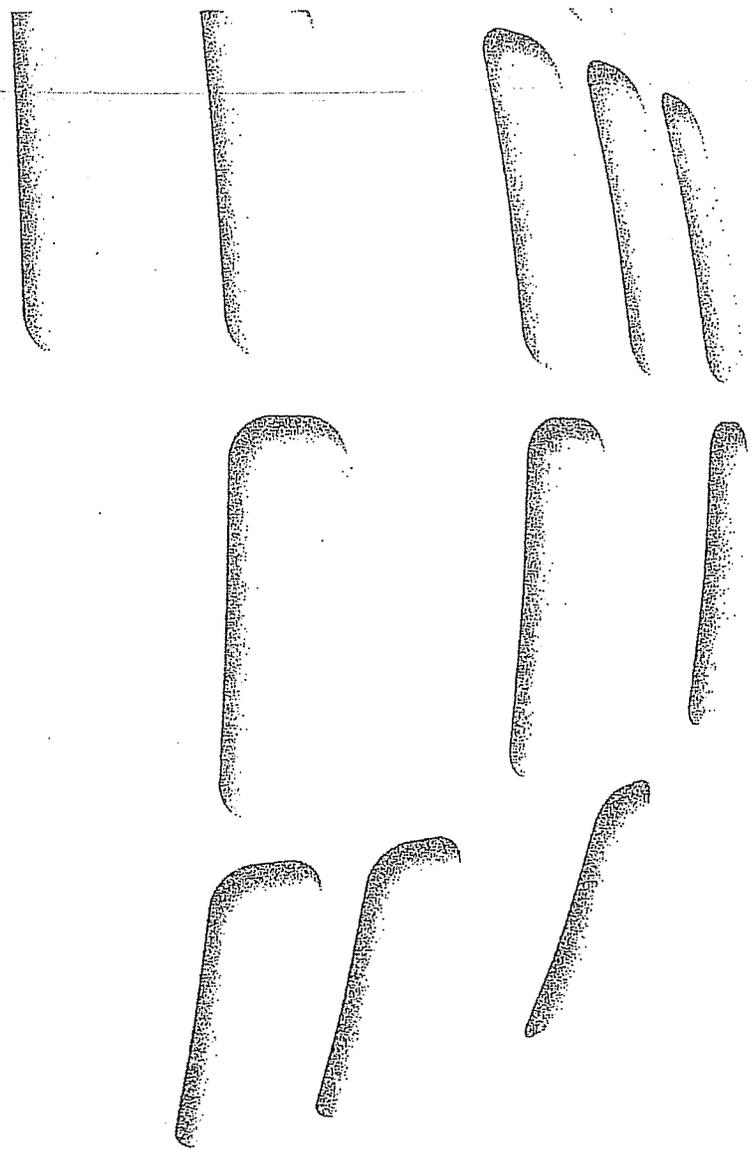
Contact Number: _____

Address: _____

Signed
Contract



Rhode Island Turnpike and Bridge
Authority
PCI Penetration Services Contract #14-6



Megaplan-IT, LLC
12900 Heiden Circle #4404
Lake Bluff, IL 60044
<https://megaplanit.com>

May 31st 2014

Primary Contact
Dominick Vitolo
PCI-QSA, GPEN, PCIP

Tel 480-269-2973
Fax 855-879-0008
dominickv@megaplanit.com

Table of Contents

EXECUTIVE SUMMARY.....3

PENETRATION TESTING OVERVIEW4

 MEGAPLAN-IT PENETRATION TESTING PROCESS4

 INTERNAL PENETRATION TESTING.....5

 EXTERNAL PENETRATION TESTING.....6

 WEB APPLICATION PENETRATION TESTING.....6

TRUSTED ADVISORY AND REMEDIATION ASSISTANCE.....9

IMPORTANT FACTORS FOR SUCCESS 10

PROJECT SCHEDULE AND ASSOCIATED FEES 11

FINAL PROJECT DELIVERABLES..... 12

TERMS AND CONDITIONS..... 13

AUTHORIZATION 15

BIOGRAPHIES OF CONSULTANTS ASSIGNED TO PROJECT 16

OPTIONAL SERVICES..... 22

Executive Summary

Megaplan-IT, LLC welcomes the opportunity to present this proposal for an Internal, External, and Website Application Penetration Test of Rhode Island Turnpike and Bridge Authority. Your customer base relies on your system controls to be in place and functioning at peak performance. Megaplan-IT's team of certified Penetration Testers appreciates the solid reputation Rhode Island Turnpike and Bridge Authority already enjoys, and understands how important it is to maintain that customer trust.

During the engagement, Megaplan-IT will work in collaboration with Rhode Island Turnpike and Bridge Authority at all stages. We strive to establish the most open and direct communication feasible. This will remain true throughout the project's lifecycle and beyond. Working together in this fashion lowers risk and helps all of us meet objectives in a timely manner. By providing the following services, Megaplan-IT will validate the security of Rhode Island Turnpike and Bridge Authority's Internal Networks, External Devices, and Website Applications:

- Penetration Testing Report
- Trusted Advisory and Remediation Assistance

Megaplan-IT performs security assessments based on a detailed process, which has continuously proven to be successful. Basically, the scope of each reviewed component is scaled relative to an associated risk level, which helps Megaplan-IT and Rhode Island Turnpike and Bridge Authority's management to consistently review and adjust the overall scope of the security assessment as needed. Most of these adjustments will be made based on the consultants observations, enabling Rhode Island Turnpike and Bridge Authority to apply recommendations that will help reduce the time, effort, and cost of the assessment. Megaplan-IT's methodology effectively narrows the scope without affecting the end results.

The following proposal delves deeper into Megaplan-IT's approach to Penetration Testing.

Penetration Testing Overview

Megaplan-IT adheres to a well-defined methodology for Internal, External, and Website Application Penetration Testing. This series of tests will effectively analyze your system from top to bottom. We will perform all tests in a seamless manner, so your normal workflow is not disrupted.

Megaplan-IT Penetration Testing Process

Review of Current Security Controls and Documentation

A Megaplan-IT Penetration Testing consultant will begin by reviewing all documentation pertaining to your current IT system, security controls, procedures or other material that can help assess the effectiveness of the controls.

This general system review takes into account how the security controls are designed and deployed. For the purpose of future enhancements and further analysis, this type of review becomes invaluable. It also helps the tester identify particular security controls for later testing.

To summarize, a Megaplan-IT consultant will be responsible for reviewing Rhode Island Turnpike and Bridge Authority's documents that include:

1. An overall look at the IT infrastructure and environment, including any general security information.
2. Website additions or edits that might adversely affect the testing process.
3. Engineered infrastructure (i.e.: network design, automated services, OS engineering).
4. Methods in which the system is monitored.

The consultant will also hold meetings or conferences with Rhode Island Turnpike and Bridge Authority to:

1. Identify key personnel, stakeholders and other compliance participants.
2. Gather evidence of specific system functions from those identified parties.
3. Review all gathered information with the appropriate personnel (the author), and identify any missing information or discrepancies between the written documentation and their oral descriptions.

Research the Network System

Megaplan-IT will study your network systems and become familiar with the network design and current security controls.

Map the Network

The penetration tester will scan the network utilizing various techniques, including Port Scanning, RF Profiling, and Layer 2 ARP Sweeps. Megaplan-IT will also scan all available IP addresses multiple times. We will then use this data to create a fully realized network map.

Identify and Classify the Network System

Once thoroughly mapped, the tester can then precisely identify each network component and security control using a separate suite of tools. Once each component is identified, the tester will classify them into discernible groups.

Test the Network

Megaplan-IT will then perform an initial Low Level Network Test, which is a rudimentary attempt at breaching security. This type of test will enable Megaplan-IT to gather information that could be used in a more sophisticated attack later on.

Fully Test the System

The Megaplan-IT tester will then devise and conduct a series of in-depth Penetration Tests. The tester will leverage the knowledge gained during the Mapping phase to attack potentially vulnerable areas. Once the vulnerable areas have been determined, Megaplan-IT will further test those areas, using both linear and non-linear techniques.

A real-life attacker would use these vulnerabilities to their advantage, so it's important that Rhode Island Turnpike and Bridge Authority's management is made fully aware of their existence (and what steps can be taken to resolve them).

Post-Testing

At this point, Megaplan-IT has fully tested the network system and found it to be compromised in several areas. Further testing might be warranted, depending on the area in question.

While the system is compromised, the tester will determine what areas contain data, and will attempt to download or copy a portion of that information.

Having now identified vulnerable areas of high importance, the Megaplan-IT tester will determine if any connected assets are also vulnerable or open for attack due to the relationship.

Final Report and Delivery

Megaplan-IT will deliver a Final Report that outlines the network security posture while highlighting vulnerable areas and offering options to remediate the issues. The Final Report will include an assessment of existing security controls and a corresponding Risk Level Rating based on the assessment. All areas of risk will be identified and options to mitigate these risks will be offered. The penetration testing consultant will also make recommendations on improving current IT architecture and revising Policy and Procedure documents.

All system information, data assets, file names, and passwords obtained during Penetration Testing will be returned and/or permanently deleted.

Internal Penetration Testing

Many companies do not realize that their own internal networks represent one of the greatest security threats to their critical data. Local Area Networks (LAN) and Wide Area Networks (WAN) have become commonplace in most work environments, as they allow for easy access to information. However, the downside to LAN/WAN is that proper security controls are often diminished, or altogether missing, from these systems.

With a fewer number of security controls in place, the risk of a security breach grows. Megaplan-IT's Internal Penetration Testing will analyze your networks and determine if the security controls are sufficiently protecting your data. This testing process is performed using an itinerant model; whereby we apply information learned from each test to improve and focus the overall process.

External Penetration Testing

To keep malicious attacks at bay, Rhode Island Turnpike and Bridge Authority's network perimeter needs to be secure and operating at peak performance. Many controls surround the network perimeter, including firewalls, host-hardening configurations, and router access control lists (ACLs). These controls are in place to maintain the security and privacy of information assets. Using the same general Penetration Testing methodology as described earlier, Megaplan-IT will perform an External Penetration Test on this specific class of controls. Megaplan-IT will classify each control and update the network map before proceeding with the test.

During an External Penetration Test, Megaplan-IT focuses on assessing the level of effectiveness that the current controls represent; how well they are implemented; and the types of configurations set up between network hosts and relevant devices. The assessment is purposefully designed to emulate an attack from the web.

Megaplan-IT will test the network for any vulnerability by utilizing a combination of automated software and manual techniques. The findings will be compiled into a detailed report that highlights potential issues, exploitable vulnerabilities, and any other flaw that might allow for unauthorized access to the network.

Web Application Penetration Testing

Identifying the Application's Architecture:

Megaplan-IT will scan and identify every application currently active in your system. A penetration tester will group the applications together in a way that identifies which server or area of the network they are housed on. It's important to validate the trust relationships between each application, so grouping them together helps us determine how they interact with each other across the environment. Locating vulnerable areas, hidden Trojan viruses, and backdoors is much easier with this information in hand.

Updating Management and Exploiting Application Vulnerabilities:

Once again, Megaplan-IT will inform Rhode Island Turnpike and Bridge Authority's management, personnel, and IT security staff about any discovered vulnerability in the application architecture. After Rhode Island Turnpike and Bridge Authority has been apprised of the situation, management can decide to exploit the application's vulnerability. Megaplan-IT utilizes a number of Testing methods based on the Open Web Application Security Project's (OWASP) Top 10:

Injection

Injection flaws, such as SQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data.

Cross Site Scripting (XSS)

XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation and escaping. XSS allows attackers to execute scripts in the victim's browser that can hijack user sessions, deface web sites, or redirect the user to malicious sites.

Broken Authentication and Session Management

Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities.

Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

Cross Site Request Forgery (CSRF)

A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically-included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests that the vulnerable application thinks are legitimate requests from the victim.

Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application, framework, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained, as many are not shipped with secure defaults. This includes keeping all software up to date, including all code libraries used by the application.

Insecure Cryptographic Storage

Many web applications do not properly protect sensitive data, such as credit cards, SSNs, and authentication credentials, with appropriate encryption or hashing. Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes.

Failure to Restrict URL Access

Many web applications check URL access rights before rendering protected links and buttons. However, applications need to perform similar access control checks each time these pages are accessed, or attackers will be able to forge URLs to access these hidden pages anyway.

Insufficient Transport Layer Protection

Applications frequently fail to authenticate, encrypt, and protect the confidentiality and integrity of sensitive network traffic. When they do, they sometimes support weak algorithms, use expired/invalid certificates or do not use them correctly.

Invalidated Redirects and Forwards

Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

Additional Penetration Tests*Compromising the System:*

As the network's vulnerable areas are tested and exploited, Megaplan-IT will detect areas that have been compromised. These results will be reported to Rhode Island Turnpike and Bridge

Authority's management. If management decides that further testing is required, Megaplan-IT will penetrate deeper into these trouble spots with additional tools and techniques.

Extracting Critical Data Assets:

While examining and testing a compromised area, Megaplan-IT will attempt to access, download or otherwise manipulate any critical data uncovered. Any data that is accessible will be properly documented and stored until the testing process is complete.

Critical System Leap Frogging:

In a connected and complex IT environment, one compromised system may give an attacker the ability to access another system that it is not directly connected to. This is known as "leap frogging." Web servers are often used as a launching pad for this type of attack, but once the internal server has been compromised any number of areas may be exploitable.

Final Report Deliverable

Upon completion of the Penetration Testing engagement, a Final Report will be drafted and delivered to Rhode Island Turnpike and Bridge Authority's management. This Final Report will contain a detailed map of the network and will outline both the system and application classification models. Results of the exploitation tests will be thoroughly documented in the Final Report, and each result will be accompanied with a recommendation for remediation.

Trusted Advisory and Remediation Assistance

Megaplan-IT assists our clients with achieving their IT security goals by employing consultants with knowledge in all aspects of technical remediation. Megaplan-IT's Trusted Advisory Service provides our clients with the support needed to incorporate new devices, website applications, or to improve the general state of network security.

Trusted Advisory and Remediation includes:

- Providing a comprehensive background into Rhode Island Turnpike and Bridge Authority's IT security requirements and objectives.
- Identifying and modeling business processes and cardholder data flows to assist in optimizing business activities to help reduce any applicable compliance scope.
- Identifying and steering clients toward Industry-Best Practices as well as keeping a cost-effective approach that is reasonable to your organization.
- Providing a detailed roadmap that will educate specific groups within your organization in regards to their remediation efforts.
- Validating and confirming internal designs and solutions so they meet or exceed all security requirements.

Important Factors for Success

Megaplan-IT has made the following assumptions regarding Rhode Island Turnpike and Bridge Authority's responsibilities. These should be reviewed for accuracy as they could impact the timely completion of the project.

- Rhode Island Turnpike and Bridge Authority will select a Lead Project Liaison to serve as a point of contact for resolving project-related issues.
- The Lead Project Liaison will ensure documents are delivered to Megaplan-IT in a timely fashion and will coordinate meetings between company personnel and Megaplan-IT's Security Assessors.
- The Lead Project Liaison will be responsible for reviewing assigned deliverables on a pre-determined schedule.
- Megaplan-IT respectfully requests all deliverables be accepted within five business days of submittal.
- Any and all issues surrounding deliverables must be presented in writing to Megaplan-IT's Engagement Manager.
- To ensure key personnel participation, Rhode Island Turnpike and Bridge Authority will assist in the coordination of facilities and meetings.
- Unless otherwise agreed to by Megaplan-IT, Rhode Island Turnpike and Bridge Authority will manage its own schedule, deliverables, personnel and other resources.
- In case immediate attention is required to alleviate a security concern, Rhode Island Turnpike and Bridge Authority will provide Megaplan-IT with an emergency contact.

Project Schedule and Associated Fees

Once Rhode Island Turnpike and Bridge Authority has accepted this proposal, Megaplan-IT will commence work on a mutually agreed-upon date. We estimate that this engagement will transpire over the course of two weeks, but understand that this estimate is subject to change based on the level of requested vulnerability verification, as well as revisions to the project plan and/or scope of project.

The date that Megaplan-IT delivers reports may change due to several factors, including resource availability, project objectives, mutual scope modifications, project assumptions or any other factor not known at the time this proposal was drafted. The following table outlines the fees associated with this project.

MEGAPLAN-IT SERVICES	HOURS	PER YEAR
Internal Penetration Testing (Remote Testing)	65 Hours	\$9,750
External Penetration Testing	40 Hours	\$7,500
Trusted Advisory and Remediation Assistance	5 Hours	<u>Included</u>
Retesting of Failing Vulnerabilities	8 Hours	<u>Included</u>
Total	118 Hours	\$17,250

Megaplan-IT requires the client to pay a 50 percent retainer fee upfront. The remaining 50 percent will be invoiced upon completion of the assessment.

Final Project Deliverables

The project deliverables, and performance of the associated tasks identified in this document, are the responsibility of Megaplan-IT. The fees in the table above are based on the estimated scope and assumptions outlined in the proposal. The project fee and related schedules may be impacted if any of the assumptions are deviated from or otherwise proven invalid, and will be handled via the project change control process. Additional requirements and deliverables that fall outside the parameters of this proposal will be billed separately as agreed-upon by Megaplan-IT and Rhode Island Turnpike and Bridge Authority.

Rhode Island Turnpike and Bridge Authority's Final Deliverables

- Penetration Testing Report
- Trustee Analysis and Remediation Assistance

Terms and Conditions

1. **Confidentiality** – The Client and Megaplanit, LLC mutually approve that the requirements of a shared non-disclosure agreement between the Client and Megaplanit, LLC, if executed, shall apply to all material supplied by either party in connection with the service(s).
2. **Authorized Disclosure** – Megaplanit, LLC. will only release information contained in any working documents, reports, etc. to the Client or third party permitted by the Client.
3. **Force Majeure** – The Client nor Megaplanit, LLC. shall not be liable for any postponement or default in performance if such delay or default is caused by conditions beyond its control, including but not limited to: Governmental acts, wars, insurrections, acts of God, terrorist acts, natural disaster, fires, and/or any other reason outside the sensible control of the party whose performance is influenced.
4. **Governing Law** – This Contract is governed by the laws of the State of Illinois excepting its choice of law provisions. The Client and Megaplanit, LLC. hereby agree to irrevocably attorn to the non-exclusive jurisdiction of the courts of the State of Illinois.
5. **Intellectual Property** – Megaplanit, LLC will provide the Client with reports that are written or on-line, facts and figures, and other materials (collectively, “Materials”) in assembly with Services. The Client agrees that all intellectual property rights in the Materials, including copyrights, trade secrets, trademarks, and patents are solely in possession by Megaplanit, LLC. The Client is allowed to hold all Materials distinct as “confidential” and use the Materials exclusively for the commitments for which they are shown. The Client does not have authorization to distribute, copy, or use the Materials without written authorization of Megaplanit, LLC. Copying, dispensing, or use of the Materials in any format or by a Megaplanit, LLC. competitor is strictly forbidden.
6. **Term** – This Contract shall be for a term of 1 year commencing on the date of execution by both parties, and is subject to earlier termination as provided in this Contract.
7. **Payment** – The Client agrees to pay all charges for the services provided from Megaplanit, LLC. The client will pay Megaplanit, LLC. per the fee schedule set forth in this contract, and except for the first payment, upon full completion of the Services and the Client's acceptance of all remaining deliverables. The client will make final payment(s) 30 days after receipt of invoice, which will be issued by Megaplanit, LLC. no earlier than the Client's acceptance of the applicable deliverable(s). Megaplanit, LLC. will bill 50% upfront of the total amount for the 1 year agreement price of \$17,250. The remaining 50% will be billed upon delivery of report.
8. **Termination for Cause** – The Client and/or Megaplanit, LLC. may terminate this Contract for basis upon the conclusion of thirty (30) calendar days succeeding comprehensive written notice to the other party of its material break of any of its material necessities and requirements under this Contract, if the other party has not alleviated such breach during the notice timeframe.
9. **Warranties** – Due to the environment of the computer security industry, no security company can guarantee that it will identify every vulnerability or security issue.

Megaplanit, LLC. provides its services on an “as is” foundation and without any warranties whatsoever.

Megaplanit, LLC. disclaims any and all warranties, including without restriction to warranties of merchantability and fitness for a specific drive, with respect to its materials, products, and services.

Megaplanit, LLC. does not warrant that the services will identify every Compliance control gap and/or Security vulnerability within your system(s), application and/or network devices. Megaplanit, LLC.'s Information Security and Compliance Assessments, will provide solutions or advice but will not be expected to be error-free. The Client agrees that Megaplanit, LLC. shall not be responsible or liable for the accuracy or usefulness of any information provided by it, or for any use of such information.

10. **Limitation of Liability** –Megaplanit, LLC. or its agents shall not be liable for any profit loss or any indirect, direct, incidental, consequential or punitive damages whatsoever with respect to its materials, services, and products even if Megaplanit, LLC. has been notified of the possibility of such damages. In any event, Megaplanit, LLC.'s total liability for any claim or damage shall not exceed the fees you have paid to Megaplanit, LLC., under this contract.
11. **General** – This is the private agreement between the Client and Megaplanit, LLC. If any term of this Contract is found void or unenforceable, all other terms shall remain in full force and effect. The Client may not assign this Contract without Megaplanit, LLC. written consent.

Authorization

Rhode Island Turnpike and Bridge Authority and Megaplanit, LLC agree that this authorization of work is executed under the deliverables set forth by the Assessment Overview.

Megaplanit, LLC accepts this Agreement for the designated services and terms as accepted by Rhode Island Turnpike and Bridge Authority:

Signature: *Frank Nudo*
 Print Name: Frank Nudo
 Title: CEO
 Effective Date: 7/14/2014

I (Rhode Island Turnpike and Bridge Authority Representative) hereby accept this Agreement for the designated services and terms as initialed below:

Signature: *[Signature]*
 Print Name: SAMUEL E. SWANBERG
 Title: DIRECTOR OF PLAZA OPERATIONS, SAFETY + SECURITY
 Date: 7/11/14

Rhode Island Turnpike and Bridge Authority and Megaplanit, LLC agree that services rendered under this proposal will be executed with great skill and care, appropriately reflecting the level of expertise possessed by the Megaplanit consultants. Rhode Island Turnpike and Bridge Authority acknowledges that any new configuration, technology, software upgrades, settings changes, and normal maintenance procedures can adversely alter systems and create unknown security exposures. Maintaining sufficiency of controls and documentation is the responsibility of Rhode Island Turnpike and Bridge Authority, due to the ever-changing nature of the control environment and Rhode Island Turnpike and Bridge Authority's dependence on an operational IT infrastructure.

Megaplanit appreciates this opportunity to assist Rhode Island Turnpike and Bridge Authority with improving its information security and risk management procedures.