CITY OF NOVI CITY COUNCIL
FEBRUARY 10, 2020

SUBJECT: Approval to award a contract for cybersecurity overlay services to Access Interactive in the amount of $76,787 for one (1) year with the option of three (3) additional years.

SUBMITTING DEPARTMENT: Integrated Solutions, Technology Division

EXPENDITURE REQUIRED	**$ 76,787**
AMOUNT BUDGETED	**$ 77,000**
APPROPRIATION REQUIRED	**$ 0**
LINE ITEM NUMBER	**101-205.00-816.042**

BACKGROUND INFORMATION: The City of Novi's Technology Division is focused on providing a secure network environment that meets the operations needs of the organization. To this end the team contracts with an external audit firm every other year to examine our security practices and test the security of our network. These audits explore different facets of the operation. Some examples of the items targeted in the audits include policies, procedures, segregation of duties, user access rights, application/server log review, physical security, user security awareness training, continuity of business planning, and network penetration testing. Given the current cybersecurity climate we are increasing the frequency with which we perform penetration testing as well as types of vulnerability tests. The requested cybersecurity overlay agreement provides a Security as a Service (SaaS) model approach to our security needs. The agreement provides services in the following five areas:

1. Identify & evaluate current security readiness.
2. Document & implement compliant regulations & controls imposed on the city.
3. Monitor & report on users' and system activity.
4. Continuously scan for vulnerabilities.

5. Support as needed in achieving yearly security milestones.

Services within the agreement are prioritized with the highest priority tasks being performed daily in real-time (e.g., log monitoring and File Integrity Monitoring). The agreement also includes consultant services to address a failure in the security model, should we experience a cybersecurity event.

RECOMMENDED ACTION: Approval to award a contract for cybersecurity overlay services to Access Interactive in the amount of $76,787 for one (1) year with the option of three (3) additional years.

`

SECURITY OVERLAY AGREEMENT

PREPARED FOR:

CITY OF NOVI

PRESENTED BY:

WALEED HADDAD
whaddad@access-interactive.com
DANIEL HEIDT
Daniel.heidt@access-interactive.com

Bill Fedak
bfedak@access-interactive.com
248-567-3000
46635 Magellan Novi, MI 48377

access interactive

TABLE OF CONTENTS

ACCESS INTERACTIVE COMPANY OVERVIEW

Access Interactive LLC., ("Access", "AI") provides technology solutions, services and support to business, educational and government organizations since 1985. Our business focus is helping our clients make the most of technology investments. Over the last 30+ years Access has experienced significant growth to establish itself as a $35 million organization proudly retaining over 65 full-time employees. We pride ourselves on being large enough to be extremely competitive and small enough to pay personal attention to our customers. We have an unwavering commitment to providing the best solutions, service and support to our customers.

Our highly skilled technical services group includes over 40 full-time technicians including VMware, Microsoft, Cisco and Dell certified system engineers and expert security/compliance consultants. Our technicians are available to you for projects ranging from on-site break/fix services to full-scale WAN/LAN integration, remote access, cyber defense, incident response, risk management and more.

Access Interactive sales consultants are technically astute and have an average over 20 years of industry experience. They are ready to apply their knowledge and technical expertise to recommending the best products and solutions and to providing efficient project management.

It is our focused mission to implement the best products, service and support in the industry to our clients.

OUR SECURITY PRACTICE

Access Interactive has developed a security/ compliance practice to help our customers deal with the ever-changing threat and compliance needs required in the modern data center. At our core we build our practice on technical expertise with HITRUST, PCIP, CEH/CPT and CISSP certified engineers, but it is our ability to help customers understand security and adapt that makes us special. We make security solutions practical and business relevant. Compliance for the sake of compliance will help you pass an audit, but when you understand the value of your security solutions your business will gain the protection it deserves and the confidence of your customers. We are designed to enhance your security posture by helping document governance goals and outlining your organizations compliance requirements. This time-tested strategy helps customers stand vigilant against not only attacks but offers a security posture that is consistent with industry best practices. Knowledge is power! Below you will find an overview of our three major pillars of engagement.

I. GOVERNANCE

The National Institute of Technology (NIST) describes IT governance as the process of establishing and maintaining a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls and provide assignment of responsibility. Access assists customers in defining these requirements as well as documenting the resolution.

II. COMPLIANCE

Compliance is a demonstration or a reporting function of how your security program meets specific security standards as laid out by regulatory organizations such as PCI, CISP, FIPS, CJIS, FOIA, HIPAA, Sarbanes-Oxley and many other industry specific needs. Once a Governance strategy has been established, we can align the security strategy with you're the customer internal processes with external regulation. Too often businesses strive to meet regularly requirements but lack the tools and communication to sustain the standards. Access helps our customer communicate internally so the culture supports regulatory compliance. This way the business is operating in a natural state that is bolstered by security, rather than encumbered by it.

III. PENETRATION TESTING

At a high level, a penetration test, “pen-test”, is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities. These vulnerabilities may exist in operating systems, services and application flaws, improper configurations or risky end-user behavior. Many Governance plans and most compliance ordinances require this type of tests at a designated cadence. Access offer several types of penetration testing, but these offerings can be categorized in three major definitions.

A. SOCIAL PENETRATION TESTING

Social engineering pen testing is designed to test employees' adherence to the security policies and practices defined by the organizations governance policies. Testing should provide a company with information about how easily an intruder could convince employees to break security rules or divulge or provide access to sensitive information. The company should also get a better understanding of how successful their security training is and how the organization stacks up, security-wise, in comparison to their peers.

B. EXTERNAL/INTERNAL PENETRATION TESTING

One of the most common vulnerability assessment activities for companies of all sizes is an external/ internal penetration testing scan, typically targeting internet-facing websites. Scanning external-facing network resources are a high priority, but a complete assessment of the hardness of your external network includes multiple steps, including:

I. Anonymous information gathering to discover all Internet-facing assets a hacker could identify as potential entry-points into your network
II. Scanning of your internet-available network access points and web servers for known vulnerabilities (non-credentialed)
III. Verifying scan-result findings through in-depth manual penetration testing attack techniques (both credentialed and non-credentialed)
IV. Providing deeply informed remediation guidance and advisory services for identified/verified vulnerabilities

C. APPLICATION PENETRATION TESTING

Application penetration testing is a key security requirement for a variety of regulatory frameworks, from PCI DSS and GLBA to HIPAA and FISMA. Many companies mistakenly assume that automated penetration testing tools can fulfill these requirements. But in truth, no automated vulnerability scanning solution can find every type of vulnerability or satisfy every regulatory requirement. Certain kinds of authorization issues or business logic flaws will only show up during manual web application penetration testing. We offer this service to our customers to make sure that the applications that run their businesses are safe. We take careful pride in application penetration testing as it is one of the most common methods of exploitation.

STRATEGIC DIRECTIVE

In response to the City of Novi (Novi) request for governance, risk and compliance engagement we firmly believe that Novi is a strong candidate for our Security Overlay offering. The Security Overlay is designed to create governance and policies that are audited, monitored and maintained throughout the enterprise. The beauty of The Security Solution is that Novi will receive consistent and inclusive security process consulting coupled with the due diligence of follow up maintenance. This product is uniquely designed to quickly to bring customer to security compliance and educate them on mechanics and tactics to maintain the agreed upon security parameters. The Security Overlay Program is designed to give you a team of security professionals using best of breed tools to document, defend and manage customer security objectives. This program will accomplish the following 5 steps:

1. Identify & evaluate current security readiness
2. Document & implement compliant regulations & controls imposed on customers
3. Monitor & report on users' and system activity
4. Continuously scan vulnerabilities
5. Support as needed in achieving yearly security milestones

In conclusion this solution is more than just a virtual Information Security Officer, it embodies the type of time attention it requires to maintain a valid environment industry standard best practices as well as the CJIS, HIPAA/HITECH and ISO 27001/2 frameworks. The customization of this agreement was built specifically on our yearly efforts ensuring compliance and industry best practices.

NOVI RESPONSIBILITIES

Novi acknowledges that its timely provision of and access to office accommodations, facilities, equipment, assistance, cooperation, complete and accurate information and data from Novi officers, agents, and employees, and suitably configured computer products (collectively, "**cooperation**") are essential to the performance of any Services set forth in this *SOW*. Novi acknowledges that Access Interactive's ability to perform the Services and any financial estimate related thereto depends upon the fulfillment of the responsibilities outlined in the Project Scope Considerations section of this SOW. If Novi fails to provide the requisite cooperation on a timely basis, Access Interactive shall be relieved of any schedule or milestone commitments associated with the Services.

As a condition of services, Novi agrees to and is responsible for:

- Provide Access Interactive with reasonable access to Novi functional, technical and business staff as necessary for Access Interactive to perform the Services. Access Interactive recognizes that Novi staff is dedicated to the daily operations of the facilities, and Access Interactive will use reasonable efforts to limit the demands on Novi staff to the best of its ability
- Provide working conditions that are conducive for the successful completion of the project for the duration of this engagement, including suitable office space, telephone access, and meeting facilities if needed

- Provide Access Interactive personnel, as required, with workstation(s) to enable Access Interactive and/or its agents to gain access to the software identified in the Service Description section
- Assign an Executive/Project Sponsor as the single Point-of-Contact for issue resolution, activity scheduling, interview scheduling, and information collection and dissemination. The Project Sponsor is responsible to ensure compliance with Novi obligations
- Work with Access Interactive via a documented change/prioritization process as identified in the SOW to agree on project deliverables, timing and resources in addition to any change to project priorities
- Provide updated organizational charts to Access Interactive to ensure proper communication channels are followed and understood by all parties
- Designate the Access Interactive Point-of-Contact as a central point-of-contact for all security activities for the duration of this *SOW*
- Provide an escalation to the Access Interactive Point-of-Contact for prompt issue resolution to minimize business impact from a time and cost prospective
- Work with Access Interactive Point-of-Contact by providing access to personnel who have knowledge of Novi Business Consultants current storage and server environments, as well as be able to identify appropriate support personnel who may be required to participate on project teams
- Make appropriate system maintenance windows available for Access Interactive (or authorized agents) as needed to perform Services
- Provide technical support for implementation teams, all vendors, and third parties as necessary
- Respond timely to Access Interactive's requests that Novi Business Consultants resources work on issues and tasks not directly stated in this *SOW*, but have a direct impact on the successful completion of this *SOW*
- Allow Access Interactive to post, at any site at which Services are performed, any documents necessary for Access Interactive to provide Services in compliance with the law
- Inform Access Interactive via email of all major changes to Novi Business Consultants network infrastructure and devices at least ten (10) business days ahead of the change.

NOVI SECURITY DELIVERABLES

The Security Solution was designed to maintain the commitments required to consistently attain compliance. In its origin The Security Solution was designed to create vigilance for compliance, but due to its expert nature allows for compliance advancement in many frameworks. Novi deliverables:

1. Gap Analysis – We will continually validate security controls & procedures to your compliance requirements
2. Security & Awareness Training – Continuous training, communication & testing of security awareness and industry best practices
3. The Security Solution Implementation – Will position your organization to achieve continuous compliance across various compliance frameworks
4. 3rd Party Accountability – Novi will have access to senior level compliance experts for all security related concerns
5. Security Peace of Mind – Continuously ensure security best practices are implemented & monitored in accordance to industry best practices
6. Defendable Position – Invigorating compliance aligned with customer & regulatory requirements

NOVI SECURITY COMPONENTS

The Security Solution is comprised of 4 major components:

1. **Software** – We use software tools for scanning & validating an environment
2. **Professional Services** – Hours are invested throughout the year in-order to maintain everchanging security requirements
3. **Subscription** – We are leveraging licenses of e-Tracker for continuous monitoring
4. **Annual Work Product** – Access will facilitate a one yearly Penetration-Test (External, Internal, Phishing, Social and Application Testing)

SUPPORTED COMPLIANCE FRAMEWORKS

(Listed below are compliance frameworks that Novi leverages in its monthly activities. Novi is not designed to certify compliance with any individual framework, but rather to prepare for compliance.)

NIST SP 800 – XXX

PCI DSS

HIPAA/ HITECH

ISO 27001/ 27002

FISMA

HITRUST

GLBA

GDPR

IRS PUBLICATION 1075

ITAR

NOVI SECURITY SCOPE OF SERVICES

ACTIVTY	Period	PCI Control Domain	In Scope/ Out Scope
Update Network and Data Flow Diagrams	Annually	1	Yes
Confirm training of developers in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities	Annually	6	Not included in scope, quoted separately
Review the security of off-site storage locations	Annually	9	Yes
Consult on/ review media inventory audit	Annually	9	Yes
Review of information security policy	Annually	12	Yes
Risk Assessment Matrix	Annually	12	Yes
Security Awareness program training upon hire and annually	Annually	12	Yes
Acknowledgement that personnel have read and understood the information security policy	Annually	12	Yes
Monitor status of all service providers – Third Party Assessments	Annually	12	Yes
Consult on test incidence response procedures	Annually	12	Yes
Public Facing Web Applications ONLY - if there is not a web application firewall in use a Web application vulnerability security assessment must be completed.	Annually & after any changes	6	Yes
Consult Review firewall and router rulesets	Bi-Annually	1	Yes
Service Providers - Internal Penetration Test, *or after any significant change*	Bi-Annually	11	Yes
Service Providers - External Penetration Test, *or after any significant change*	Bi-Annually	11	Yes
Keep all anti-virus policies updated as changes occur	Customer - Ongoing	5	Yes
Consult as needed ensure personal firewalls are actively running and not alterable by user	Customer - One-Time	1	Yes
Review the following daily: • All security events • Logs of all system components that store, process, or transmit sensitive data • Logs of all critical system components • Logs of all servers and system components that perform security functions.	Daily	10	Yes

Service Providers - reporting of failures of critical security control systems, including, but not limited to failure of: • Firewalls • IDS/IPS • FIM - (Not Included) • Anti-virus - (Not Included) • Physical access controls - (Not Included) • Logical access controls • Audit logging mechanisms	Daily	10	Yes
Consult as needed all network device configuration standards updated as changes occur	Ongoing	1	Yes
Consult as needed list of all ports/protocols/services along with business use	Ongoing	1	Yes
Consult as needed list of all insecure ports/protocols/services along with documented security features	Ongoing	1	Yes
Consult as needed all network device management polices updated as changes occur	Ongoing	1	Yes
Consult as needed: Wireless environments - change encryption keys when anytime anyone with knowledge of the keys leaves the company or changes positions	Ongoing	2	Yes
Consult as needed wireless configuration standards as changes occur	Ongoing	2	Yes
Consult as needed system configuration standards as changes occur	Ongoing	2	Yes
Consult as needed keep all system administration polices updated as changes occur	Ongoing	2	Yes
Consult as needed Encryption keys for storage are changed at the defined crypto period; or the retirement or replacement of keys when the integrity of the key has been weakened; or the replacement of known or suspected compromised keys.	Ongoing	3	Not included in scope, quoted separately
Consult as needed keep all data transmission polices updated as changes occur	Ongoing	3	Yes
Consult as needed keep all data retention and encryption policies up to as changes occur	Ongoing	4	Yes
New Security vulnerabilities are regularly identified	Ongoing	6	Yes

Risk Ranking is completed on all new vulnerabilities including identifying all "high" and critical" vulnerabilities	Ongoing	6	Yes
Consult as needed Installation of applicable critical vendor-supplied security patches within one month of release	Ongoing	6	Yes
Consult as needed Installation of all applicable vendor-supplied security patches within an appropriate time frame.	Ongoing	6	Yes
Consult as needed software development - affected systems/networks to verify that applicable requirements were implemented, and documentation updated as part of the change.	Ongoing	6	Yes
Consult as needed if any significant changes are made to the web application a web security assessment should be consulted on	Ongoing	6	Yes
SDLC documentation is updated and maintained as changes occur	Ongoing	6	Not included in scope, quoted separately
Consult as needed keep all patch management documentation updated and maintained	Ongoing	6	Yes
Consult as needed access control documentation is updated and maintained as changes occur	Ongoing	7	Yes
Consult as needed update physical security documentation as changes occur	Ongoing	9	Yes
Consult as needed maintain a list of devices	Ongoing	9	Yes
Consult as needed periodically inspect devices (the timeframe needs to be determined by the business entity.)	Ongoing	9	Yes
Keep all usage policies updated and maintained	Ongoing	12	Yes
Consult as needed keep all physical security and device management documentation updated and maintained	Ongoing	9	Yes
Consult as needed time synchronization technology is kept current	Ongoing	10	Yes
Consult as needed keep all logging process and policy documents up to date as changes occur	Ongoing	10	Yes

Consult as needed Service Provider – Respond to failures of critical security control systems in a timely manner. Processes for responding to failures in security controls must include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls	Ongoing		Yes
Consult as needed keep all vulnerability management documentation updated and maintained	Ongoing	11	Yes
Consult as needed keep inventory of authorized wireless access points up to date and include business justification	Ongoing	11	Yes
Consult as needed maintain a list of service providers - including which requirements are managed by each service provider, and which are managed by the entity	Ongoing	12	Yes
Consult as needed updating incident response plan as changes to the environment are made, industry updates, and lessons learned	Ongoing	12	Yes
Consult as needed periodically train personnel that are responsible for security breach procedures (time frame for training is determined by the business entity)	Ongoing	12	Yes
Consult as needed maintain a list and keep recent implementation guides for payment applications	Ongoing	All	Yes
Consult as needed maintain a table of all stored sensitive data including database, tables, and files storing data along with what data is stored and how it is protected	Ongoing	All	Yes
Consult as needed update and maintain asset inventory of all in scope systems	Ongoing	All	Yes

Consult as needed key Management Process Documentation	One-Time	3	Yes
Consult as needed Service Provider - if sharing keys, guidance given to customers on how to securely transmit, store and update customers' keys	One-Time	3	Yes
Consult as needed Service Provider - documented description of the cryptographic architecture • Details of all algorithms, protocols, and keys used for the protection of sensitive data, including key strength and expiry date • Description of the key usage for each key. • Inventory of any HSMs and other SCDs used for key management	One-Time	3	Yes
Consult as needed - incorporate multi-factor authentication for all non-console access into the administrative access for critical data.	One-Time	8	Yes
Documented Risk Assessment Process	One-Time	12	Yes
Documented Security Awareness Program	One-Time	12	Yes
Documented process for engaging service providers including due diligence prior to engagement	One-Time	12	Yes
Service Providers - acknowledge in writing to customers the for which they are responsible and those that belong to their customers	One-Time	12	Yes
Consult as needed Service Providers - Executive management shall establish responsibility for the protection of data and a compliance program to include: • Overall accountability for maintaining compliance • Defining a charter for a compliance program and communication to executive management	One-Time	12	Yes
Consult as needed key custodians to acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.	One-Time	3	Not included in scope, quoted separately
Provide training for personnel to be aware of attempted tampering or replacement of devices (the timeframe needs to be determined by the business entity.)	Quarterly	9	Yes
Identify and securely delete stored data that exceeds defined retention requirements	Quarterly	3	Yes
Review & Track - Remove/disable inactive user accounts	Quarterly	8	Yes

Consult as needed Implement a process to test for wireless access points and detect and identify all authorized and unauthorized wireless access points within the environment	Quarterly	11	Yes
Service Providers ONLY - Perform reviews to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: • Daily log reviews • Firewall rule-set reviews • Applying configuration standards to new systems • Responding to security alerts · Change management processes	Quarterly	12	Yes
Review FIM Alerts	Real-Time	11	Yes
Consult as needed Review IDS/IPS Alerts	Real-Time	11	Yes

**The above matrix is a synopsis of the work included in our Novi Solution. Access Interactive has a formal process for validation and completion of work.*

OUT OF SCOPE

Only the Services specified in the above Services Description section will be provided. The following are examples of services that Access Interactive will not provide, unless specifically stated in the description of the Service:

- Inform Novi via email of all third parties that Access Interactive may encounter while performing its contracted services
- Maintain a service agreement for all equipment and applications
- Access Interactive is responsible for performing only the Services described in this SOW. All other services are considered outside the scope of this SOW. If Novi Business Consultants wishes to modify the Services, or the systems that the Services are performed on, Novi Business Consultants must comply with the change procedures described in the Change Procedures section.

ASSUMPTIONS

- Novi services begin on the designated start day after signed contract
- Novi authorizes Access with the proper security authentication permissions
- Novi will be available for support and oversight throughout the course of the contract
- Incidents contained during the duration of the contract can be resolved with separate scopes of work based on size and severity
- Novi does not include internal penetration testing or application penetration testing. These items can be quoted on a case by case basis.
- Novi agrees to analog recommendations and the findings associated with Novi services
- Novi is designed to document, improve and maintain security practices. This product is designed to create visibility and change, it is not an Audit

NOVI CONTRACT TERMS

Fee Schedule: A 12-month contract is required to initiate the Security Solution Service. One month down payment is required to begin the project. All licenses purchase if any are to be purchased 100% upon signature.

Early Termination: In event of early termination, customer is responsible for the payments up to the point of termination. Either Party can request termination. Termination requests will need to be presented 182 Days before the Security contract is terminated.

Contract Renewal: After 12-months, service will continue to run at the agreed upon monthly rates unless otherwise negotiated. 60-days' notice for cancellation is required.

Late Payment: Novi shall make payments to Access Interactive within Forty-five (45) days of receiving any invoice for services. Any amount remaining unpaid after twenty-one (21) days shall accrue interest at a rate equal to the lesser of: (a) one and one-half percent (1.5%) per month; or (b) the highest rate allowed by law. Invoices submitted by Access Interactive to Novi are deemed accepted and approved unless disputed by Novi within twenty-eight (28) business days of Novi receipt of the invoice.

PHASE	DESCRIPTION	QTY	
I.	Security Overlay & Assessment	1	
II.	Carbon Black Threat Hunter Yearly	425	
III.	Nessus/ Qualys Vulnerability Scanning Yearly	425	
IV.	BlueMira (SIEM) Yearly	425	
V.	Phishing Email Fishing Campaign	1	
VI.	Passing External Vulnerability Scan	4	
VII.	Passing Internal Vulnerability Scans	4	
VIII.	Live Security Awareness & Training	1	
IX.	Pen Test (Internal, External & WebApp)	2	
X.	Third Party Risk Assessments (Critical Vendors)	10	
		SUBTOTAL:	$76,787
		TAX:	--
		TOTAL:	$ 76,787
		MONTHLY TOTAL:	$ 6,398.91

Quote Valid for 14-Days. Prices Subject to Change with Notice Depending on Current Market Conditions.

AUTHORIZED SIGNATURE: ____ **DATE:** _________________________

PRINTED NAME: ___________________________________ **PURCHASE ORDER NO:** ______________________