

City of Santa Fe, New Mexico

memo

DATE: January 27, 2015

TO: Finance Committee

FROM: Robert Rodarte, Officer
Purchasing Division

VIA: Oscar S. Rodriguez, Director
Finance Department

SUMMARY: Procurement of ITT Security Assessment:
Procurement Method: State Price Agreement #10-000-00-0051AI:
Vendor: CAaNES, LLC. (Albuquerque)

The ITT Department is requesting the procurement of Professional Service Contract, to conduct an Information Security Posture Assessment on the City's Network and Application System Infrastructure. CAaNES, LLC is the authorized vendor under this State Price Agreement. The total amount of the contract will be \$55,000 plus applicable gross receipt taxes.

By City policy, the City can use State or Federal Price Agreements without having to bid the items on its own. By City policy, procurement from State of Federal Price Agreements over \$50,000, require City Council approval (City Purchasing Manual Section 11.1).

Funding for this procurement will be available in City Account Numbers 12029.510340 and 12029.530710 (ITT Consulting Services and Software Subscription). The ITT Department has attached a "BAR" to transfer the funds into the correct line items.

ACTION REQUESTED:

It is requested that this procurement of Professional Services to CAaNES, LLC, from State Price Agreement #10-000-00-0051AI, in the amount \$55,000.00 plus applicable gross receipt taxes, be reviewed, approved and submitted to the City Council for its consideration.

City of Santa Fe, New Mexico

memo

DATE: January 23, 2015

TO: Finance Committee/Council
Brian Snyder, City Manager

VIA: Renée Martínez, ITT Department Director *RM*
Oscar Rodriguez, Finance Director *OR*
Robert Rodarte, Purchasing Director *RR*

FROM: Yodel M Catanach, Telecommunication Specialist *YMC*

RE: Computational Analysis and Network Enterprise Solution a/k/a CAaNES

SUMMARY:

We request approval of the attached CAaNES PSA to conduct an Information Security Posture Assessment on the City's Network and Application System Infrastructure. The PSA will allow CAaNES to analysis and test Internal and External City Infrastructure. The following are some of the key assessments outlined in PSA.

- Information Security Assessment Plan
- Penetration Testing Summary
- Identify Gaps in Required Regulatory Compliance (HIPAA and FISMA) and Best Practices
- RiskSense Annual Software to Optimize and Manage Security and Vulnerability

The cost of this PSA is \$55,000 and will be charged to 12029.510340 Consulting Services in the amount of \$35,000 and 12029.530710 Software Subscription in the amount of \$20,000.

Legal has reviewed, approved, and signed the PSA, and Purchasing has approved and reviewed the SPA Contract #10-000-00-00051AI.

ACTION REQUESTED

ITT Department request approval of CAaNES Professional Services Agreement.



SUSANA MARTINEZ
GOVERNOR

ED BURCKLE
CABINET SECRETARY

LAWRENCE O. MAXWELL
DIRECTOR
STATE PURCHASING DIVISION

State of New Mexico

General Services Department

ADMINISTRATIVE SERVICES DIVISION
(505) 827-2000

FACILITIES MANAGEMENT DIVISION
(505) 827-2141

STATE PURCHASING DIVISION
(505) 827-0472

RISK MANAGEMENT DIVISION
(505) 827-0442

STATE PRINTING & GRAPHIC SERVICES BUREAU
(505) 476-1950

TRANSPORTATION SERVICES DIVISION
(505) 827-1958

Date: January 23, 2014

CAaNES, LLC
7801 Academy Road NE, Ste. 1-202
Albuquerque, NM 87109

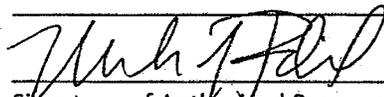
RE: Extend the term of IT Professional Services Price Agreement No. 10-000-00-00051A1

Please be advised, the New Mexico Statewide Price Agreement above will expire **March 30, 2014**. By mutual agreement between the New Mexico State Purchasing Agent and CAaNES, LLC the awarded vendor, we would like to extend this price agreement through **March 31, 2015** at the same terms, price and conditions of the original price agreement or any subsequent amendments thereafter. Be advised, the New Mexico State Purchasing Division must receive a response from you, the awarded vendor for this extension to be in effect.

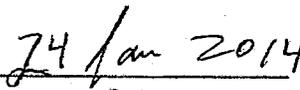
Please respond by EMAILING your signature on this memorandum to Teri Arevalo at teri.arevalo@state.nm.us **no later than February 7, 2014**.

- I wish to extend
 I do not wish to extend

Company Name and Address (if different than above):



Signature of Authorized Representative



Date

Thank you for your business with the State.
Sincerely,



Teri Arevalo
GSD IT Procurement Specialist

CITY OF SANTA FE
PROFESSIONAL SERVICES AGREEMENT

THIS AGREEMENT is made and entered into by and between the City of Santa Fe (the "City") and Computational Analysis and Network Enterprise Solutions, LLC (the "Contractor"). The date of this Agreement shall be the date when it is executed by the City and the Contractor, whichever occurs last.

1. SCOPE OF SERVICES

The Contractor shall provide the following services for the City and also described in Exhibit "A" attached hereto and incorporated herein:

- A. Security Assessment Executive Summary
- B. Security Posture Assessment Reports
- C. Snapshot of Critical Information Security Risks
- D. Web and Application Information Security Posture
- E. Penetration Testing Summary
- F. Configurations Review Summary with Recommendations
- G. Recommendations and Executive level presentations summarizing the assessment process and results

2. STANDARD OF PERFORMANCE; LICENSES

A. The Contractor represents that it possesses the personnel, experience and knowledge necessary to perform the services described under this Agreement.

B. The Contractor agrees to obtain and maintain throughout the term of this Agreement, all applicable professional and business licenses required by law, for itself, its employees, agents, representatives and subcontractors.

3. COMPENSATION

A. The City shall pay to the Contractor in full payment for services rendered, a sum not to exceed Fifty-Five Thousand dollars (\$55,000.00), plus applicable gross receipts taxes. Payment shall be made for services actually rendered as described in Exhibit "A" attached hereto.

B. The Contractor shall be responsible for payment of gross receipts taxes levied by the State of New Mexico on the sums paid under this Agreement.

C. Payment shall be made upon receipt and approval by the City of detailed statements containing a report of services completed. Compensation shall be paid only for services actually performed and accepted by the City.

4. APPROPRIATIONS

The terms of this Agreement are contingent upon sufficient appropriations and authorization being made by the City for the performance of this Agreement. If sufficient appropriations and authorization are not made by the City, this Agreement shall terminate upon written notice being given by the City to the Contractor. The City's decision as to whether sufficient appropriations are available shall be accepted by the Contractor and shall be final.

5. TERM AND EFFECTIVE DATE

This Agreement shall be effective when signed by the City and terminate on June 30, 2015, unless sooner pursuant to Article 6 below.

6. TERMINATION

A. This Agreement may be terminated by the City upon 30 days written notice to the Contractor.

(1) The Contractor shall render a final report of the services performed up to the date of termination and shall turn over to the City original copies of all work product, research or papers prepared under this Agreement.

(2) If compensation is not based upon hourly rates for services rendered, the City shall pay the Contractor for the reasonable value of services satisfactorily performed through the date Contractor receives notice of such termination, and for which compensation has not already been paid.

(3) If compensation is based upon hourly rates and expenses, then Contractor shall be paid for services rendered and expenses incurred through the date Contractor receives notice of such termination.

7. STATUS OF CONTRACTOR; RESPONSIBILITY FOR PAYMENT OF EMPLOYEES AND SUBCONTRACTORS

A. The Contractor and its agents and employees are independent contractors performing professional services for the City and are not employees of the City. The Contractor, and its agents and employees, shall not accrue leave, retirement, insurance, bonding, use of City vehicles, or any other benefits afforded to employees of the City as a result of this Agreement.

B. Contractor shall be solely responsible for payment of wages, salaries and benefits to any and all employees or subcontractors retained by Contractor in the performance of the services under this Agreement.

C. The Contractor shall comply with City of Santa Fe Minimum Wage, Article 28-1-SFCC 1987, as well as any subsequent changes to such article throughout the term of this contract.

8. CONFIDENTIALITY

Any confidential information provided to or developed by the Contractor in the performance of this Agreement shall be kept confidential and shall not be made available to any individual or organization by the Contractor without the prior written approval of the City.

9. CONFLICT OF INTEREST

The Contractor warrants that it presently has no interest and shall not acquire any interest, direct or indirect, which would conflict in any manner or degree with the performance of services required under this Agreement. Contractor further agrees that in the performance of this Agreement no persons having any such interests shall be employed.

10. ASSIGNMENT; SUBCONTRACTING

The Contractor shall not assign or transfer any rights, privileges, obligations or other interest under this Agreement, including any claims for money due, without the prior written consent of the City. The Contractor shall not subcontract any portion of the services to be performed under this Agreement without the prior written approval of the City.

11. RELEASE

The Contractor, upon acceptance of final payment of the amount due under this Agreement, releases the City, its officers and employees, from all liabilities, claims

and obligations whatsoever arising from or under this Agreement. The Contractor agrees not to purport to bind the City to any obligation not assumed herein by the City unless the Contractor has express written authority to do so, and then only within the strict limits of that authority.

12. INSURANCE

A. The Contractor, at its own cost and expense, shall carry and maintain in full force and effect during the term of this Agreement, comprehensive general liability insurance covering bodily injury and property damage liability, in a form and with an insurance company acceptable to the City, with limits of coverage in the maximum amount which the City could be held liable under the New Mexico Tort Claims Act for each person injured and for each accident resulting in damage to property. Such insurance shall provide that the City is named as an additional insured and that the City is notified no less than 30 days in advance of cancellation for any reason. The Contractor shall furnish the City with a copy of a Certificate of Insurance as a condition prior to performing services under this Agreement.

B. Contractor shall also obtain and maintain Workers' Compensation insurance, required by law, to provide coverage for Contractor's employees throughout the term of this Agreement. Contractor shall provide the City with evidence of its compliance with such requirement.

C. Contractor shall maintain professional liability insurance throughout the term of this Agreement providing a minimum coverage in the amount required under the New Mexico Tort Claims Act. The Contractor shall furnish the City with proof of insurance of Contractor's compliance with the provisions of this section as a condition

prior to performing services under this Agreement.

13. INDEMNIFICATION

The Contractor shall indemnify, hold harmless and defend the City from all losses, damages, claims or judgments, including payments of all attorneys' fees and costs on account of any suit, judgment, execution, claim, action or demand whatsoever arising from Contractor's performance under this Agreement as well as the performance of Contractor's employees, agents, representatives and subcontractors.

14. NEW MEXICO TORT CLAIMS ACT

Any liability incurred by the City of Santa Fe in connection with this Agreement is subject to the immunities and limitations of the New Mexico Tort Claims Act, Section 41-4-1, et. seq. NMSA 1978, as amended. The City and its "public employees" as defined in the New Mexico Tort Claims Act, do not waive sovereign immunity, do not waive any defense and do not waive any limitation of liability pursuant to law. No provision in this Agreement modifies or waives any provision of the New Mexico Tort Claims Act.

15. THIRD PARTY BENEFICIARIES

By entering into this Agreement, the parties do not intend to create any right, title or interest in or for the benefit of any person other than the City and the Contractor. No person shall claim any right, title or interest under this Agreement or seek to enforce this Agreement as a third party beneficiary of this Agreement.

16. RECORDS AND AUDIT

The Contractor shall maintain, throughout the term of this Agreement and for a period of three years thereafter, detailed records that indicate the date, time and nature of services rendered. These records shall be subject to inspection by the City, the

Department of Finance and Administration, and the State Auditor. The City shall have the right to audit the billing both before and after payment. Payment under this Agreement shall not foreclose the right of the City to recover excessive or illegal payments.

17. APPLICABLE LAW; CHOICE OF LAW; VENUE

Contractor shall abide by all applicable federal and state laws and regulations, and all ordinances, rules and regulations of the City of Santa Fe. In any action, suit or legal dispute arising from this Agreement, the Contractor agrees that the laws of the State of New Mexico shall govern. The parties agree that any action or suit arising from this Agreement shall be commenced in a federal or state court of competent jurisdiction in New Mexico. Any action or suit commenced in the courts of the State of New Mexico shall be brought in the First Judicial District Court.

18. AMENDMENT

This Agreement shall not be altered, changed or modified except by an amendment in writing executed by the parties hereto.

19. SCOPE OF AGREEMENT

This Agreement incorporates all the agreements, covenants, and understandings between the parties hereto concerning the services to be performed hereunder, and all such agreements, covenants and understandings have been merged into this Agreement. This Agreement expresses the entire Agreement and understanding between the parties with respect to said services. No prior agreement or understanding, verbal or otherwise, of the parties or their agents shall be valid or enforceable unless embodied in this Agreement.

20. NON-DISCRIMINATION

During the term of this Agreement, Contractor shall not discriminate against any employee or applicant for an employment position to be used in the performance of services by Contractor hereunder, on the basis of ethnicity, race, age, religion, creed, color, national origin, ancestry, sex, gender, sexual orientation, physical or mental disability, medical condition, or citizenship status.

21. SEVERABILITY

In case any one or more of the provisions contained in this Agreement or any application thereof shall be invalid, illegal or unenforceable in any respect, the validity, legality, and enforceability of the remaining provisions contained herein and any other application thereof shall not in any way be affected or impaired thereby.

22. NOTICES

Any notices required to be given under this Agreement shall be in writing and served by personal delivery, email or by mail, postage prepaid, to the parties at the following addresses:

City of Santa Fe:
Yodel Catanach
ITT
P.O. Box 909
Santa Fe, NM 87504

Contractor:
Mark J. Fidel, President
7801 Academy Rd. NE, Suite 1-202
Albuquerque, NM 87109
505.217.9422 x 101
mfidel@caanes.com

IN WITNESS WHEREOF, the parties have executed this Agreement on the date set forth below.

CITY OF SANTA FE:

CONTRACTOR:
Computational Analysis and
Network Enterprise Solutions, LLC

JAVIER M. GONZALES, MAYOR

Mark Field, President

NAME & TITLE

DATE: _____

DATE: 31 Dec 2014

CRS # 03-079518-00-4
City of Santa Fe Business
Registration # 14-00102385

ATTEST:

YOLANDA Y. VIGIL
CITY CLERK

APPROVED AS TO FORM:

MBM *12/15/14*

KELLEY A. BRENNAN, CITY ATTORNEY

APPROVED:

OSCAR RODRIGUEZ, DIRECTOR
FINANCE DEPARTMENT

Exhibit A

1. Description of Work

CAaNES security posture assessment and penetration testing methodology enables proactive detection and remediation of security vulnerabilities. The assessment is conducted to evaluate (Technical, Operational, and Management) controls in place at the network, system, and application layers that help protect Customer systems and data from unauthorized access, use and compromise.

The IT risk assessment services provide a comprehensive evaluation of Customer's Security Posture with minimal disruption to the Customer.

The assessment is divided into four major categories:

- Infrastructure and Technical Controls Assessment (Internal and External)
- Application Security Posture Assessment
- Penetration Testing
- Road Map to achieve Baseline Security

The assessment includes the operations and technologies associated with directly defending against interruption, interception, modification, and fabrication to the Customer's network. To ensure complete information security posture assessment the assessment includes analysis of information systems, network peripherals, information security devices, and applications.

Descriptions of the four major categories are given below:

- **Infrastructure and Technical Controls Assessment (Internal and External):**

Is a comprehensive evaluation of current network, applications, systems, and computing environments using best practices and non-invasive methods to identify gaps in Customer's computing environment.

To ensure complete information security posture assessment, our team performs assessments using a multi scanner approach based on

100% coverage of every device (every device with an IP address printers, network peripherals, desktops, servers, VMs, etc.) within the internal network and external IP ranges owned by the Customer.

- **Application Security Posture Assessment:**

Is an evaluation of web applications in a distinct and customized approach based on the target web application's features. CAaNES provides an in-depth understanding of how an input changes data inside the application.

CAaNES uses a proprietary framework to discover multiple attack vectors by passing or inputting data to user interfaces, network interfaces, application programming interfaces (APIs), and other places where inputs are processed.

- **Penetration Testing (Infrastructure and Web Applications)**

Is a test designed with an adversarial intent to gain unauthorized access to portions of Customer's network and Web Applications from the perspective of a trusted user and adversary from inside, remote and external.

Target web applications are tested for privilege escalation in which CAaNES security consultants login to the application using a least privileged user account, try to escalate user access level by identifying insecure direct object references and gain access to data items that are restricted to users with higher privilege access levels.

During this testing phase, session controls of the application are also validated and session hijacking is performed to gain privilege escalation

- **Recommendations and Road Map to Achieve Baseline Security:**

CAaNES team provides recommendations on how to address the identified gaps within Customer's regulatory, infrastructure, and applications.

CAaNES provides a detailed analysis on vulnerability/threat pairs and their impact to the Customer as well as a requirement traceability matrix to mitigate current threats and achieve baseline security for High-Impact systems.

A few key differentiators are listed below:

- Vulnerabilities are presented with context and mapped to Tactics, Techniques and Procedures (TTPs) commonly used by most advanced adversaries.
- Assessments provide insights and context into ease of attackers ability to access or damage sensitive data linearly and laterally on the network and Web applications.

- Our analytical skills, automated in RiskSense®, provide our clients a platform to ingest massive amounts of vulnerability data and scale to thousands of machines to gain meaningful insights to reduce threats to critical business systems.
- We Use Semantics and Context Based Crawling for Web Application Security Assessments. Our proprietary crawler pares HTML, Java scripts, and hidden objects to extract links to gain maximum overage.

About RiskSense®

- RiskSense is engineered as a scalable solution for distributed complex enterprise networks. While not limiting itself to key assets, RS can be applied to the entire organizational information technology infrastructure to immensely reduce the time involved in vulnerability management life cycle (from detection to remediation) from weeks to hours and minutes.
- RiskSense ingests large volumes of security data, quickly identifies the information that is relevant with veracity, determines the existence and severity of advanced attacks, and provides solutions to fix critical vulnerabilities and change the threat landscape.

2. Deliverables

CAaNES will perform the services and activities described. These services, activities, and responsibilities characterize the full set of deliverables for this Project.

1. Security Assessment Executive Summary

- a. The Executive Summary is a high level report of the summary findings from the assessment and is intended for senior managers. It will identify and discuss the top findings from the assessment with the highest potential for risk impact to the End-Client.

2. Security Posture Assessment Reports

- a. The Security Posture Assessment Reports provide a broad view of IT infrastructure elements and functional components with regard to their vulnerabilities associated with internal and external threats.
- b. The findings are determined through scans and penetration tests and provided detailed technical information on the vulnerabilities and remediation approaches. The elements and functional components for this report are as follows:

- External, internal, and remote security posture

3. Snapshot of Critical Information Security Risks

- a. This report provides a summary and ranking of the top 5 critical areas of the End-Client's IT security posture that have the greatest risks impact from an information assurance standpoint.
- b. Our risk ranking methodology presents risks as High, Medium, and Low priority based on many factors, including ease of exploitation, business criticality of the host and prevalence of the threat.
- c. The vulnerabilities associated with the identified risks and how they may be compromised is detailed in this report.

4. Web and Application Information Security Posture

- a. The Web and Application Information Security Posture report is a consolidated report includes findings from

all of the web and applications scanners including the CAaNES proprietary data mining analysis work.

- b. The report organizes the findings based on the OWASP Top 10 and the CWE/SANS Top 25.
- c. Within the report, the vulnerabilities found will be categorized as High, Medium or Low risks.

5. Penetration Testing Summary

- a. The Penetration Testing Summary provides the details of finding determined from internal and external attempts to compromise IT systems. The vulnerabilities associated with these risks and how they may be compromised is detailed in this report.

6. Configurations Review Summary with Recommendations

- a. This report provides a summary of recommendations for security controls setting configurations of the various devices in the IT infrastructure found to be at risk. It includes details down to operating system control settings.

7. Recommendations and Executive level presentations summarizing the assessment process and results:

- a. Presentations are prepared which summarizes of all of reports and the major findings from the assessment. They are written to an appropriate level of detail for Executive Management and for IT Staff and Division Directors.

3. Project Pricing

Assessment Type	Service Description	Estimated Effort	Cost
<p>Infrastructure Vulnerability Assessment and Penetration Testing (Internal and External) Upto 2000 Active Nodes</p>	<p>Assess and Test technical infrastructure controls for security vulnerabilities from inside and outside the network:</p> <ul style="list-style-type: none"> • Reconnaissance and Device Discovery (Identify Darknets and Active IPs) • Vulnerability Scanning (Multiple Scanners to Discover Vulnerable Services and Misconfigurations) • Penetration Testing (To Verify Vulnerabilities – Eliminate False Positives) Automated and Manual • Analyze the Assessment Results to Develop Recommendations to Remediate Identified Vulnerabilities • Conduct Knowledge Transfer and be Available to Answer Questions 	<p>150 Hours 92 B (58+) 7</p>	<p>20,000</p>
<p>Web Application Security Assessment – Penetration Testing (Upto 5 Web Applications)</p>	<p>Coordinate and perform in-depth manual and automated security testing on critical applications:</p> <ul style="list-style-type: none"> • Discovery: Gather and review documentation and data required to conduct the testing. • Automated Testing: Utilize several different software tools to discover as many vulnerabilities as possible. • Manual Testing: Using output from the automated testing tools, analyze any additional threats that might have been missed or that require further testing. • Findings Analysis: Manually verify issues that have been identified in automated and manual testing. Identify and rate the business impact and risk for inclusion in reports and presentations. • Documentation & Reporting: Provide a report that summarizes results, findings and recommendations—to individual 	<p>A 120 Hours</p>	<p>15,000</p>

	agencies, and collectively.		
RiskSense (Annual Software as a Service)	<ul style="list-style-type: none"> • RiskSense: Single Pane of Glass to Optimize and Manage Security and Vulnerability Data. • RiskSense: continuously ingests massive amounts of data, quickly identifies vulnerabilities that are relevant and provides solutions to fix most critical vulnerabilities and change the threat landscape. • RiskSense facilitates communication between all levels of an organization, from upper management to technicians, providing users with a holistic and succinct assessment of their security posture and risks. 		20,000
Total Cost		\$55,000 + NMGRT	

4. **Authorization**

By signing this SOW, City of Santa Fe authorizes CAaNES to begin scheduling of work to deliver the professional services per this SOW.

The effective date of this SOW is the latest signature date shown below. Electronic signatures on this SOW will be accepted only in the form and manner prescribed by CAaNES LLC.

Acknowledged & Agreed

City of Santa Fe

CAaNES LLC



Signature

Signature

Print Name

Mark J. Fidel

Print Name

Title

President and Managing Partner

Title

Date

11/05/2014

Date

Project Completion Form

Please sign below to confirm your acceptance that CAaNES has completed the Project in accordance with the SOW for City of Santa Fe dated November 05, 2014.

City of Santa Fe - Security Posture Assessment and Penetration Testing

COMPLETION DATE _____

Acknowledged & Agreed

City of Santa Fe

Signature

Print Name

Title

Appendix: Service Descriptions

5. Infrastructure and Technical Controls Assessment (Internal and External)

Our assessments are based on proven, non-intrusive and patent pending methodologies and are the most comprehensive in the industry. Our experts will use proprietary tools and redundant benchmark tools to ensure cross validation and uniformity of process and consistency of results. The assessment effort will be divided into three major categories, internal, external and remote assessment.

Assessments include the operations, processes and technologies associated with directly defending against interruption, interception, modification, and fabrication to the client's network, information systems and information operations. To ensure complete information security posture assessment, our team performs assessments based on **100% coverage** of every device. Every device with an IP address will be assessed for security risks (System, Network, Application, and Compliance).

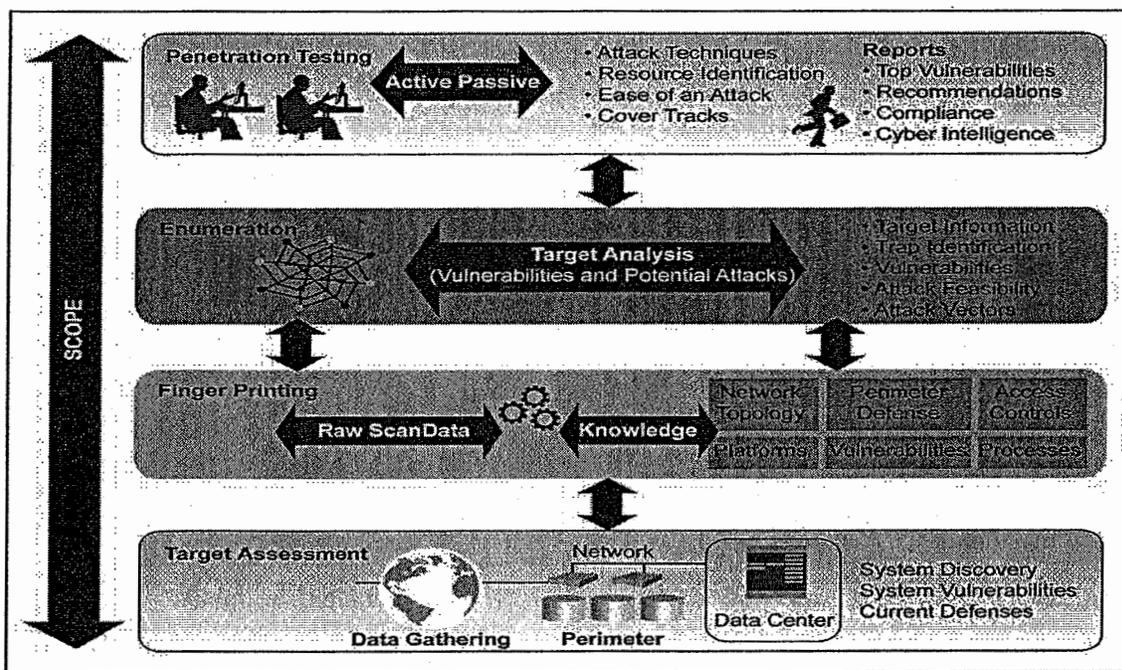


Figure 2: Strike Force Technical Controls Assessment Process and Framework

The assessment will include analysis and review of policies, applications, information systems, network peripherals, information security devices (firewalls, intrusion prevention and detection systems), remote access services, wireless access points, printers, back-up systems, log management systems, voice over IP systems, disaster recovery techniques and physical

security. **Figure 2** illustrates the Strike Force Assessment Process and Framework process developed by our Team to perform assessments.

Our security assessments provide a comprehensive evaluation of current network, applications, systems, and computing environments using best practices and non-invasive methods. To ensure a complete information internal security posture assessment, the assessment will include analysis and review of information systems (core components of client's infrastructure, routers, firewalls, desktops, and servers), network peripherals, information security devices, printers, back-up systems, log management systems, disaster recovery techniques and physical security.

Network Posture Assessment

A review of client's network architecture to determine how it effectively isolates untrusted outside networks from gaining access to client's internal, trusted networks and information.

- Review of current network architecture
- Analysis of individual nodes, servers and peripherals on the network
- Assessment of current authentication methods (user and hardware perspective)
- Network topology review and assessment of current services
- Critical node assessment for fail over analysis

Review all Communication Channels, Protocols, and Data Flow

A review of client network design and implementations to determine how effectively it isolates insiders based on their roles and need to access client's information resources

- Data flow analysis
- Assessment of physical and logical connections
- Network Assets inventory and classification
- Protocols used for communication
- Dial-in and remote connection assessments

Security Posture Assessment

A thorough review of security controls of the client covering policy, processes, procedures, people, access controls, network, communications, systems and compliance from inside, remote and outside.

- Perimeter analysis

- Internal analysis
- Remote access services and virtual private network analysis

Firewall Security Posture Assessment

A review of client's firewall architecture to determine how effectively it isolates untrusted outside networks from gaining access to client's internal, trusted networks and information. Analysis is completed from both an egress and ingress perspective.

- Review of current firewall architecture
- Analysis of firewall configuration
- Review and analysis of redundant rules, unused rules, and permissive rules
- Patching and version control analysis

Assessment and analysis of firewall rule base to include identifying: promiscuous rules, shadowed rules, redundant rules and misconfigurations.

- Assessment and analysis for insecure communications (port | protocols | services)
- Critical node assessment for fail over analysis

Penetration Testing and Analysis

Penetration Testing - A test designed with an adversarial intent to gain unauthorized access to portions of client's network from the perspective of a trusted user and adversary from inside, remote and outside.

- Perform reconnaissance and penetration testing on the network from internal nodes, remote nodes and external nodes
- Perform analysis on possible secondary exploits
- Red teaming refers to the work performed to provide an adversarial perspective
- Perform war driving and attempt to gain access to client's wireless access points

Virtual Infrastructure Review

A review of policies, procedures, and processes surrounding virtual infrastructure to identify gaps and mitigate risks

- Review virtual infrastructure architecture
- Review access controls, patch management and system separation

- Review virtual network segmentation, logging, and audit controls

Common Tools

Network security assessments are very dynamic in nature and use a wide variety of tools. The following is a list of tools that are used during this type of engagement. The specific demands of a test may necessitate additional tools or code to be created.

Network Security Assessment Tools			
Tool Name	Category	Functionality	Notes
Metasploit	Framework	Exploitation, Post-Exploitation	Metasploit Framework
Wireshark	Analyzer	Network Traffic Analysis	Wireshark
Nmap	Scanner	Network Discovery, Port Scanning	Nmap
Metasploit	Framework	Exploitation, Post-Exploitation	Metasploit Framework

6. Web Application Security Posture Assessment

CAaNES evaluates web applications in a distinct and customized approach based on the target web application's features. This is achieved using CAaNES' proprietary framework and industry's leading automated tools. We divide a web application security posture into two phases:

- Automated Testing Phase
- Manual Testing and Penetration Phase

Automated testing forms the initial layer of web application security posture and reflects black box testing of the web application. In this phase leading web application vulnerability scanners are used to scan and test the web application for critical vulnerabilities. CAaNES' security consultants are proficient in training these tools based on application's architecture and compliance requirements.

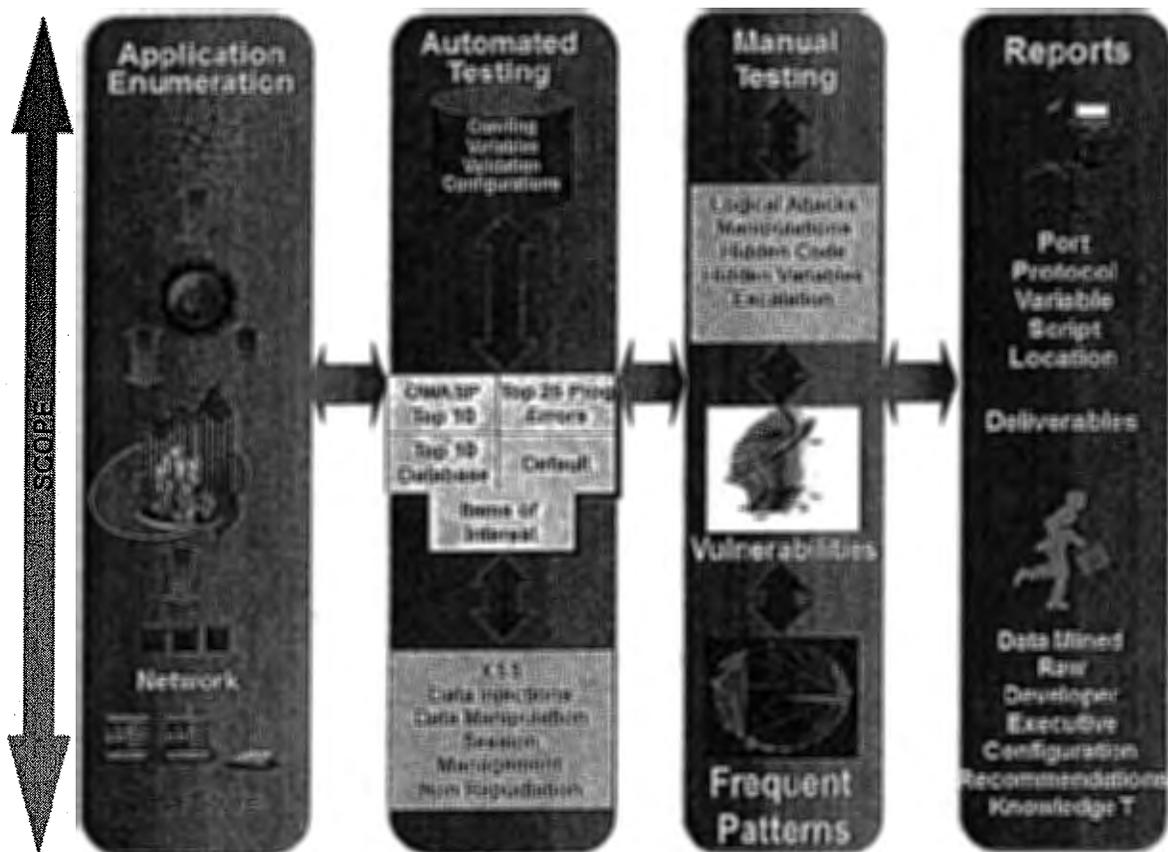


Figure 3: Proprietary Web Application Security Posture Assessment Methodology

Why go beyond automated testing?

Manual testing forays into areas where automated testing fails to make its mark. CAaNES uses its proprietary framework in this phase to overcome limitations of automated tools which CAaNES security experts have identified using their vast web application penetration testing knowledge. This phase is used to test security standards followed in every aspect of a web application; ranging from its internal logic control flow to any existing misconfiguration issues. CAaNES powered manual testing provides following additional features:

- **Business Logic Testing**

CAaNES security consultants analyze the existing business logic of a web application and find security flaws within the control flow of data. E-commerce and financial applications are targets of attacks, which exploit security flaws in control flow of data within the application. In this testing phase, data flow of hidden variables is analyzed and manipulated to validate security flaws while the application still meets business logic requirements.

- **Privilege Escalation (Grey box testing)**

Target web applications are tested for privilege escalation in which CAaNES security consultants login to the application using a least privileged user account, try to escalate user access level by identifying insecure direct object references and gain access to data items that are restricted to users with higher privilege access levels. During this testing phase, session controls of the application are also validated and session hijacking is performed to gain privilege escalation.

- **Virtual Directory Crawling**

Automated scanners have a serious limitation in crawling virtual directories configured for a web application. Since the virtual directory is not being crawled, all web pages and data within the virtual directory is omitted for testing during the automated phase. CAaNES detects existing virtual directories within a web application and crawls using its proprietary framework **AppSploit** and performs vulnerability testing on pages and data within virtual directory.

- **Web 2.0 Vulnerabilities**

Emerging web 2.0 technologies have increased the leverage users have on web applications. Applications built using web 2.0 technologies like AJAX (Asynchronous JavaScript and XML) enable

users to upload and change content existing on web applications. These technologies are capable of querying web service related data directly from the back end.

Considering these advances in web applications, CAaNES consultants test for vulnerabilities related to web 2.0 like AJAX injections and XML injections using proprietary scripts. This stage is used to analyze security standards of different APIs communicating with the target web application.

- **Complex Vulnerability Demonstration**

Automated scanners might find and report vulnerabilities existing in a web application, but they often fail to project the true criticality of these vulnerabilities. CAaNES security consultants combine vulnerabilities found during the automated phase and manual phase, explore and integrate multiple attack vectors possible to prove existence of more complex and critical vulnerabilities in the target web application.

- **Database Vulnerabilities**

CAaNES security consultants detect databases that interact with target web applications and try to penetrate into respective back end databases by exploiting vulnerabilities existing in the database. Web application is used as interface while penetrating into the database. This goes beyond SQL injections performed by automated tools since CAaNES security consultants insert executable code to penetrate into back end database.

- **Security Misconfigurations**

CAaNES security consultants analyze and review the directory structure of a web application based on crawling results obtained during automated testing and virtual directory crawling. This testing stage is used to validate permissions assigned to directories and files within. Communication channels used by the web application are tested for encryption standards.

- **Automated Testing**

Automated testing is sometimes conducted concurrently with discovery. The automated testing process includes common, off-the-shelf tools, freeware and CAaNES-developed code. Several different scanners and tools are used to ensure that the maximum quantities of vulnerabilities are discovered and minimize the risk of oversights.

The automated testing process is routinely run in an iterative fashion, and each iteration expands upon previously discovered

issues. Automated testing is used to determine a baseline and to help the consultant locate potential threat vectors that may require additional manual testing. Automated testing features are highlighted in the chart on the next page.

Automated Testing Features		
Data Injection and Manipulation	Sessions and Authentication	Server and General HTTP
<ul style="list-style-type: none"> • Reflected Cross-Site Scripting (XSS) • Persistent XSS • Cross-site Request Forgery • SQL Injection • Blind SQL Injection • Buffer Overflows • Integer Overflows • Log Injection • Remote File Include Injection • Server Side Include (SSI) Injection • Operating System Command Injection • Local File Include (LFI) • Custom Fuzzing • Path Manipulation - Traversal • Path Truncation 	<ul style="list-style-type: none"> • Session Strength • Authentication Attacks • Insufficient Authentication • Insufficient Session Expiration • Brute Force Authentication Attacks • Support For CAPTCHA • Support for Single Sign-On • Support for Two Factor Authentication Mechanisms • Secure Sockets Layer (SSL) Certificate Issues • SSL Protocols Supported • SSL Ciphers Supported • Password Auto Complete • Cookie Security 	<ul style="list-style-type: none"> • Server Misconfigurations • Directory Indexing and Enumeration • Denial of Service • HTTP Response Splitting • Windows 8.3 File Name • DOS Device Handle DoS • Canonicalization Attacks • URL Redirection Attacks • Ajax Auditing • WebDAV Auditing • Web Services Auditing • File Enumeration • Information Disclosure • Directory and Path Traversal • Spam Gateway Detection • Known Application and Platform Vulnerabilities • Detects Dangerous HTTP

Manual Testing

The ever-changing landscape of technology makes automated scanners difficult to keep updated. Based on the output from the automated testing tools, CAaNES' consultants use their expertise to analyze all potential threats and to conduct proof-of-concept testing where appropriate.

To ensure that the deepest possible analysis is conducted on every engagement, our consultants execute numerous manual-testing processes. These processes use publicly available tools coupled with CAaNES-created code to identify as many issues as possible.

Manual Testing Features		
Data Injection and Manipulation	Sessions and Authentication	Server and General HTTP
<ul style="list-style-type: none"> • SQL injections • Blind SQL Injections • Translate Encoding Standards • Regex Editing • SOAP Editing • Web Fuzzing/Buffer overflow check 	<ul style="list-style-type: none"> • Brute Force authentication s • Cookie crunching 	<ul style="list-style-type: none"> • HTTP Request/Response monitoring • HTTP/HTTPS Requests Editing • Mapping applications to ports • Server Analysis

Common Tools

Application security assessments are very dynamic in nature and use a wide variety of tools. The following is a sample list of tools that are commonly used during this type of engagement. The specific demands of a test may necessitate additional tools or code to be created.

Application Security Assessment Tools		
• NTO Spider	• CAaNES - AppSploit	• Nessus - Web Plugins
• Acunetix	• Wikto	• NeXpose - Web Plugins
• Burp Suite	• Zap Proxy	• CAaNES - ORCA

7. Recommendations and Road Map to Achieve Baseline Security

After each individual test is performed, the team will provide a verbal summary of the security test performed. Every evening, all of work will be verbally summarized to the client. If a critical security issue is discovered, our team will immediately notify the client and work with them to mitigate risk.

At the completion of the assessment, the team provides a report containing summary and detailed information on the findings. The documentation covers the technical and business risk results of the performed tests, a high level executive overview of the findings, the recommendations of corrective actions and a detailed prioritization of those actions.

Additionally, CAaNES' consultants use this phase to discuss the activities performed during the assessment and all other relevant information as part of the knowledge transfer process. This process ensures that the client team has all the information they need to take action to remediate any discovered issues.

Information Generated

Our team provides a summary of the network topology, the top 5 most vulnerable machines on the network, top 5 most vulnerable segments of the network, a cyber-intelligence report that maps to the global information security trends, user privilege summary (users never logged on, users that have never changed passwords and users with weak passwords), a summary of default settings (SNMP, FTP, default user names and passwords on computing devices), a port protocol service summary, a summary of the top 25 most dangerous programming errors, and top 10 OWASP vulnerabilities.

Summary of Task Reports

After the engagement is complete, a formal presentation is given with the methodology, findings and recommendations. The full, formal, written report is provided after the presentation and includes an executive summary, web/applications report, system component report, general audit and compliance report, network assessment report and recommendations.

This scope of this project includes the delivery of two separate presentations of the findings for the following customer audiences:

- Information Technology Team
- Senior Management

Next Activities

The presentation and the detailed reports provide a prioritized list of the most critical issues and vulnerabilities that need to be addressed.

8. Preview of Assessment Results - RiskSense

CAaNES unique and proprietary security analytics and threat prioritization platform RiskSense will enhance threat analysis, provide risk prioritization, and perform live scoring of vulnerabilities with context.

RiskSense will empower AZ State to deal with the root cause, the vulnerabilities in their handling of complex IT security risks and compliance requirements across industries and sectors - a key component in risk management.

While not limiting to key assets, RiskSense can be applied to the entire organizational information technology infrastructure to immensely reduce the time involved in vulnerability management life cycle (from detection to remediation) from weeks to hours and minutes.

RiskSense: Single Pane of Glass to Optimize and Manage Security and Vulnerability Data.

RiskSense facilitates communication between all levels of an organization, from upper management to technicians, providing users with a holistic and succinct assessment of their security posture and risks.

Below are A few Exhibits from CAaNES Proprietary Framework RiskSense:

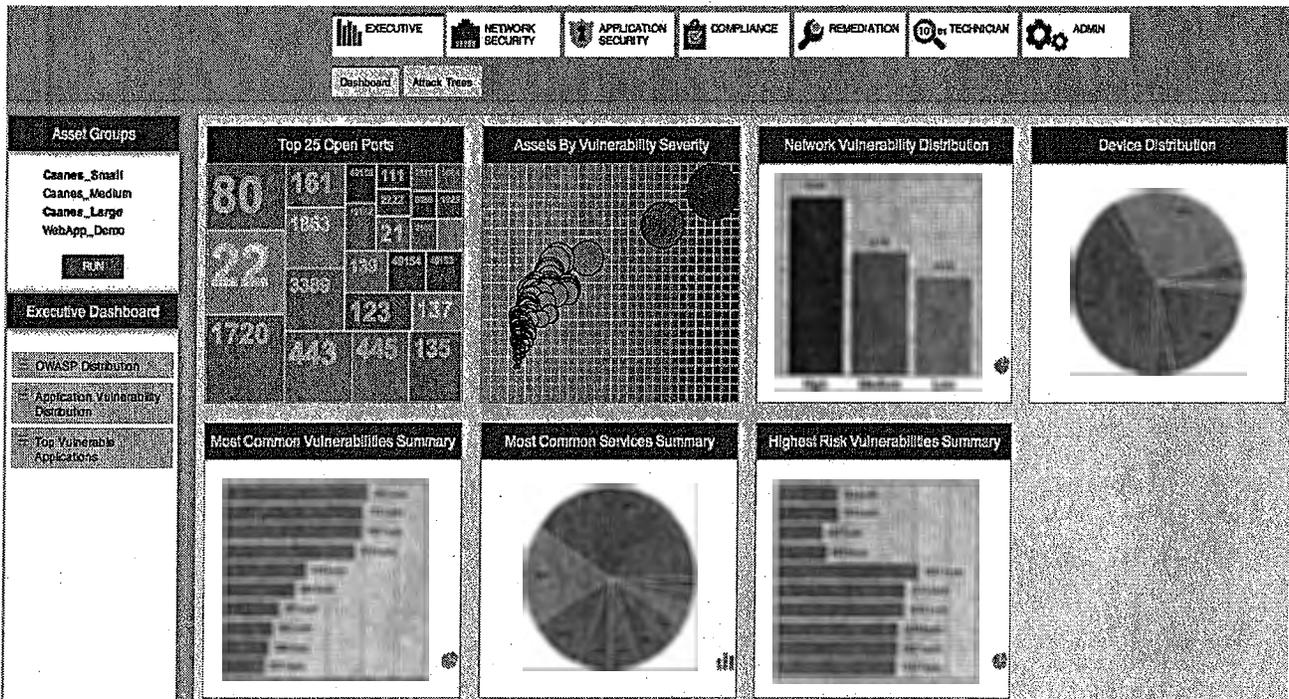


Exhibit 1: Summarizes Security Posture With a Heat Map – Most Vulnerable Ports – Asset View

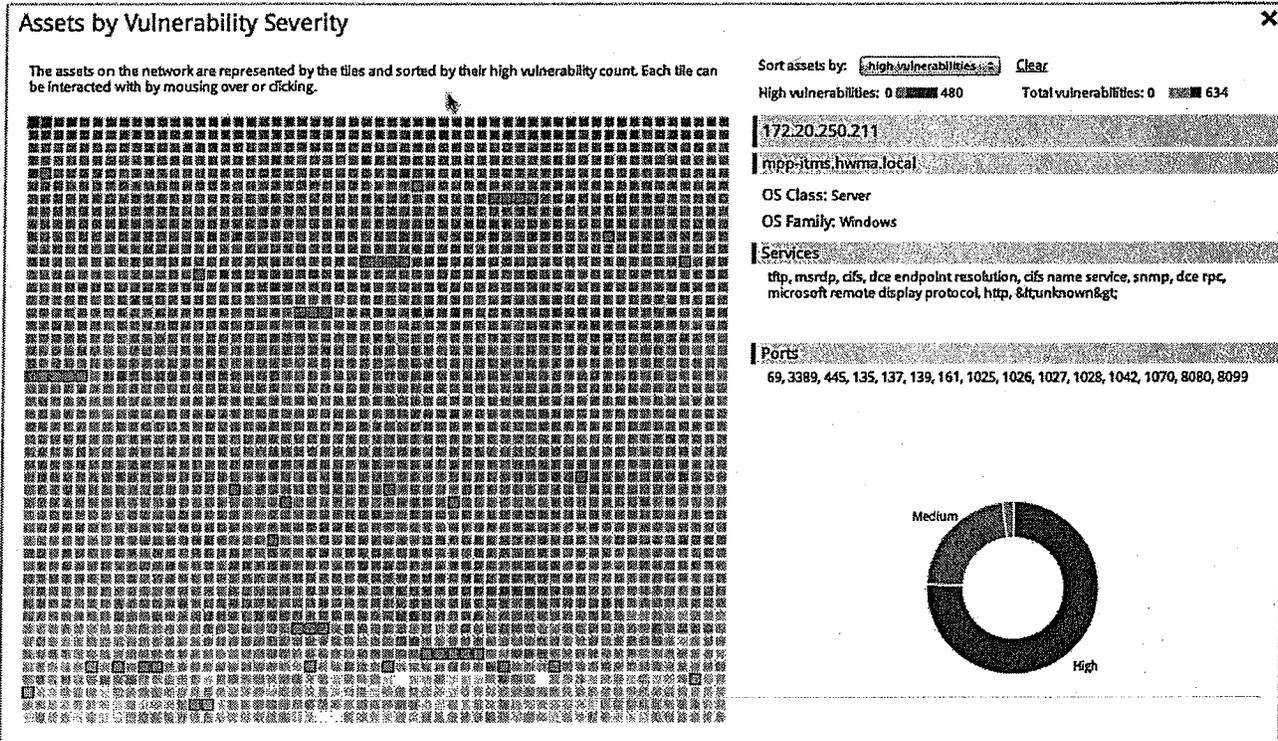


Exhibit: Asset Heat Map and Subnets With Most Vulnerabilities

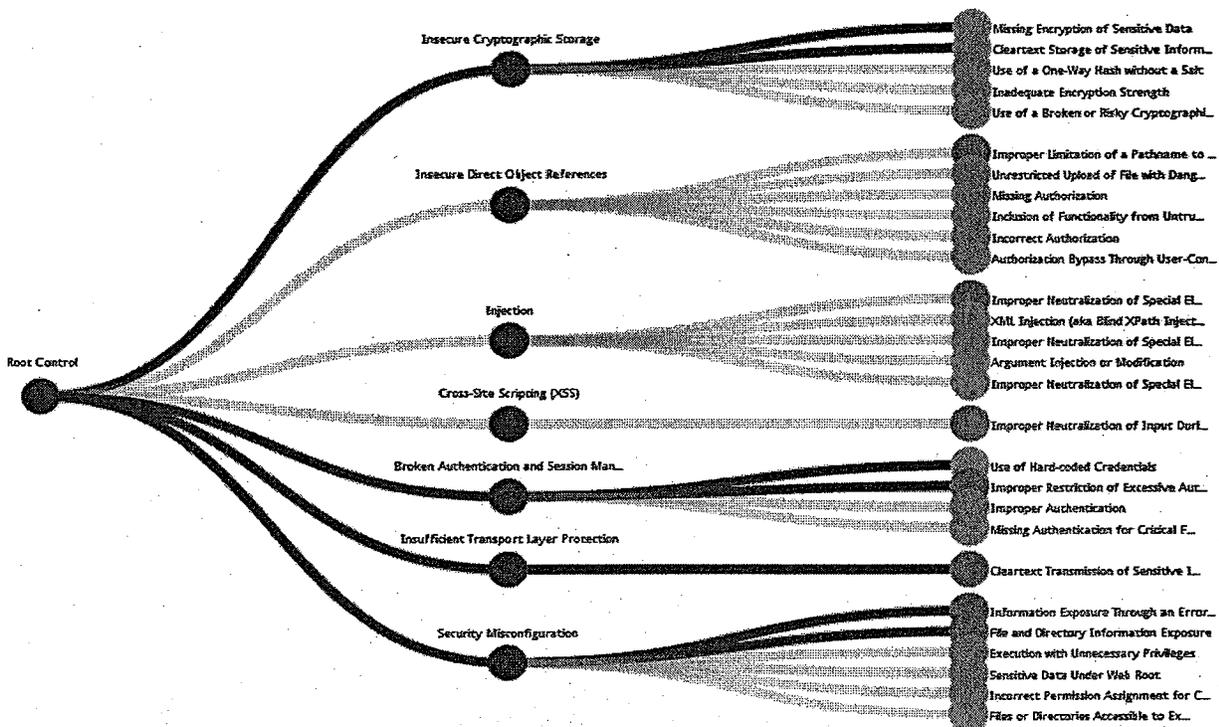


Exhibit: Web Application Vulnerabilities Mapped to Attack Paths - Attack Trees

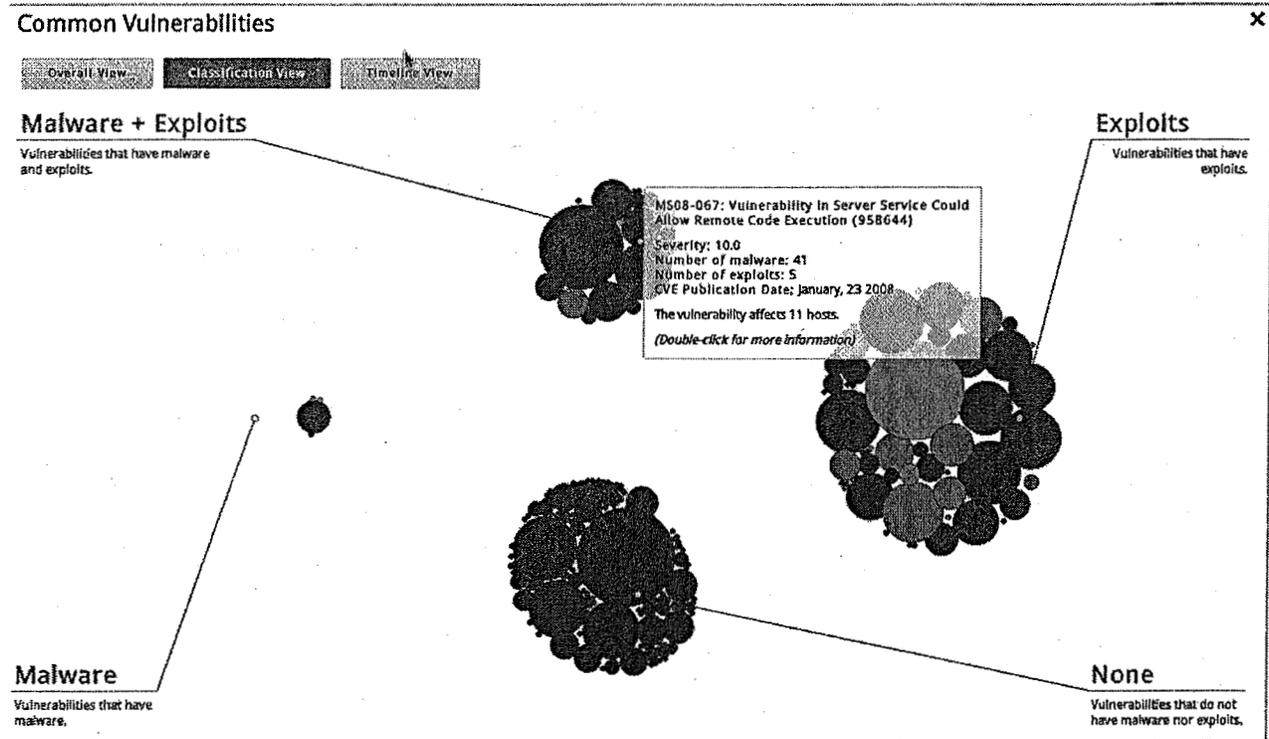


Exhibit: Contextual Intelligence - Vulnerabilities Mapped to Know Exploits and Malware

ID	Severity	Status	Title	CVSS	Exploit	Page	Source
10	10.0	Known	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	10.0	Yes	Yes	msrc.microsoft.com
11	10.0	Known	MS08-068: Vulnerability in Server Service Could Allow Remote Code Execution (958645)	10.0	Yes	Yes	msrc.microsoft.com
12	10.0	Known	MS08-069: Vulnerability in Server Service Could Allow Remote Code Execution (958646)	10.0	Yes	Yes	msrc.microsoft.com
13	10.0	Known	MS08-070: Vulnerability in Server Service Could Allow Remote Code Execution (958647)	10.0	Yes	Yes	msrc.microsoft.com
14	10.0	Known	MS08-071: Vulnerability in Server Service Could Allow Remote Code Execution (958648)	10.0	Yes	Yes	msrc.microsoft.com
15	10.0	Known	MS08-072: Vulnerability in Server Service Could Allow Remote Code Execution (958649)	10.0	Yes	Yes	msrc.microsoft.com
16	10.0	Known	MS08-073: Vulnerability in Server Service Could Allow Remote Code Execution (958650)	10.0	Yes	Yes	msrc.microsoft.com
17	10.0	Known	MS08-074: Vulnerability in Server Service Could Allow Remote Code Execution (958651)	10.0	Yes	Yes	msrc.microsoft.com
18	10.0	Known	MS08-075: Vulnerability in Server Service Could Allow Remote Code Execution (958652)	10.0	Yes	Yes	msrc.microsoft.com
19	10.0	Known	MS08-076: Vulnerability in Server Service Could Allow Remote Code Execution (958653)	10.0	Yes	Yes	msrc.microsoft.com
20	10.0	Known	MS08-077: Vulnerability in Server Service Could Allow Remote Code Execution (958654)	10.0	Yes	Yes	msrc.microsoft.com
21	10.0	Known	MS08-078: Vulnerability in Server Service Could Allow Remote Code Execution (958655)	10.0	Yes	Yes	msrc.microsoft.com
22	10.0	Known	MS08-079: Vulnerability in Server Service Could Allow Remote Code Execution (958656)	10.0	Yes	Yes	msrc.microsoft.com
23	10.0	Known	MS08-080: Vulnerability in Server Service Could Allow Remote Code Execution (958657)	10.0	Yes	Yes	msrc.microsoft.com
24	10.0	Known	MS08-081: Vulnerability in Server Service Could Allow Remote Code Execution (958658)	10.0	Yes	Yes	msrc.microsoft.com
25	10.0	Known	MS08-082: Vulnerability in Server Service Could Allow Remote Code Execution (958659)	10.0	Yes	Yes	msrc.microsoft.com
26	10.0	Known	MS08-083: Vulnerability in Server Service Could Allow Remote Code Execution (958660)	10.0	Yes	Yes	msrc.microsoft.com
27	10.0	Known	MS08-084: Vulnerability in Server Service Could Allow Remote Code Execution (958661)	10.0	Yes	Yes	msrc.microsoft.com
28	10.0	Known	MS08-085: Vulnerability in Server Service Could Allow Remote Code Execution (958662)	10.0	Yes	Yes	msrc.microsoft.com
29	10.0	Known	MS08-086: Vulnerability in Server Service Could Allow Remote Code Execution (958663)	10.0	Yes	Yes	msrc.microsoft.com
30	10.0	Known	MS08-087: Vulnerability in Server Service Could Allow Remote Code Execution (958664)	10.0	Yes	Yes	msrc.microsoft.com

Exhibit: Vulnerabilities Mapped to Know Exploits and Malware - List View

Common Vulnerabilities

x

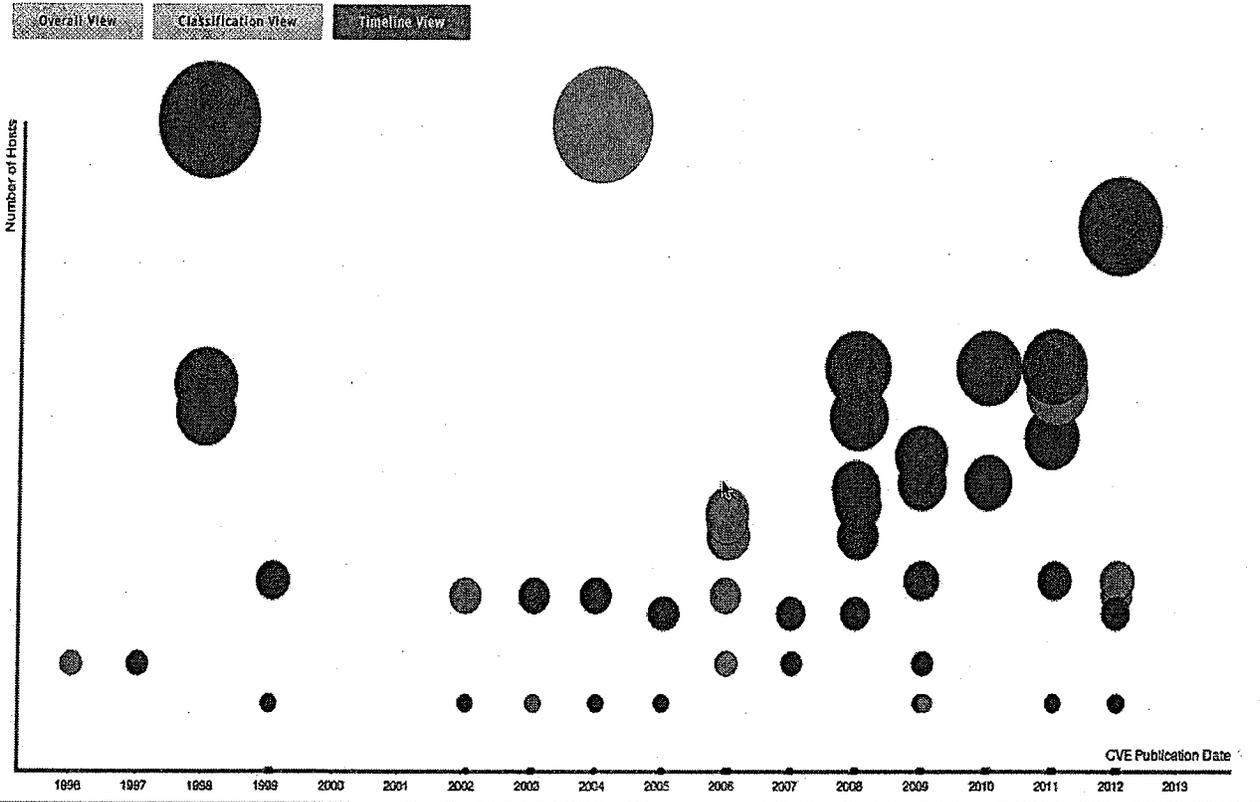


Exhibit: Insights to Develop Patterns: What's Working and What Not (CVE Aging)

ID	Severity	Status	Title	First	Type	Count
10	High	Fixed	Microsoft Exchange Server Remote Code Execution Vulnerability	10/20/2009	Exchange	1000
11	High	Fixed	Microsoft Exchange Server Remote Code Execution Vulnerability	10/20/2009	Exchange	1000
12	High	Fixed	Microsoft Exchange Server Remote Code Execution Vulnerability	10/20/2009	Exchange	1000
13	High	Fixed	Microsoft Exchange Server Remote Code Execution Vulnerability	10/20/2009	Exchange	1000
14	High	Fixed	Microsoft Exchange Server Remote Code Execution Vulnerability	10/20/2009	Exchange	1000
15	High	Fixed	Microsoft Exchange Server Remote Code Execution Vulnerability	10/20/2009	Exchange	1000
16	High	Fixed	Microsoft Exchange Server Remote Code Execution Vulnerability	10/20/2009	Exchange	1000
17	High	Fixed	Microsoft Exchange Server Remote Code Execution Vulnerability	10/20/2009	Exchange	1000
18	High	Fixed	Microsoft Exchange Server Remote Code Execution Vulnerability	10/20/2009	Exchange	1000
19	High	Fixed	Microsoft Exchange Server Remote Code Execution Vulnerability	10/20/2009	Exchange	1000
20	High	Fixed	Microsoft Exchange Server Remote Code Execution Vulnerability	10/20/2009	Exchange	1000
21	High	Fixed	Microsoft Exchange Server Remote Code Execution Vulnerability	10/20/2009	Exchange	1000
22	High	Fixed	Microsoft Exchange Server Remote Code Execution Vulnerability	10/20/2009	Exchange	1000
23	High	Fixed	Microsoft Exchange Server Remote Code Execution Vulnerability	10/20/2009	Exchange	1000
24	High	Fixed	Microsoft Exchange Server Remote Code Execution Vulnerability	10/20/2009	Exchange	1000
25	High	Fixed	Microsoft Exchange Server Remote Code Execution Vulnerability	10/20/2009	Exchange	1000

Exhibit: Remediation Report Mapped to Severity - Tools - Exploit - Malware Mapped

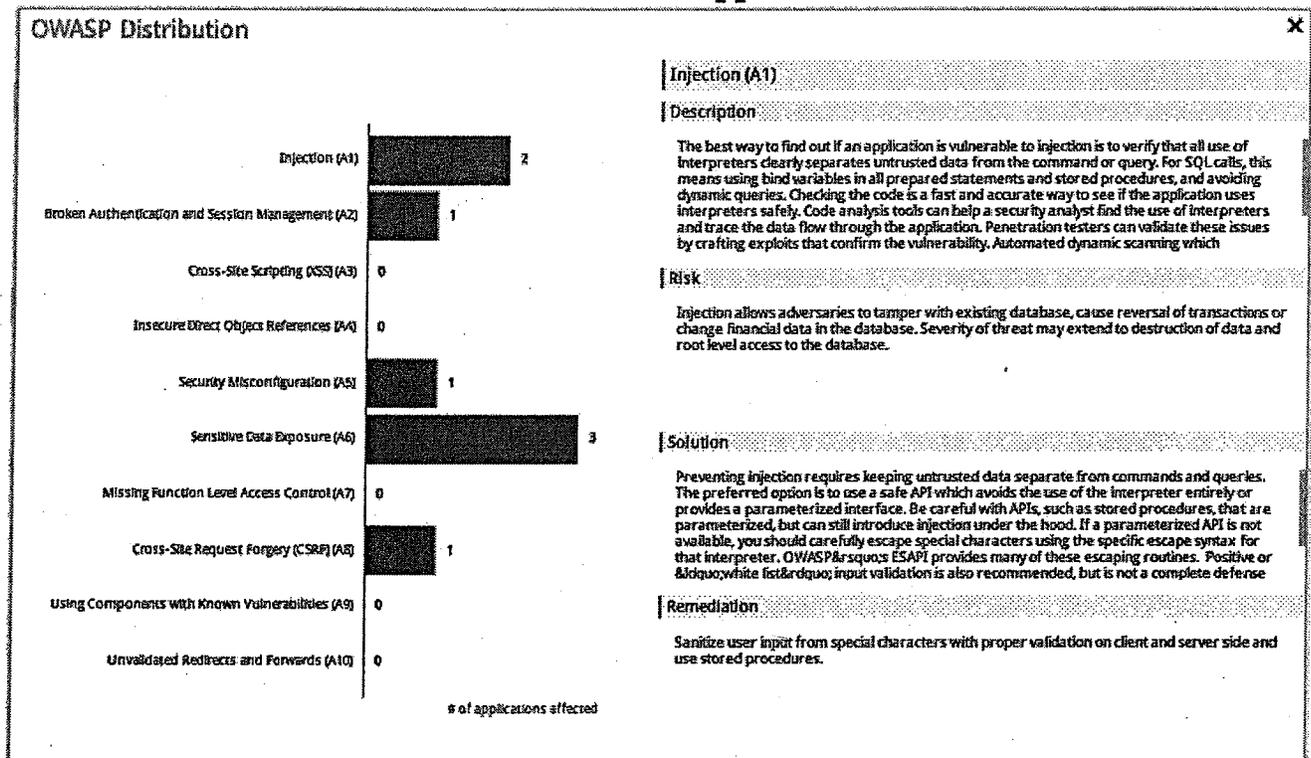


Exhibit: Web Application Security Posture Mapped to OWASP

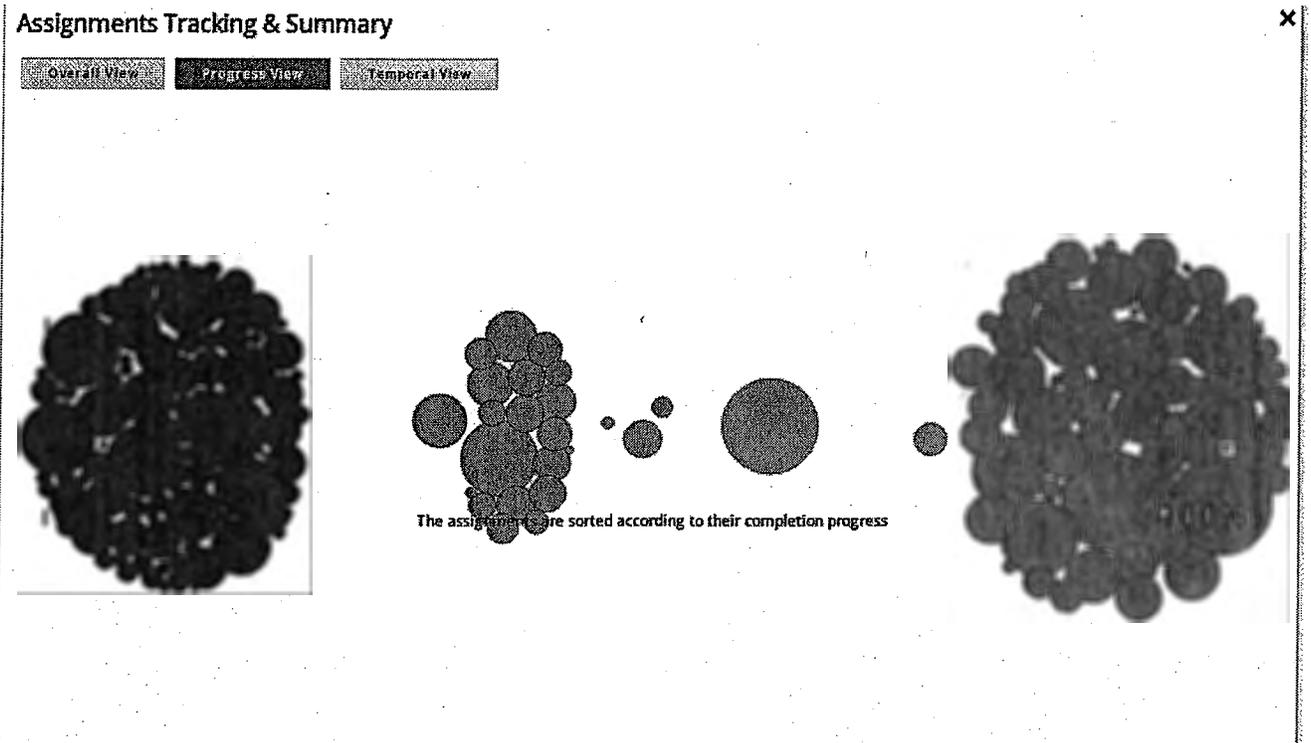


Exhibit: Remediation Tracking with Progress (Open Items, Pending Review, Remediated)

City of Santa Fe, New Mexico BUSINESS LICENSE



City Of Santa Fe
PO BOX 909
Santa Fe NM, 87504

Official Document
Please Post

Business Name: CAANES LLC

Location: LINCOLN AVE

Class: BUSINESS REGISTRATION-STANDARD PSA W/CTY

Comment:

Control Number: 0058823

License Number: 15-00102385

Issue Date November 06, 2014

Expiration Date December 31, 2015

CAANES LLC
7801 ACADEMY RD NE 1 STE 202

ALBUQUERQUE NM 87109

THIS IS NOT A CONSTRUCTION PERMIT OR SIGN PERMIT. APPROPRIATE PERMITS MUST BE OBTAINED FROM THE CITY OF SANTA FE BUILDING PERMIT DIVISION PRIOR TO COMMENCEMENT OF ANY CONSTRUCTION OR THE INSTALLATION OF ANY EXTERIOR SIGN.

THIS REGISTRATION/LICENSE IS NOT TRANSFERABLE TO OTHER BUSINESSES OR PREMISES.



City of Santa Fe Summary of Contracts, Agreements, & Amendments

Section to be completed by department for each contract or contract amendment

1 **FOR:** ORIGINAL CONTRACT or CONTRACT AMENDMENT

2 Name of Contractor Computational Analysis and Network Enterprise Solutions

3 Complete information requested Plus GRT

Inclusive of GRT

Original Contract Amount: \$55,000.00

Termination Date: June 30, 2015

Approved by Council Date: _____

or by City Manager Date: _____

Contract is for: Network security posture assessment & gap analysis

Amendment # _____ to the Original Contract# 13-1040

Increase/(Decrease) Amount \$ 38,070

Extend Termination Date to: June 30, 2014

Approved by Council Date: _____

or by City Manager Date: _____

Amendment is for: Network security posture assessment & gap analysis

4 **History of Contract & Amendments:** (option: attach spreadsheet if multiple amendments) Plus GRT

Inclusive of GRT

Amount \$ 25,000.00 of original Contract# 12-0432 Termination Date: 06/30/2012

Reason: _____

Amount \$ 20,000.00 amendment # 11-0241 Termination Date: 06/30/2011

Reason: _____

Amount \$ 20,000.00 amendment # 11-0058 Termination Date: 06/30/2011

Reason: _____

Amount \$ _____ amendment # _____ Termination Date: _____

Reason: _____

Total of Original Contract plus all amendments: \$ _____



City of Santa Fe
Summary of Contracts, Agreements, & Amendments

5 Procurement Method of Original Contract: (complete one of the lines)

RFP# _____ Date: _____

RFQ [] _____ Date: _____

Sole Source [] _____ Date: _____

Other Vendor initiated contact _____

6 Procurement History: _____
example: (First year of 4 year contract)

7 Funding Source: ITT Professional Services BU/Line Item: 12029.51034

8 Any out-of-the ordinary or unusual issues or concerns:
None
(Memo may be attached to explain detail.)

9 Staff Contact who completed this form: Yodel Catanach
Phone # 955-5575

10 Certificate of Insurance attached. (if original Contract) [x]

Submit to City Attorney for review/signature
Forward to Finance Director for review/signature
Return to originating Department for Committee(s) review or forward to City Manager for review
and approval (depending on dollar level).

To be recorded by City Clerk:

Contract # _____

Date of contract Executed (i.e., signed by all parties): _____

Note: If further information needs to be included, attach a separate memo.

Comments:

Large empty rectangular box for comments.

City of Santa Fe, New Mexico

BUDGET ADJUSTMENT REQUEST (BAR)

DEPARTMENT / DIVISION / SECTION / UNIT NAME				DATE	
ITT DEPARTMENT				01/23/2015	
ITEM DESCRIPTION	BU / LINE ITEM	<small>(Finance Dept Use Only)</small>		INCREASE	DECREASE
		SUBLEDGER / SUBSIDIARY	DR / (CR)		
Consulting	12029.510340			5,000	
Software Subscription	12029.530710			20,000	
Repair & Maint Furn/Fixture	12029.520300				25,000
TOTAL				\$ 25,000	\$ 25,000

JUSTIFICATION: (use additional page if needed)
 --Attach supporting documentation/memo

CAaNES PSA

<p><i>Yodel Catanach</i> 1/23/15 Prepared By Yodel Catanach Date</p> <p><i>Renée Martinez</i> 1/25/15 Department Director Renée Martinez Date</p>	<p>CITY COUNCIL APPROVAL</p> <p>City Council Approval Required <input type="checkbox"/></p> <p>City Council Approval Date <input type="text"/></p> <p>Agenda Item #: <input type="text"/></p>	<p><i>Carl Bruner</i> 1/23/15 Budget Officer Date</p> <p><i>[Signature]</i> 1-27-2015 Finance Director Date</p> <p>City Manager Date</p>
---	--	--

CITY OF SANTA FE
PROFESSIONAL SERVICES AGREEMENT

THIS AGREEMENT is made and entered into by and between the City of Santa Fe (the "City") and Computational Analysis and Network Enterprise Solutions (the "Contractor"). The date of this Agreement shall be the date when it is executed by the City.

1. SCOPE OF SERVICES

A. The Contractor shall provide the following services for the City:

- (1) Security Posture Assessment;
- (2) Progress Reporting Procedures;
- (3) Internal Infrastructure Assessment;
- (4) External Infrastructure Assessment;
- (5) Internal Environment Assessment;
- (6) Web & Application Security Posture Assessment;
- (7) Provide templates for Information Security Policies covering Risk Assessment & Disaster Recovery;
- (8) Resolve outstanding remediation tasks related to 2012 assessment.

B. The Contractor shall provide the following deliverables for the City:

- (1) Information security assessment plan;
- (2) Security assessment executive summary;
- (3) Security posture assessment approach;
- (4) Security posture assessment reports;

- (5) Snapshot of current information security posture;
- (6) Snapshot of current information security;
- (7) Penetration testing summary;
- (8) Web and application information security posture;
- (9) Configurations Review Summary;
- (10) Summary of Crucial Policies & Procedures;
- (11) Information security audit as per standard federal institutions guidelines and best practices;
- (12) Security Technical Implementation guides for Operating Systems and Network Devices;
- (13) Security Awareness, Identity Management, Social Networking, and Social Engineering Seminar;
- (14) Recommendations;
- (15) Two separate executive presentations to review all findings with the following audiences: Information Technology Team; Senior Management.
- (16) Provide drafts for an Information Security Policy, Risk Assessments, and Data Back-Up & Disaster Recovery

2. STANDARD OF PERFORMANCE; LICENSES

A. The Contractor represents that it possesses the personnel experience and knowledge necessary to perform the services described under this Agreement.

B. The Contractor agrees to obtain and maintain throughout the term

of this Agreement, all applicable professional and business licenses required by law, for itself, its employees, agents, representatives and subcontractors.

3. COMPENSATION

A. The City shall pay to the Contractor in full payment for services rendered, a sum not to exceed thirty eight thousand and seventy dollars (\$38,070.00), plus applicable gross receipts taxes and more particularly described in Exhibit "A" attached hereto and incorporated herein.

B. The Contractor shall be responsible for payment of gross receipts taxes levied by the State of New Mexico on the sums paid under this Agreement.

C. Payment shall be made upon receipt and approval by the City of detailed statements containing a report of services completed. Compensation shall be paid only for services actually performed and accepted by the City.

4. APPROPRIATIONS

The terms of this Agreement are contingent upon sufficient appropriations and authorization being made by the City for the performance of this Agreement. If sufficient appropriations and authorization are not made by the City, this Agreement shall terminate upon written notice being given by the City to the Contractor. The City's decision as to whether sufficient appropriations are available shall be accepted by the Contractor and shall be final.

5. TERM AND EFFECTIVE DATE

This Agreement shall be effective when signed by the City and terminate on June 30, 2014, unless sooner pursuant to Article 6 below.

6. TERMINATION

A. This Agreement may be terminated by the City upon 30 days written notice to the Contractor.

(1) The Contractor shall render a final report of the services performed up to the date of termination and shall turn over to the City original copies of all work product, research or papers prepared under this Agreement.

(2) Compensation is based upon hourly rates and expenses, therefore the Contractor shall be paid for services rendered and expenses incurred through the date Contractor receives notice of such termination.

7. STATUS OF CONTRACTOR; RESPONSIBILITY FOR PAYMENT OF EMPLOYEES AND SUBCONTRACTORS

A. The Contractor and its agents and employees are independent contractors performing professional services for the City and are not employees of the City. The Contractor, and its agents and employees, shall not accrue leave, retirement, insurance, bonding, use of City vehicles, or any other benefits afforded to employees of the City as a result of this Agreement.

B. Contractor shall be solely responsible for payment of wages, salaries and benefits to any and all employees or subcontractors retained by Contractor in the performance of the services under this Agreement.

C. The Contractor shall comply with City of Santa Fe Minimum Wage, Article 28-1-SFCC 1987, as well as any subsequent changes to such article throughout the term of this Agreement.

8. CONFIDENTIALITY

Any confidential information provided to or developed by the Contractor in the performance of this Agreement shall be kept confidential and shall not be made available to any individual or organization by the Contractor without the prior written approval of the City.

9. CONFLICT OF INTEREST

The Contractor warrants that it presently has no interest and shall not acquire any interest, direct or indirect, which would conflict in any manner or degree with the performance of services required under this Agreement. Contractor further agrees that in the performance of this Agreement no persons having any such interests shall be employed.

10. ASSIGNMENT; SUBCONTRACTING

The Contractor shall not assign or transfer any rights, privileges, obligations or other interest under this Agreement, including any claims for money due, without the prior written consent of the City. The Contractor shall not subcontract any portion of the services to be performed under this Agreement without the prior written approval of the City.

11. RELEASE

The Contractor, upon acceptance of final payment of the amount due under this Agreement, releases the City, its officers and employees, from all liabilities, claims and obligations whatsoever arising from or under this Agreement. The Contractor agrees not to purport to bind the City to any obligation not assumed herein by the City unless the

Contractor has express written authority to do so, and then only within the strict limits of that authority.

12. INSURANCE

A. The Contractor, at its own cost and expense, shall carry and maintain in full force and effect during the term of this Agreement, comprehensive general liability insurance covering bodily injury and property damage liability, in a form and with an insurance company acceptable to the City, with limits of coverage in the maximum amount which the City could be held liable under the New Mexico Tort Claims Act for each person injured and for each accident resulting in damage to property. Such insurance shall provide that the City is named as an additional insured and that the City is notified no less than 30 days in advance of cancellation for any reason. The Contractor shall furnish the City with a copy of a Certificate of Insurance or other evidence of Contractor's compliance with the provisions of this section as a condition prior to performing services under this Agreement.

B. Contractor shall also obtain and maintain Workers' Compensation insurance, required by law, to provide coverage for Contractor's employees throughout the term of this Agreement. Contractor shall provide the City with evidence of its compliance with such requirement.

C. Contractor shall maintain professional liability insurance throughout the term of this Agreement providing a minimum coverage the amount required under the New Mexico Tort Claims Act. The Contractor shall furnish the City with proof of insurance of Contractor's compliance with the provisions of this section as a condition prior to performing services under this Agreement.

13. INDEMNIFICATION

The Contractor shall indemnify, hold harmless and defend the City from all losses, damages, claims or judgments, including payments of all attorneys' fees and costs on account of any suit, judgment, execution, claim, action or demand whatsoever arising from Contractor's performance under this Agreement as well as the performance of Contractor's employees, agents, representatives and subcontractors.

14. NEW MEXICO TORT CLAIMS ACT

Any liability incurred by the City of Santa Fe in connection with this Agreement is subject to the immunities and limitations of the New Mexico Tort Claims Act, Section 41-4-1, et. seq. NMSA 1978, as amended. The City and its "public employees" as defined in the New Mexico Tort Claims Act, do not waive sovereign immunity, do not waive any defense and do not waive any limitation of liability pursuant to law. No provision in this Agreement modifies or waives any provision of the New Mexico Tort Claims Act.

15. THIRD PARTY BENEFICIARIES

By entering into this Agreement, the parties do not intend to create any right, title or interest in or for the benefit of any person other than the City and the Contractor. No person shall claim any right, title or interest under this Agreement or seek to enforce this Agreement as a third party beneficiary of this Agreement.

16. RECORDS AND AUDIT

The Contractor shall maintain, throughout the term of this Agreement and for a period of three years thereafter, detailed records that indicate the date, time and nature of services rendered. These records shall be subject to inspection by the City, the

Department of Finance and Administration, and the State Auditor. The City shall have the right to audit the billing both before and after payment. Payment under this Agreement shall not foreclose the right of the City to recover excessive or illegal payments.

17. APPLICABLE LAW; CHOICE OF LAW; VENUE

Contractor shall abide by all applicable federal and state laws and regulations, and all ordinances, rules and regulations of the City of Santa Fe. In any action, suit or legal dispute arising from this Agreement, the Contractor agrees that the laws of the State of New Mexico shall govern. The parties agree that any action or suit arising from this Agreement shall be commenced in a federal or state court of competent jurisdiction in New Mexico. Any action or suit commenced in the courts of the State of New Mexico shall be brought in the First Judicial District Court.

18. AMENDMENT

This Agreement shall not be altered, changed or modified except by an amendment in writing executed by the parties hereto.

19. SCOPE OF AGREEMENT

This Agreement incorporates all the agreements, covenants, and understandings between the parties hereto concerning the services to be performed hereunder, and all such agreements, covenants and understandings have been merged into this Agreement. This Agreement expresses the entire Agreement and understanding between the parties with respect to said services. No prior agreement or understanding, verbal or otherwise, of the parties or their agents shall be valid or enforceable unless embodied in this Agreement.

20. NON-DISCRIMINATION

During the term of this Agreement, Contractor shall not discriminate against any employee or applicant for an employment position to be used in the performance of services by Contractor hereunder, on the basis of ethnicity, race, age, religion, creed, color, national origin, ancestry, sex, gender, sexual orientation, physical or mental disability, medical condition, or citizenship status.

21. SEVERABILITY

In case any one or more of the provisions contained in this Agreement or any application thereof shall be invalid, illegal or unenforceable in any respect, the validity, legality, and enforceability of the remaining provisions contained herein and any other application thereof shall not in any way be affected or impaired thereby.

22. NOTICES

Any notices required to be given under this Agreement shall be in writing and served by personal delivery or by mail, postage prepaid, to the parties at the following addresses:

City of Santa Fe:
200 Lincoln Ave.
Santa Fe, NM 87501

Contractor: CAaNES
7801 Academy Rd, NE
Albuquerque, NM 87113

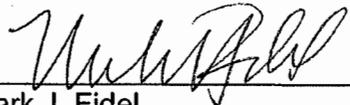
IN WITNESS WHEREOF, the parties have executed this Agreement on the dates set forth below.

CITY OF SANTA FE:

CONTRACTOR:
CAaNES



BRIAN K. SNYDER, CITY MANAGER



Mark J. Fidel

DATE: 9-30-13

DATE: 13 Oct 2013

ATTEST:

NM Taxation & Revenue
CRS#0307951800
City of Santa Fe Business
Registration #13-00102385



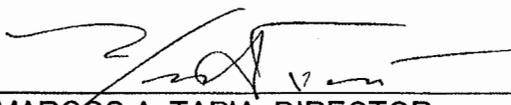
YOLANDA VIGIL, CITY CLERK

APPROVED AS TO FORM:



GENO ZAMORA, CITY ATTORNEY 8/5/13

APPROVED:



MARCOS A. TAPIA, DIRECTOR
FINANCE DEPARTMENT 9/26/13

12029.510300
BU/LI



CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)
07/18/13

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

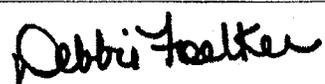
PRODUCER Walker Agency 1501 San Juan Blvd Ste 201 Farmington, NM 87401 Phone (505) 326-4952 Fax (505) 326-5027		CONTACT NAME: Debbie Foelker PHONE (A/C, No, Ext): (505) 326-4952 FAX (A/C, No): (505) 326-5027 E-MAIL ADDRESS: dfoelker@diglii.net	
INSURED CAANES,LLC 7801 Academy NE Bldg 1 Ste 202 Albuquerque, NM 87109		INSURER(S) AFFORDING COVERAGE INSURER A: The Hartford Insurance Company INSURER B: CNA surety INSURER C: INSURER D: INSURER E: INSURER F:	

COVERAGES	CERTIFICATE NUMBER:	REVISION NUMBER:
------------------	----------------------------	-------------------------

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSR	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	GENERAL LIABILITY <input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> <input type="checkbox"/> GEN'L AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC	Y	N	34SBAPK1653	07/28/2013	07/28/2014	EACH OCCURRENCE \$ 2,000,000.00 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 1,000,000.00 MED EXP (Any one person) \$ 5,000.00 PERSONAL & ADV INJURY \$ 2,000,000.00 GENERAL AGGREGATE \$ 4,000,000.00 PRODUCTS - COMPROP AGG \$ 4,000,000.00 \$
B	AUTOMOBILE LIABILITY <input type="checkbox"/> ANY AUTO <input type="checkbox"/> ALL OWNED AUTOS <input type="checkbox"/> SCHEDULED AUTOS <input checked="" type="checkbox"/> HIRED AUTOS <input checked="" type="checkbox"/> NON-OWNED AUTOS <input type="checkbox"/>	Y	N	34SBAPK1653	07/28/2013	07/28/2014	COMBINED SINGLE LIMIT (Ea accident) \$ 2,000,000.00 BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$ \$
A	<input type="checkbox"/> UMBRELLA LIAB <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE <input type="checkbox"/> DED <input type="checkbox"/> RETENTION \$	Y	N	34SBAPK1653	07/28/2013	07/28/2014	EACH OCCURRENCE \$ 3,000,000.00 AGGREGATE \$ 3,000,000.00 \$
A	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) <input type="checkbox"/> Y / N If yes, describe under DESCRIPTION OF OPERATIONS below	N/A	N/A	34WECEBF5488	07/28/2013	07/28/2014	<input type="checkbox"/> WC STATU-TORY LIMITS <input type="checkbox"/> OTH-ER E.L. EACH ACCIDENT \$ 1,000,000.00 E.L. DISEASE - EA EMPLOYE \$ 1,000,000.00 E.L. DISEASE - POLICY LIMIT \$ 1,000,000.00
B	Bond			16061986	12/17/2013	12/17/2014	100000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (Attach ACORD 101, Additional Remarks Schedule, if more space is required)

CERTIFICATE HOLDER	CANCELLATION
City of Santa Fe PO Box 909 Santa Fe, NM 87504-0909	SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS. AUTHORIZED REPRESENTATIVE 

City of Santa Fe, New Mexico

memo

DATE: August 27, 2013

TO: Brian Snyder, City Manager

FROM: Thomas J. Williams, ITT Division Director *TJW*

VIA: Marcos Tapia, Finance Director *[Signature]*

VIA: Robert Rodarte, Purchasing Director *[Signature]*

ISSUE: CAaNES Professional Services Agreement – Information Security Posture Assessment

SUMMARY:

I request approval of the attached PSA with CAaNES, LLC to conduct an Information Security Posture Assessment on the city's network and application systems infrastructure.

The scope of the engagement will include an analysis of existing security policies, procedures and processes. It will also include a regulatory compliance assessment and risk assessment, and recommendations to achieve baseline security based on best business practices and regulatory requirements. The following are some of the key deliverables outlined in the PSA:

- Information Security Assessment Plan
- Security Assessment Executive Summary
- Security Posture Assessment Reports
- Penetration Testing Summary
- Executive Presentation of Findings to Senior Management
- Formal Recommendations
- Draft Information Security, Risk Assessment, & Data Back-Up Policies
- Draft Disaster Recovery Plan

The cost of this PSA is \$38,070 and will be charged to 12029.510300. The price is per SPD Contract# 10-000-00-00051AI (attached).

Legal has reviewed, approved and signed the PSA, and Purchasing has approved and reviewed the SPD Contract.

ACTION:

Request approval of Gartner Inc. Professional Services Agreement



State of New Mexico
General Services Department
Purchasing Division

Statewide Price Agreement Amendment

Awarded Vendor
000063360
CAaNES, LLC
7801 Academy Rd NE Ste. 1-202
Albuquerque, NM 87109

Telephone No. (505) 217-9422

Price Agreement Number: 10-000-00-00051A1

Price Agreement Amendment No.: Two

Term: July 1, 2011 – March 30, 2014

Ship To:
All State of New Mexico agencies, commissions,
institutions, political subdivisions and local public
bodies allowed by law.

Procurement Specialist: India Garcia

Telephone No.: (505) 827-0483

Invoice:
As Requested

Title: IT Professional Services

This Price Agreement Amendment is to be attached to the respective Price Agreement and become a part thereof.

In accordance with Price Agreement provisions, and by mutual agreement of all parties, this Price Agreement is extended from June 1, 2013 to March 30, 2014 at the same price, terms and conditions.

Except as modified by this amendment, the provisions of the Price Agreement shall remain in full force and effect.

Accepted for the State of New Mexico

New Mexico State Purchasing Agent

Date: 2/18/13

Purchasing Division, 1100 St. Francis Drive 87505, PO Box 6850, Santa Fe, NM 87502-6850 (505) 827-0472

AM
[Handwritten initials]



State of New Mexico
General Services Department

Statewide Price Agreement

Awarded Vendor
0000063360
CAaNES, LLC
10200 Comanche Drive NE
Albuquerque, NM 87111

Telephone No. 505-217-9422

Price Agreement Number: 10-000-00-00051A1

Payment Terms: Per Contract

F.O.B.: Per Contract

Delivery: Per Contract

Ship To:
All State of New Mexico agencies, commissions,
institutions, political subdivisions and local public bodies
allowed by law.

Procurement Specialist: Gerrie Becker

Telephone No.: 505-476-3121

Invoice:
As Requested

Title: IT Professional Services

MARCH 2015

Term: July 1, 2011 thru March 30, 2012

This Price Agreement is made subject to the "terms and conditions" shown on the reverse side of this page, and as indicated in this Price Agreement.

Accepted for the State of New Mexico



New Mexico State Purchasing Agent

Date: 6/21/11

Purchasing Division, 1100 St. Francis Drive, PO Box 6850, Santa Fe, NM 87502-6850 (505) 827-0472

CM

**State of New Mexico
Information Technology**

Price Agreement

Price Agreement No. 10-000-00-00051A1

THIS Information Technology Price Agreement ("Agreement") is made by and between the State of New Mexico, State Purchasing Division, hereinafter referred to as the "Agency" and CAaNES, LLC, hereinafter referred to as the "Contractor" and collectively referred to as the "Parties".

WHEREAS, pursuant to the Procurement Code, NMSA 1978 13-1-28 *et. seq.*; and Procurement Code Regulations, NMAC 1.4.1 *et. seq.*; the Contractor has held itself out as expert in implementing the Scope of Work as contained herein and the Agency has selected the Contractor as the Offeror most advantageous to the State of New Mexico; and

WHEREAS, all terms and conditions of this Agreement, the Contractor's proposal, including any best and final offers, and the RFP are hereby incorporated by reference in this contract. In the event of a conflict between these items, the conflict will be resolved by giving priority in the following order:

1. All federal and New Mexico laws, rules and regulations regarding services within the Contractor's scope of work.
2. This Agreement and any written amendments to this Agreement.
3. The Request for Proposal (RFP), all RFP amendments, written clarifications to the RFP, and written answers to written questions concerning the RFP.
4. Contractor's Best and Final Offer
5. Contractor's Proposal.

ARTICLE 1 – DEFINITIONS

- A. "Acceptance" shall mean the approval, after Quality Assurance, of all Deliverables by an executive level representative ("Executive Level Representative") of the Agency.
- B. "Change Request" shall mean the document utilized to request changes or revisions in the Scope of Work.
- C. "Chief Information Officer ("CIO")" shall mean the Secretary of the Department of Information Technology for the State of New Mexico or designated representative.
- D. "Deliverable" shall mean any verifiable outcome, result, service or product that must be delivered, developed, performed or produced by the Contractor as defined by the Scope of Work.
- E. "DoIT" shall mean the Department of Information Technology.
- F. "DFA" shall mean the Department of Finance and Administration; "DFA/CRB" shall mean the Department of Finance and Administration, Contracts Review Bureau.
- G. "Escrow" shall mean a legal document (such as the software source code) delivered by the contractor into the hands of a third party, to be held by that party until the performance of a condition is accepted; in the event contractor fails to perform, the grantee agency receives the legal document, in this case, source code.

H. "Enhancement" means any modification or addition that, when made or added to the program, materially changes its or their utility, efficiency, functional capability, or application, but does not constitute solely an Error Correction. After conferring with Agency, an Enhancement may be identified as minor or major.

I. "Know How" shall mean all technical information, data and knowledge including, but not limited to, all documents, computer storage devices, drawings, flow charts, plans, proposals, records, notes, memoranda, manuals and other tangible items containing, relating or causing the enablement of any Intellectual Property developed under this Agreement.

J. "Intellectual Property" shall mean any and all proprietary information developed pursuant to the terms of this Agreement.

K. "Independent Verification and Validation ("IV&V")" shall mean the process of evaluating a project and the project's product to determine compliance with specified requirements and the process of determining whether the products of a given development phase fulfill the requirements established during the previous stage, both of which are performed by an entity independent of the Agency.

L. "Payment Invoice" shall mean a detailed, certified and written request for payment of services rendered from the Contractor to the Agency. Payment Invoice(s) must contain the fixed price Deliverable cost and identify the Deliverable for which the invoice is submitted.

M. "Performance Bond" shall mean a surety bond which guarantees that the contractor will fully perform the contract and guarantees against breach of contract.

N. "Project" shall mean a temporary process undertaken to solve a well-defined goal or objective with clearly defined start and end times, a set of clearly defined tasks, and a budget. The project terminates once the project scope is achieved and project approval is given by the Executive Level Representative and verified by the agency CIO to the DoIT.

O. "Project Manager" shall mean a qualified person from the Agency responsible for all aspects of the Project

P. "Quality Assurance" shall mean a planned and systematic pattern of all actions necessary to provide adequate confidence that a Deliverable conforms to established requirements, customer needs, and user expectations.

Q. "State Purchasing Agent (SPA)" - shall mean the State Purchasing Agent for the State of New Mexico or designated representative.

R. "State Purchasing Division (SPD)" - shall mean the State Purchasing Division of the General Services Department for the State of New Mexico

ARTICLE 2 - SCOPE OF WORK

A. Scope of Work. The Contractor shall provide information technology services to the Procuring Agency in accordance with the completed IT Professional Services Contract and the terms and conditions of the price agreement at the rate shown in Exhibit A.

B. Performance Measures. In addition, each IT Professional Services Contract will become a part of the agreement. In the event of any conflict among these documents, the following order of precedence shall apply:

- 1) The terms and conditions of this document;
- 2) The completed Contract/Purchase Order;
- 3) The request for proposals document; and
- 4) The contractor's written proposal including the Best and Final Offer, if one was submitted.

C. This is not an exclusive Price Agreement. Procuring Agencies may obtain services from other sources during the Price Agreement term. The SPA makes no expressed or implied warranties whatsoever that any particular number of Purchase Orders will be issued or that any particular quantity or dollar amount of services will be procured.

ARTICLE 3 - COMPENSATION

All payments under this Price Agreement are subject to the following provisions:

a. Acceptance - In accordance with Section 13-1-158 NMSA 1978, Project Manager shall determine if the services provided meet Purchase Order specifications contained therein. No payment shall be made for any service until the services have been accepted in writing by the Project Manager. Unless otherwise agreed upon between Procuring Agency and the Contractor, within fifteen (15) days from the date the Project Manager receives written notice (Contractor's Invoice) from the Contractor that payment is requested for services, the Project Manager shall issue a written certification to the Contractor of complete or partial acceptance or rejection of the services.

b. Rejection - Unless the Executive Level Representative gives notice of rejection within the fifteen (15) day business day Acceptance period, the Deliverable will be deemed to have been accepted. If the Deliverable is deemed unacceptable under Quality Assurance, fifteen (15) days from the date the Executive Level Representative receives the Deliverable(s) and accompanying Payment Invoice, the Executive Level Representative will send a consolidated set of comments indicating issues, unacceptable items, and/or requested revisions accompanying the rejection. Upon rejection and receipt of comments, the Contractor will have ten (10) business days to resubmit the Deliverable to the Executive Level Representative with all appropriate corrections or modifications made and/or addressed. The Executive Level Representative will again determine whether the Deliverable(s) is Acceptable under Quality Assurance and provide a written determination within fifteen (15) business days of receipt of the revised or amended Deliverable. If the Deliverable is once again deemed unacceptable under Quality Assurance and thus rejected, the Contractor will be required to provide a remediation plan that shall include a timeline for corrective action acceptable to the Executive Level Representative. The Contractor shall also be subject to all damages and remedies attributable to the late delivery of the Deliverable under the terms of this Agreement and available at law or equity. In the event that a Deliverable must be resubmitted more than twice for Acceptance, the Contractor shall be deemed as in breach of this Agreement. The

Agency may seek any and all damages and remedies available under the terms of this Agreement and available at law or equity. Additionally, the Agency may terminate this Agreement.

c. Compensation - The approved maximum rates to be paid for services rendered are contained in the Services Schedule. The Procuring Agency may reimburse Contractor for reasonable travel/per diem expenses for work performed at distances greater than 100 miles from the Contractor's primary place of business in New Mexico. The conditions for travel, the type and amount expenses to be reimbursed shall be stated in the Procuring Agency Agreement. Travel time from the Contractor's primary place of business and the worksite is not billable.

d. Payment of Invoice - Payment will be made to the Contractor's designated mailing address.

e. Payment of Taxes - The Contractor shall be reimbursed by the Procuring Agency for applicable New Mexico gross receipts taxes or local option taxes for services rendered. Such taxes must be itemized separately on the invoice.

The payment of taxes for any money received under this Price Agreement shall be the Contractor's sole responsibility and shall be reported under the Contractor's Federal and State tax identification number(s).

f. Invoices - Invoices shall be submitted to the Project Manager.

g. Facilities and Equipment - The Procuring Agency shall provide contractor personnel with reasonable office work space and facilities including access to a local telephone service, copy machine usage and office supplies. Unless otherwise stated in the Procuring Agency Agreement, the contractor shall provide contractor personnel with any required personal computer equipment and software and shall reimburse the procuring agencies for all long distance telephone calls charged to the Procuring Agency.

h. Appropriations - The terms of this Price Agreement and any Purchase Orders are contingent upon sufficient appropriations and authorization being made by the Legislature of New Mexico or other appropriate governing bodies for performance pursuant to this Price Agreement. Notwithstanding any language to the contrary in this Price Agreement or in any Purchase Order or other document, a Procuring Agency may terminate its obligation under a Purchase Order, or any extension thereof, if sufficient appropriations and authorization are not made by the Legislature or other appropriate governing body to pay amounts due. The Procuring Agency's decision as to whether sufficient appropriations are available shall be accepted by the Contractor and shall be final and binding. However, Procuring Agencies agree not to use insufficient appropriations as a means of terminating a Purchase Order in order to acquire functionally equivalent services from a third party.

i. Release - The Contractor, upon final payment of the amount due under a Purchase Order, releases the State of New Mexico, and its agencies and public employees, from all liabilities, claims and obligations whatsoever arising from or under this Price Agreement. The Contractor agrees not to purport to bind the State of New Mexico to any obligation not assumed herein by the State of New Mexico, unless the Contractor has express written authority to do so, and then only within the strict limits of that authority.

ARTICLE 4 - TERM

The initial term of this Price Agreement shall be March 31, 2011 or as soon as possible thereafter, through March 30, 2012.

The SPA may extend the initial term of the Price Agreement for three (3) additional one-year terms, or portions thereof, by giving the Contractor a written offer to renew the agreement at least thirty (30) days prior to the expiration of the then-current term. Service rates can change each year at the time of renewal if exercised, any proposed increase in the maximum rates for each authorized service shall not exceed the lower of the increase in the published Consumer Price Index (or other index approved by the Agreement Administrator) during the previous agreement term or the percentage increase in the Contractor's published consultant rates.

Except as noted elsewhere in this paragraph, the SPA expects all terms and conditions of this Price Agreement to apply to any option terms exercised. No changes to terms and conditions shall be effective unless reduced to written amendment in accordance with Paragraph 15 of this Price Agreement.

ARTICLE 5 – TERMINATION

This Agreement may be terminated as follows:

A. General. By either Party upon written notice to be delivered to the other party not less than thirty (30) business days prior to the intended date of termination.

C. Obligations and Waiver. By termination pursuant to this Article, neither party may nullify obligations already incurred for performance or failure to perform prior to the date of termination. THIS ARTICLE IS NOT EXCLUSIVE AND DOES NOT CONSTITUTE A WAIVER OF ANY OTHER LEGAL RIGHTS AND REMEDIES AFFORDED THE AGENCY AND THE STATE OF NEW MEXICO CAUSED BY THE CONTRACTOR'S DEFAULT OR BREACH OF THIS AGREEMENT.

ARTICLE 6 – TERMINATION MANAGEMENT

A. Contractor. In the event this Agreement is terminated for any reason, or upon expiration, and in addition to all other rights to property set forth in this Agreement, the Contractor shall:

- 1.) Transfer, deliver, and/or make readily available to the Agency property in which the Agency has a financial interest and any and all data, Know How, Intellectual Property, inventions or property of the Agency.
- 2.) Incur no further financial obligations for materials, services, or facilities under the Agreement without prior written approval of the Agency;
- 3.) Terminate all purchase orders or procurements and any subcontractors and cease all work, except as the Agency may direct, for orderly completion and transition;
- 4.) Take such action as the Agency may direct, for the protection and preservation of all property and all records related to and required by this Agreement;
- 5.) Agree that the Agency is not liable for any costs arising out of termination and that the Agency is liable only for costs of Deliverables Accepted prior to the termination of the Agreement;
- 6.) Cooperate fully in the closeout or transition of any activities to permit continuity in the administration of Agency programs;
- 7.) In the event that this Agreement is terminated due to the Contractor's course of performance, negligence or willful misconduct and that course of performance, negligence, or willful misconduct results in reductions in the Agency's receipt of program funds from any governmental agency, the Contractor shall remit to the Agency the full amount of the reduction.

8.) Should this Agreement terminate due to the Contractor's default, the Contractor shall reimburse the Agency for all costs arising from hiring new contractor/subcontractors at potentially higher rates and for other costs incurred.

9.) In the event this Agreement is terminated for any reason, or upon its expiration, the Contractor shall assist and cooperate with the Agency in the orderly and timely transfer of files, computer software, documentation, system turnover plan, Know How, Intellectual Property and other materials, whether provided by the Agency or created by the Contractor under this Agreement, to the Agency, including but not limited to, user manuals with complete documentation, functional technical descriptions of each program and data flow diagrams. At the request of the Project Manager, the Contractor shall provide to the Agency a copy of the most recent versions of all files, software, Know How, Intellectual Property and documentation, whether provided by the Agency or created by the Contractor under this Agreement.

B. Agency. In the event this Agreement is terminated for any reason, or upon expiration, and in addition to all other rights to property set forth in this Agreement, the Agency shall 1) Retain ownership of all work products and documentation created pursuant to this Agreement; and 2) Pay the Contractor all amounts due for services Accepted prior to the effective date of such termination or expiration.

ARTICLE 7 – INDEMNIFICATION

A. General. The Contractor shall defend, indemnify and hold harmless the Agency, the State of New Mexico and its employees from all actions, proceedings, claims, demands, costs, damages, attorneys' fees and all other liabilities and expenses of any kind from any source which may arise out of the performance of this Agreement, caused by the negligent act or failure to act of the Contractor, its officers, employees, servants, subcontractors or agents, or if caused by the actions of any client of the Contractor resulting in injury or damage to persons or property during the time when the Contractor or any officer, agent, employee, servant or subcontractor thereof has or is performing services pursuant to this Agreement. In the event that any action, suit or proceeding related to the services performed by the Contractor or any officer, agent, employee, servant or subcontractor under this Agreement is brought against the Contractor, the Contractor shall, as soon as practicable, but no later than two (2) days after it receives notice thereof, notify, by certified mail, the legal counsel of the Agency, and the Risk Management Division of the New Mexico General Services Department.

B. The indemnification obligation under this Agreement shall not be limited by the existence of any insurance policy or by any limitation on the amount or type of damages, compensation or benefits payable by or for Contractor or any subcontractor, and shall survive the termination of this Agreement. Money due or to become due to the Contractor under this Agreement may be retained by the Agency, as necessary, to satisfy any outstanding claim that the Agency may have against the Contractor.

ARTICLE 8 – INTELLECTUAL PROPERTY

A. Product of Services: Copyright. All materials developed or acquired by the Contractor under this Price Agreement shall become the property of the Procuring Agency. Nothing produced, in whole or in part, by the Contractor under this Price Agreement shall be the subject of an application for copyright by or on behalf of the Contractor. The original and one copy of all materials, work papers, design documents, or other documents produced by the Contractor shall be indexed and placed in appropriately labeled binders and delivered to the Project Manager at the conclusion of a Purchase Order.

ARTICLE 9 – INTELLECTUAL PROPERTY INDEMNIFICATION

A. Intellectual Property Indemnification. The Contractor shall defend, at its own expense, the Agency, the State of New Mexico and/or any other State of New Mexico body against any claim that any product or service provided under this Agreement infringes any patent, copyright or trademark, and shall pay all costs, damages and attorney's fees that may be awarded as a result of such claim. In addition, if any third party obtains a judgment against the Agency based upon Contractor's trade secret infringement relating to any product or services provided under this Agreement, the Contractor agrees to reimburse the Agency for all costs, attorneys' fees and the amount of the judgment. To qualify for such defense and/or payment, the Agency shall:

- 1.) Give the Contractor written notice, within forty-eight (48) hours, of its notification of any claim;
- 2.) Allow the Contractor to control the defense and settlement of the claim; and
- 3.) Cooperate with the Contractor, in a reasonable manner, to facilitate the defense or settlement of the claim.

B. Agency Rights. If any product or service becomes, or in the Contractor's opinion is likely to become, the subject of a claim of infringement, the Contractor shall, at its sole expense:

- 1.) Provide the Agency the right to continue using the product or service and fully indemnify the Agency against all claims that may arise out of the Agency's use of the product or service;
- 2.) Replace or modify the product or service so that it becomes non-infringing; or
- 3.) Accept the return of the product or service and refund an amount equal to the value of the returned product or service, less the unpaid portion of the purchase price and any other amounts, which are due to the Contractor. The Contractor's obligation will be void as to any product or service modified by the Agency to the extent such modification is the cause of the claim.

ARTICLE 10 - WARRANTIES

NA

ARTICLE 11 - CONTRACTOR PERSONNEL

A. Approval of Contractor Personnel

Personnel proposed in the Contractor's written proposal to the Procuring Agency are considered material to any work performed under this Price Agreement.

a. Once a Purchase Order has been issued, no changes of personnel will be made by the Contractor without prior written consent of the Procuring Agency. Replacement of any Contractor personnel, if approved, shall be with personnel of equal ability, experience and qualifications. The Contractor will be responsible for any expenses incurred in familiarizing the replacement personnel to insure their being productive to the project immediately upon receiving assignments. Approval of replacement personnel shall not be unreasonably withheld.

b. The Procuring Agency shall retain the right to request the removal of any of the Contractor's personnel at any time.

ARTICLE 12 – STATUS OF CONTRACTOR

A. **Independent Contractor.** The Contractor and its agents and employees are independent contractors performing professional services for the Agency and are not employees of the State of New Mexico. The Contractor and its agents and employees shall not accrue leave, retirement, insurance, bonding, use of state vehicles, or any other benefits afforded to employees of the State of New Mexico as a result of this Agreement. The Contractor acknowledges that all sums received hereunder are personally reportable by it for income tax purposes as self-employment or business income and are reportable for self-employment tax.

B. **Subject of Proceedings.** Contractor warrants that neither the Contractor nor any officer, stockholder, director or employee of the Contractor, is presently subject to any litigation or administrative proceeding before any court or administrative body which would have an adverse effect on the Contractor's ability to perform under this Agreement; nor, to the best knowledge of the Contractor, is any such litigation or proceeding presently threatened against it or any of its officers, stockholders, directors or employees. If any such proceeding is initiated or threatened during the term of this Agreement, the Contractor shall immediately disclose such fact to the Agency.

ARTICLE 13- CHANGE MANAGEMENT

A. **Changes.** Contractor may only make changes or revisions within the Scope of Work as defined by Article 2 and Exhibit A after receipt of written approval by the Executive Level Representative. Such change may only be made to Tasks or Sub-Task as defined in the Exhibit A. Under no circumstance shall such change affect the:

- 1) Deliverable requirements;
- 2) Compensation due under the terms of this Agreement; or
- 3) Due Date of any Deliverable.

B. **Change Request Process.** In the event that circumstances warrant a change to accomplish the Scope of Work as described above, a Change Request shall be submitted that meets the following criteria: 1) The Project Manager shall draft a written Change Request for Executive Level Representative review and approval to include: the name of the person requesting the change, a summary of the required change, the start date for the change, the reason and necessity for change, the urgency level for the change, the elements to be altered, the impact of the change, the staffing plan associated with the change, the impact on the schedule for implementing the change, the cost impact, the risk assessment and a recommended approach to the change, and 2) The Executive Level Representative shall provide a written decision on the Change Request to the Contractor within a maximum of ten (10) working days of receipt of the Change Request. All decisions made by the Executive Level Representative are final. Change requests, once approved, become a part of the contract and become binding as a part of the original contract.

ARTICLE 14 – DEFAULT/BREACH

In case of default and/or breach by the Contractor, for any reason whatsoever, the Agency and the State of New Mexico may procure the goods or services from another source and hold the Contractor responsible for any resulting excess costs and/or damages, including but not limited to, direct damages, indirect

damages, consequential damages, special damages and the Agency and the State of New Mexico may also seek all other remedies under the terms of this Agreement and under law or equity.

ARTICLE 15 – EQUITABLE REMEDIES

Contractor acknowledges that its failure to comply with any provision of this Agreement will cause the Agency irrevocable harm and that a remedy at law for such a failure would be an inadequate remedy for the Agency, and the Contractor consents to the Agency's obtaining from a court of competent jurisdiction, specific performance, or injunction, or any other equitable relief in order to enforce such compliance. Agency's rights to obtain equitable relief pursuant to this Agreement shall be in addition to, and not in lieu of, any other remedy that Agency may have under applicable law, including, but not limited to, monetary damages.

ARTICLE 16 - LIABILITY

Contractor shall be liable for damages arising out of injury to persons and/or damage to real or tangible personal property before or after Acceptance, delivery, installation and use of the equipment, either at the Contractor's site or the Agency's place of business, provided that the injury or damage was caused by the fault or negligence of the Contractor or defect of the equipment or installation. Contractor shall not be liable for damages arising out of, or caused by, alterations to the equipment (other than alterations performed or caused by Contractor's officers, employees or agents) made by the Agency or for losses occasioned by the Agency's fault or negligence. Nothing in this Agreement shall limit the Contractor's liability, if any, to third parties and employees of the Agency or the State of New Mexico, or any remedy that may exist under law or equity in the event a defect in the manufacture of the equipment, or the negligent acts or omissions of the Contractor, its officers, employees, or agents, is the cause of injury to such person.

ARTICLE 17 – ASSIGNMENT

The Contractor shall not assign or transfer any interest in this Agreement or assign any claims for money due or to become due under this Agreement without the prior written approval of this Agreement's approval authorities.

ARTICLE 18 – SUBCONTRACTING

The Contractor shall not subcontract any portion of this Agreement without the prior written approval of the Agency. No such subcontracting shall relieve the Contractor from its obligations and liabilities under this Agreement, nor shall any subcontracting obligate payment from the Agency.

ARTICLE 19 – RELEASE

The Contractor's acceptance of final payment of the amount due under this Agreement shall operate as a release of the Agency, its officers and employees, and the State of New Mexico from all liabilities, claims and obligations whatsoever arising from or under this Agreement. The Contractor agrees not to purport to bind the State of New Mexico unless the Contractor has express written authority to do so, and then only within the strict limits of that authority.

ARTICLE 20 – CONFIDENTIALITY

Any confidential information provided to the contractor by the agency or, developed by the Contractor based on information provided by the agency in the performance of this Agreement shall be kept confidential and shall not be made available to any individual or organization by the Contractor without the prior written approval of the Agency. Upon termination of this Agreement, Contractor shall deliver all confidential material in its possession to the Agency within thirty (30) business days of such termination. Contractor acknowledges that failure to deliver such confidential information to the Agency will result in direct, special and incidental damages.

ARTICLE 21 – CONFLICT OF INTEREST

The Contractor warrants that it presently has no interest and shall not acquire any interest, direct or indirect, which would conflict in any manner or degree with the performance or services required under the Agreement. The Contractor certifies that the requirements of the Governmental Conduct Act, Sections 10-16-1 through 10-16-18, NMSA 1978, regarding contracting with a public officer, state employee or former state employee have been followed.

ARTICLE 22 - RECORDS AND AUDIT

The Contractor shall maintain detailed time and expenditure records that indicate the date, time, nature and cost of services rendered during this Agreement's term and effect and retain them for a period of three (3) years from the date of final payment under this Agreement. The records shall be subject to inspection by the Agency, CIO, SPA, and DFA. The Agency shall have the right to audit billings both before and after payment. Payment for services under this Agreement shall not foreclose the right of the Agency to recover excessive or illegal payments.

ARTICLE 23 - AMENDMENT

This Agreement shall not be altered, changed, or amended except by an instrument in writing executed by the Parties hereto. No amendment shall be effective or binding unless approved by all of the approval authorities.

ARTICLE 24 – NEW MEXICO EMPLOYEES HEALTH COVERAGE

A. If Contractor has, or grows to, six (6) or more employees who work, or who are expected to work, an average of at least 20 hours per week over a six (6) month period during the term of the contract, Contractor certifies, by signing this agreement, to:

- (1) have in place, and agree to maintain for the term of the contract, health insurance for those employees and offer that health insurance to those employees no later than July 1, 2008 if the expected annual value in the aggregate of any and all contracts between Contractor and the State exceed one million dollars or;

(2) have in place, and agree to maintain for the term of the contract, health insurance for those employees and offer that health insurance to those employees no later than July 1, 2009 if the expected annual value in the aggregate of any and all contracts between Contractor and the State exceed \$500,000 dollars or;

(3) have in place, and agree to maintain for the term of the contract, health insurance for those employees and offer that health insurance to those employees no later than July 1, 2010 if the expected annual value in the aggregate of any and all contracts between Contractor and the State exceed \$250,000 dollars.

B. Contractor agrees to maintain a record of the number of employees who have (a) accepted health insurance; (b) declined health insurance due to other health insurance coverage already in place; or (c) declined health insurance for other reasons. These records are subject to review and audit by a representative of the state.

C. Contractor agrees to advise all employees of the availability of State publicly financed health care coverage programs by providing each employee with, as a minimum, the following web site link to additional information: <http://insurenwmxico.state.nm.us/>.

D. For Indefinite Quantity, Indefinite Delivery contracts (price agreements without specific limitations on quantity and providing for an indeterminate number of orders to be placed against it); Contractor agrees these requirements shall apply the first day of the second month after the offeror reports combined sales (from state and, if applicable, from local public bodies if from a state price agreement) of \$250,000, \$500,000 or \$1,000,000, depending on the dollar value threshold in effect at that time.

ARTICLE 25 - MERGER, SCOPE, ORDER OF PRECEDENCE

A. **Severable.** The provisions of this Agreement are severable, and if for any reason, a clause, sentence or paragraph of this Agreement is determined to be invalid by a court or agency or commission having jurisdiction over the subject matter hereof, such invalidity shall not affect other provisions of this Agreement, which can be given effect without the invalid provision.

B. **Merger/Scope/Order.** This Agreement incorporates any and all agreements, covenants and understandings between the Parties concerning the subject matter hereof, and all such agreements, covenants and understanding have been merged into this Agreement. No prior agreement or understanding, verbal or otherwise, of the Parties or their agents or assignees shall be valid or enforceable unless embodied in this Agreement.

ARTICLE 26 - NOTIFICATION

Either party may give written notice to the other party in accordance with the terms of this paragraph. Any written notice required or permitted to be given hereunder shall be deemed to have been given on the date of delivery if delivered by personal service or hand delivery, or three (3) business days after being mailed.

To SPA:

State Purchasing Agent
Purchasing Division
Joseph M. Montoya State Building, Room 2016

1100 St. Francis Drive
Santa Fe, New Mexico 87505

To Contractor: CAaNES, LLC
10200 Comanche Rd. NE
Albuquerque, NM 87111

Either party may change its representative or address above by written notice to the other in accordance with the terms of this Paragraph 26. The carrier for mail delivery and notices shall be the agent of the sender.

ARTICLE 27- GENERAL PROVISIONS

- A. **Civil and Criminal Penalties.** The Procurement Code, Sections 13-1-28 through 13-1-199 NMSA 1978, imposes civil and criminal penalties for its violation. In addition, the New Mexico criminal statutes impose felony penalties for illegal bribes, gratuities and kickbacks.
- B. **Equal Opportunity Compliance.** The Contractor agrees to abide by all federal and state laws and rules and regulations, and executive orders of the Governor of the State of New Mexico, pertaining to equal employment opportunity. In accordance with all such laws of the State of New Mexico, the Contractor agrees to assure that no person in the United States shall, on the grounds of race, religion, color, national origin, ancestry, sex, age, physical or mental handicap, serious medical condition, spousal affiliation, sexual orientation or gender identity, be excluded from employment with or participation in, be denied the benefits of, or be otherwise subjected to discrimination under any program or activity performed under this Agreement. If Contractor is found not to be in compliance with these requirements during the life of this Agreement, Contractor agrees to take appropriate steps to correct these deficiencies.
- C. **Workers Compensation.** The Contractor agrees to comply with state laws and rules applicable to workers compensation benefits for its employees. If the Contractor fails to comply with the Workers Compensation Act and applicable rules when required to do so, this Agreement may be terminated by the Agency.
- D. **Applicable Law.** The laws of the State of New Mexico shall govern this Agreement. Venue shall be proper only in a New Mexico court of competent jurisdiction in the county where the Agency's main office is located. By execution of this Agreement, Contractor acknowledges and agrees to the jurisdiction of the courts of the State of New Mexico over any and all such lawsuits.
- E. **Waiver.** A party's failure to require strict performance of any provision of this Agreement shall not waive or diminish that party's right thereafter to demand strict compliance with that or any other provision. No waiver by a party of any of its rights under this Agreement shall be effective unless expressed and in writing, and no effective waiver by a party of any of its rights shall be effective to waive any other rights.
- F. **Headings.** Any and all headings herein are inserted only for convenience and ease of reference and are not to be considered in the construction or interpretation of any provision of this Agreement. Numbered or lettered provisions, sections and subsections contained herein, refer only to provisions, sections and subsections of this Agreement unless otherwise expressly stated.

G. Work Site. Work shall be performed at the Procuring Agency's site unless specified otherwise in the Procuring Agency Agreement.

H. Succession. This Price Agreement shall extend to and be binding upon the successors and assigns of the parties.

ARTICLE 28 - SURVIVAL

The Articles entitled Intellectual Property, Intellectual Property Ownership, Confidentiality, and Warranties shall survive the expiration or termination of this Agreement. Software License and Software Escrow agreements and other unexpired agreements entered into in conjunction with this Agreement shall survive the expiration or termination of this Agreement.

ARTICLE 29 - TIME

Calculation of Time. Any time period herein calculated by reference to "days" means calendar days; provided, however, that if the last day for a given act falls on a Saturday, Sunday, or a holiday as observed by the State of New Mexico, the day for such act shall be the first day following that is not a Saturday, Sunday, or such observed holiday.

ARTICLE 30- AGREEMENT ADMINISTRATOR

The SPA shall appoint an agreement administrator whose duties shall include, but not be limited to, the following:

- a. The agreement administrator shall attempt to facilitate dispute resolution between the Contractor and procuring agencies. Unresolved disputes shall be presented to the SPA for resolution.
- b. The agreement administrator shall review and recommend approval or disapproval of all requested changes to the Contractor's Services Schedule.
- c. The agreement administrator shall advise the SPA regarding the Contractor's performance under the terms and conditions of the agreement.
- d. The agreement administrator shall assist procuring agencies with the preparation of purchase orders and the approval thereof.
- e. The agreement administrator shall review and accept quarterly utilization reports.

ARTICLE 31 - ADMINISTRATIVE REPORTING FEES

a. The contractor agrees to provide periodic price agreement utilization reports to the agreement administrator in accordance with the following schedule:

<u>Period End</u>	<u>Report Due</u>
June 30	July 31
September 30	October 31

December 31 January 31
March 31 April 30

b. The periodic report shall include the gross revenues for the period subtitled by Procuring Agency name. If no revenue was generated for the period, a report shall be filed stating that fact. Reports containing revenue shall be accompanied with a check payable to SPA for an amount equal to one-half of one percent (0.0050) of the gross revenue for the period.

c. The failure to file the utilization reports and fees on a timely basis shall constitute grounds for suspension of the Price Agreement or termination of the Price Agreement for cause.

ARTICLE 32 – EMPLOYEE PAY EQUITY REPORTING

*Contractor agrees if it has ten (10) or more employees OR eight (8) or more employees in the same job classification, at any time during the term of this contract, to complete and submit the required reporting form (PE10-249 or PE250, depending on their size at the time) either within thirty (30) calendar days of contract award (if the contract did not result from a solicitation) or on the annual anniversary of the initial report submittal for contracts up to one (1) year in duration (if the contract did result from a solicitation).

*For contracts that extend beyond one (1) calendar year, or are extended beyond one (1) calendar year, contractor also agrees to complete and submit the required form annually within thirty (30) calendar days of the annual contract anniversary date of the initial submittal date and, if more than 180 calendar days has elapsed since submittal of the last report, at the completion of the contract.

*Should contractor not meet the size requirement for reporting at contract award but subsequently grows such that they meet or exceed the size requirement for reporting, contractor agrees to provide the required report within ninety (90) calendar days of meeting or exceeding the size requirement. That submittal date shall serve as the basis for submittals required thereafter.

*Contractor also agrees to levy these reporting requirements on any subcontractor(s) performing more than 10% of the dollar value of this contract if said subcontractor(s) meets, or grows to meet, the stated employee size thresholds during the term of the contract. Contractor further agrees that, should one or more subcontractor not meet the size requirement for reporting at contract award but subsequently grows such that they meet or exceed the size requirement for reporting, contractor will submit the required report, for each such subcontractor, within ninety (90) calendar days of that subcontractor meeting or exceeding the size requirement. Subsequent report submittals, on behalf of each such subcontractor, shall be due on the annual anniversary of the initial report submittal. Contractor shall submit the required form(s) to the State Purchasing Division of the General Services Department, and other departments as may be determined, on behalf of the applicable subcontractor(s) in accordance with the schedule contained in this paragraph. Contractor acknowledges that this subcontractor requirement applies even though contractor itself may not meet the size requirement for reporting and be required to report itself.

*Contractor shall not be required to report more frequently than annually unless more than 180

calendar days has elapsed since submittal of the last report and the contract has reached completion. The requirement for reporting at contract completion shall not apply in the case of a one-time fulfillment of a purchase order."

ARTICLE 33 - FORCE MAJEURE

Neither party shall be liable in damages or have any right to terminate this Agreement for any delay or default in performing hereunder if such delay or default is caused by conditions beyond its control including, but not limited to Acts of God, Government restrictions (including the denial or cancellation of any export or other necessary license), wars, insurrections and/or any other cause beyond the reasonable control of the party whose performance is affected.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the date of the signature by the required approval authorities below.

By: [Signature] Date: 26 MAY 2011
CAINES, LLC

By: [Signature] Date: 6/2/11
Jay Jones, GSD General Council
For Legal Sufficiency

The records of the Taxation and Revenue Department reflect that the Contractor is registered with the Taxation and Revenue Department of the State of New Mexico to pay gross receipts and compensating taxes:

CRS ID Number: 03-079518-00-4

By: [Signature] Date: 6/3/11
Taxation & Revenue Department

Approved as to information technology contractual specifications and compliance with the Department of Information Technology Act, Laws 2007, Chapter 290 and any and all Executive Orders relating to Information Technology issued by the Governor of the State of New Mexico:

By: [Signature] Date: 6/13/11
Darryl Ackley, Secretary
Department of Information Technology

This Agreement has been approved by the SPA:

By: [Signature] Date: 6/21/11
Purchasing Agent for the State of New Mexico

Exhibit A

Service Category 5: Security Services

Sub-service Category	Skills	Maximum Hourly Service Rate	Training Rate	Products Supported
IT Security Services	ITSS1	\$75.00	N/A	Please see below table.
	ITSS2	\$105.00		
	ITSS3	\$135.00		

Network Discovery tools	Look@Lan, Angry IP scanner, OpUtilis, 3Com Network
Password Crackers	Cain and Abel, John the Ripper
Sniffers	Wireshark, Kismet, Ntop, NetStumbler
Vulnerability Scanners	Nessus, Nmap, Retina, LANguard, QualysGuard, NeXpose express, Microsoft Baseline Security Analyzer
Wireless Testing tools	Netstumbler, Aircrack, Backtrack
Penetration Testing tools	Metasploit framework, Backtrack, Core Impact, Canvas
Forensic tools	DEFT, Helix, Backtrack
Networking Software	Cisco IOS, Cisco PIX, Cisco ASA, Packet tracer
Networking Hardware	Cisco routers and Switches, Cisco Firewall (ASA, PIX)
Networking Protocols	TCP/IP, UDP, SNMP, RIP, EIGRP, OSPF, IS-IS, ARP, RARP,
Network and Log monitoring tools	Cacti Network monitoring tool, Spiceworks, PRTG, Kiwi Syslog, Logwatch, Solarwinds Orion
Antivirus Software/ Malware Removal tools	Symantec Endpoint Protection, Sophos, Kaspersky Virus Removal Tools, Avira Rescue Disk, Bit Defender Rescue Disks
War Dialers	ToneLoc, THC-Scan, PhoneSweep
Packet Crafting	Scapy, Yersinia, Hping2
VoIP Sniffing Tools	Cain and Abel, SIPVicious Tool Suite
Encryption Tools	Truecrypt, GnuPG

Assessment Frameworks	ISO 27002, HIPAA, PCI DSS, FISMA, FFIEC, New Mexico State Security standards, NIST, Zachman Framework, ITIL, ISACA auditing standards
Operating systems	Microsoft Windows (2000, XP, Vista, 7), Windows Server (2000, 2003, 2008) , Linux (Fedora, Debian), Mainframe



State of New Mexico
General Services Department
Purchasing Division

Statewide Price Agreement Amendment

Awarded Vendor
0000063360
CAaNES, LLC
7801 Academy Rd NE Ste. 1-202
Albuquerque, NM 87109

Telephone No. (505) 217-9422

Price Agreement Number: 10-000-00-00051AI

Price Agreement Amendment No.: Two

Term: July 1, 2011 – March 30, 2014

Ship To:
All State of New Mexico agencies, commissions,
institutions, political subdivisions and local public
bodies allowed by law.

Invoice:
As Requested

Procurement Specialist: India Garcia

Telephone No.: (505) 827-0483

Title: IT Professional Services

This Price Agreement Amendment is to be attached to the respective Price Agreement and become a part thereof.

In accordance with Price Agreement provisions, and by mutual agreement of all parties, this Price Agreement is extended from June 1, 2013 to March 30, 2014 at the same price, terms and conditions.

Except as modified by this amendment, the provisions of the Price Agreement shall remain in full force and effect.

Accepted for the State of New Mexico

New Mexico State Purchasing Agent

Date: 2//18/13

Purchasing Division, 1100 St. Francis Drive 87505, PO Box 6850, Santa Fe, NM 87502-6850 (505) 827-0472

AM
2/18/13

1. Executive Summary

Our cyber assessment and penetration testing methodology enables proactive detection and remediation of security vulnerabilities. The assessment is conducted to evaluate (Technical, Operational, and Management) controls in place at the network, system, and application layers that help protect client's systems and data from unauthorized access, use and compromise.

Our IT risk assessment services will provide a comprehensive evaluation of CSF-NM's Security Governance, Risk Management and Compliance (GRC). Our assessments and tests are targeted; hence we are able to accomplish this with minimal disruption to the client's enterprise operations. Our assessments are also very comprehensive by providing 100% coverage and not using "sampling" methods that is the common practice of our competitors.

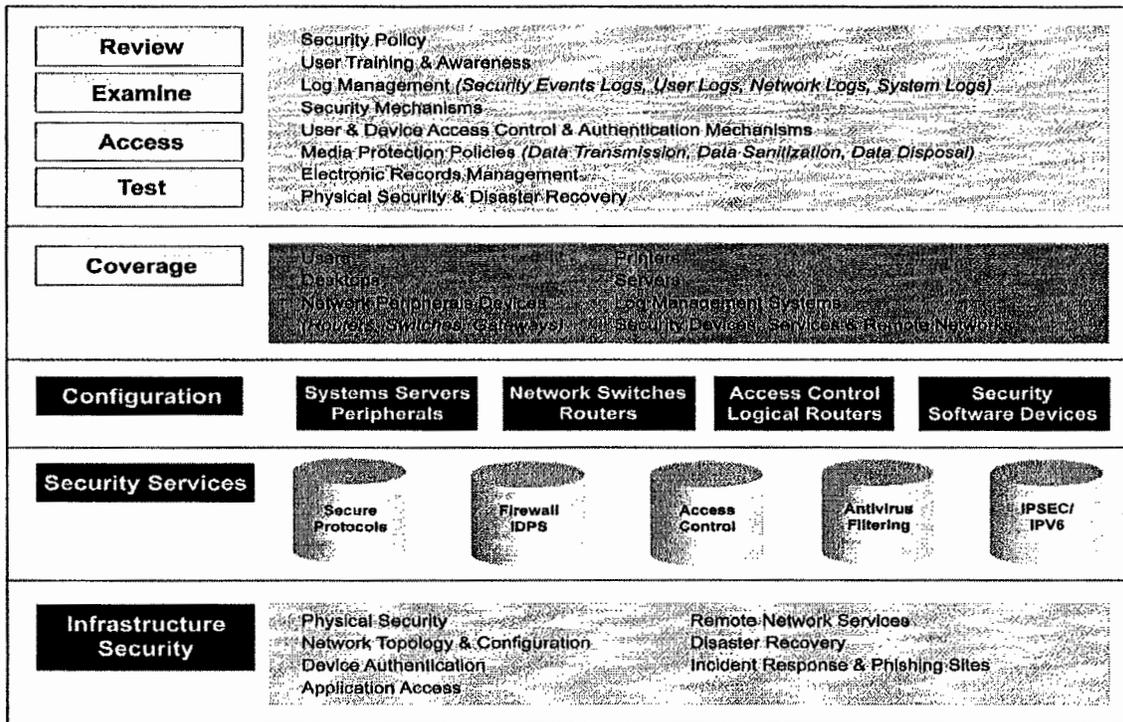


Figure1: Cyber Assessment Coverage and Penetration Testing

The assessment effort is divided into four major categories:

- Regulatory Compliance Assessment,
- Infrastructure and Technical Controls Assessment (Internal and External),
- Application Security Posture Assessment,
- Road Map to achieve Baseline Security.

The assessment includes the operations and technologies associated with directly defending against interruption, interception, modification, and fabrication to the client enterprise network. To ensure complete information security posture assessment the assessment includes analysis of information systems, network peripherals, information security devices, and applications. Descriptions of five major categories and an optional category are given below:

- **Regulatory Compliance Assessment:**

CAaNES conducts assessments that are based on multiple best practice frameworks including ISO27001/27002, COBIT, ITIL, Zachman, COSO, NIST, and FSAM, as well as relevant regulatory requirements such as HIPAA, NIST, and State laws.

Our assessments are comprehensive, cost effective, and are performed in accordance with customer specified federal, state, and industry regulations which assist organizations to embed a well-defined and compliant framework into their operations.

- **Infrastructure and Technical Controls Assessment (Internal and External):**

This is a comprehensive evaluation of current network, applications, systems, and computing environments using best practices and non-invasive methods to identify gaps within CSF-NM's computing environment.

To ensure complete information security posture assessment, our team performs assessments using a multi scanner approach based on **100% coverage of every device** (every device with an IP address printers, network peripherals, desktops, servers, VMs, etc.) within the internal network and external IP ranges owned by CSF-NM.

- **Application Security Posture Assessment:**

This is an evaluation of web applications in a distinct and customized approach based on the target web application's features. We provide an in-depth understanding of how an input changes data inside the application.

We use a proprietary framework to discover multiple attack vectors by passing or inputting data to user interfaces, network interfaces, application programming interfaces (APIs), and other places where inputs are processed.

- **Recommendations and Road Map to Achieve Baseline Security:**

CAaNES provides recommendations on how to address the identified gaps within CSF-NM regulatory, infrastructure, and applications. We provide a detailed analysis on vulnerability/threat pairs and their impact to CSF-NM.

We also provide a requirement traceability matrix to mitigate current threats and achieve baseline security for High-Impact systems.

2. Regulatory Compliance Assessment

This is a comprehensive, in-depth security posture assessment based on multiple best practice frameworks including ISO27001/27002, COBIT, NIST, ITIL, Zachman, COSO, and FSAM, as well as relevant regulatory requirements such as HIPAA, NIST, and State laws. Our assessments services and audits are comprehensive, cost effective, and are performed in accordance with customer specified federal, state, and industry regulations which assist organizations to embed a well-defined and compliant framework into their operations.

We utilize a segmented architecture approach for internal auditing, as shown in Exhibit 1, which employs a consistent and iterative assessment and implementation of compliance requirements into each infrastructure element. Application of this methodology encompasses the controls that are required to be implemented by federal, state, local, and industry specific regulations and guidelines. The phases defined are as follows:

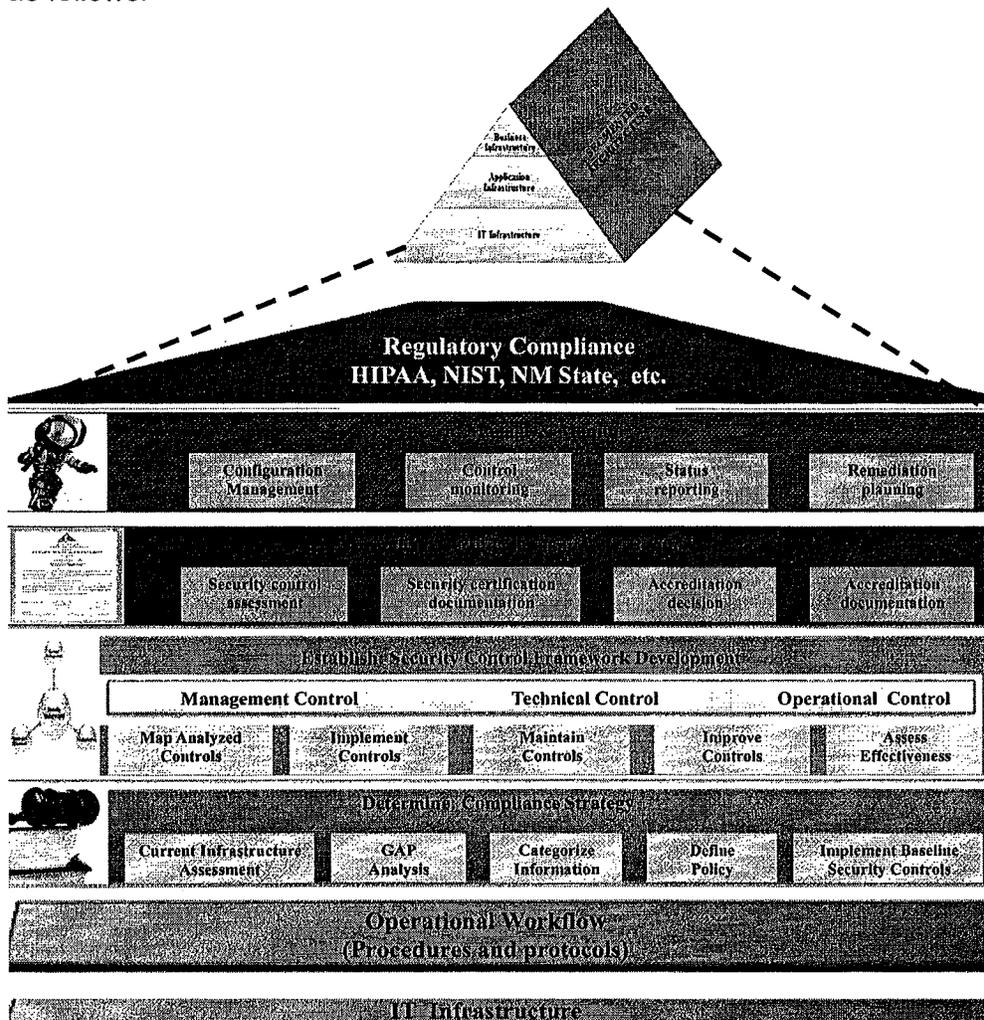


Figure 2: Segmented Architecture Approach for Security Posture Assessment

- **Determine (Compliance Strategy):** During this initiation phase, we work with an organization to identify established procedures which will be assessed. This phase is the first step in completing a strategic gap analysis. The gap analysis provides a vision of the policies and controls to be implemented to achieve required compliance levels. By the end of this phase, a security baseline is established.
- **Establish (Security Control Framework Development):** This phase defines deployment of administrative, technical and operational controls. Previously defined controls are mapped respectively, implemented and assessed for effectiveness.
- **Formalize (Certification & Accreditation):** The Certification phase evaluates the extent to which controls have been established in each of the segments and if implemented controls produce desired outcomes. This phase helps in assessing vulnerabilities and risks associated with systems and applications. The Accreditation phase provides formal authorization for the operation of system and associated applications. By the end of this phase, the risks and vulnerabilities of a system are analyzed and either eliminated or risk accepted which defines the baseline for the assessment of the system.
- **Govern (Manage & Monitor):** Implementing and maintaining regulatory compliance is a process. The management within organizations is required to demonstrate accountability and due diligence in deploying, maintaining and monitoring a compliance framework. During this phase, the continuous auditing and monitoring processes are defined and established for the system controls for the ongoing maintenance of the infrastructure.

3. Infrastructure and Technical Controls Assessment (Internal and External)

Our assessments are based on proven, non-intrusive and patent pending methodologies and are the most comprehensive in the industry. Our experts will use proprietary tools and redundant benchmark tools to ensure cross validation and uniformity of process and consistency of results. The assessment effort will be divided into three major categories, internal, external and remote assessment.

Assessments include the operations, processes and technologies associated with directly defending against interruption, interception, modification, and fabrication to the client's network, information systems and information operations. To ensure complete information security posture assessment, our team performs assessments based on **100% coverage** of every device. Every device with an IP address will be assessed for security risks (System, Network, Application, and Compliance).

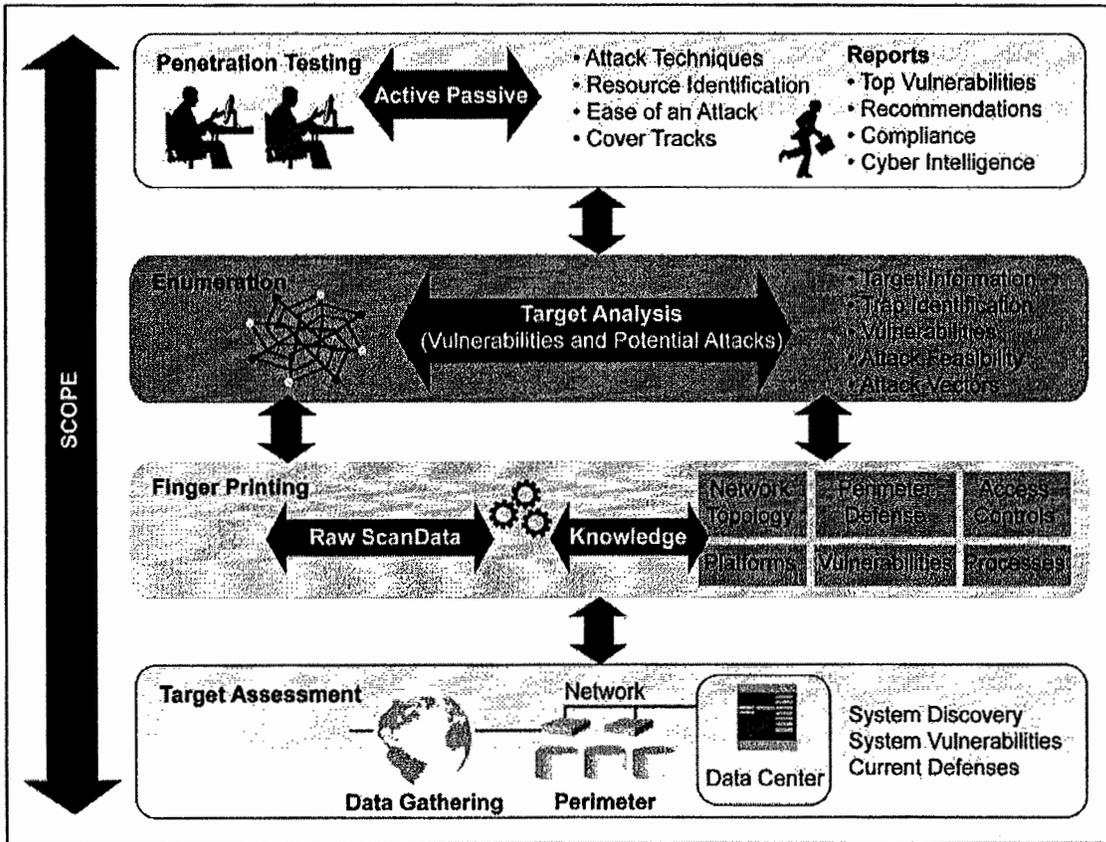


Figure 3: Strike Force Technical Controls Assessment Process and Framework

The assessment will include analysis and review of policies, applications, information systems, network peripherals, information security devices (firewalls, intrusion prevention and detection systems), remote access services, wireless access points, printers, back-up systems, log management systems, voice over IP systems, disaster recovery techniques and physical security. **Figure 3** illustrates the Strike Force

Assessment Process and Framework process developed by our Team to perform assessments.

Our security assessments provide a comprehensive evaluation of current network, applications, systems, and computing environments using best practices and non-invasive methods. To ensure a complete information internal security posture assessment, the assessment will include analysis and review of information systems (core components of CSF-NM's infrastructure, routers, firewalls, desktops, and servers), network peripherals, information security devices, printers, back-up systems, log management systems, disaster recovery techniques and physical security.

CAaNES was one of the first teams in the world to launch a **fragmented RFID malware** that would exploit vulnerabilities in middleware, embedded control systems, and penetrate heavily defended networks. CAaNES performs extensive research on Malware synthesis and analysis and has developed proprietary algorithms that help detect rapid variants which go undetected by most current antivirus technologies.

Network Posture Assessment

A review of client's network architecture to determine how it effectively isolates untrusted outside networks from gaining access to client's internal, trusted networks and information.

- Review of current network architecture
- Analysis of individual nodes, servers and peripherals on the network
- Assessment of current authentication methods (user and hardware perspective)
- Network topology review and assessment of current services
- Critical node assessment for fail over analysis

Review all Communication Channels, Protocols, and Data Flow

A review of client network design and implementations to determine how effectively it isolates insiders based on their roles and need to access client's information resources

- Data flow analysis
- Assessment of physical and logical connections
- Network Assets inventory and classification
- Protocols used for communication
- Dial-in and remote connection assessments

Security Posture Assessment

A thorough review of security controls of the client covering policy, processes, procedures, people, access controls, network, communications, systems and compliance from inside, remote and outside.

- Perimeter analysis
- Internal analysis
- Wireless security assessment
- Remote connection analysis
- Remote access services and virtual private network analysis

- Application service providers and trusted networks analysis

System and Application Components Review

Detailed analysis of system and application components using automated and manual means CAaNES will test the additional components of your application presentation. This will consist of testing the following areas as applicable:

- Operating system
- Web servers
- Databases

Within each of these Web components, CAaNES will analyze and test the following security areas:

- Configuration security
- Audit logging
- Security of directory structures and volumes
- Patches and hot-fixes
- Services, ports, and protocols
- Review of endpoint security procedures (HIPS, Antivirus technologies)
- Access, password, and account controls
- Registry settings
- Other areas as necessary

Penetration Testing and Analysis

Penetration Testing - A test designed with an adversarial intent to gain unauthorized access to portions of client's network from the perspective of a trusted user and adversary from inside, remote and outside.

- Perform reconnaissance and penetration testing on the network from internal nodes, remote nodes and external nodes
- Perform analysis on possible secondary exploits
- Red teaming refers to the work performed to provide an adversarial perspective
- Perform analysis and review of remote connection services (remote access servers, virtual private networks, terminal services, etc.)
- Perform war driving and attempt to gain access to client's wireless access points
- Perform war dialing

Analysis of Penetration Test performed

- Basic attack mapping analysis and attack trees
- Analysis of data integrity compromises
- Risk matrix of the discovered vulnerabilities

Virtual Infrastructure Review

A review of policies, procedures, and processes surrounding virtual infrastructure to identify gaps and mitigate risks

- Review virtual infrastructure architecture
- Uncover gaps with DISA/NIST STIGs for virtual infrastructure configuration
- Review access controls
- Review patch management and system separation
- Review virtual network segmentation
- Review logging and audit controls

Recommendations for Security Enhancement

- Internal and external security standards and practices
- Develop requirement traceability matrix and recommend baseline user training
- Assist in developing forms and procedures for incident reporting and response
- Perimeter defense and network performance enhancement
- Map required or preferred tools to current vulnerabilities
- Recommend patches and protection mechanisms for the identified vulnerabilities
- Recommend rules for the new security technologies procured
- Recommend enhanced network architecture

Common Tools

Network security assessments are very dynamic in nature and use a wide variety of tools. The following is a list of tools that are used during this type of engagement. The specific demands of a test may necessitate additional tools or code to be created.

LOOK@LAN	3COM Director	Nmap	Nessus
Retina	NeXpose	CAaNES – MVP BRAVE	Metasploit
CISCO SNMP Tool	Firewalk	Cain & Able	Wireshark
VirusTotal	NetStumbler	BackTrack	

4. Application Security Posture Assessment

CAaNES evaluates web applications in a distinct and customized approach based on the target web application's features. This is achieved using CAaNES' proprietary framework and industry's leading automated tools. We divide a web application security posture into two phases namely:

- Automated Testing Phase
- Manual Testing and Penetration Phase

Automated testing forms the initial layer of web application security posture and reflects black box testing of the web application. In this phase industry's leading web application vulnerability scanners are used to scan and test the web application for critical vulnerabilities. CAaNES' security consultants are proficient in training these tools based on application's architecture and compliance requirements.

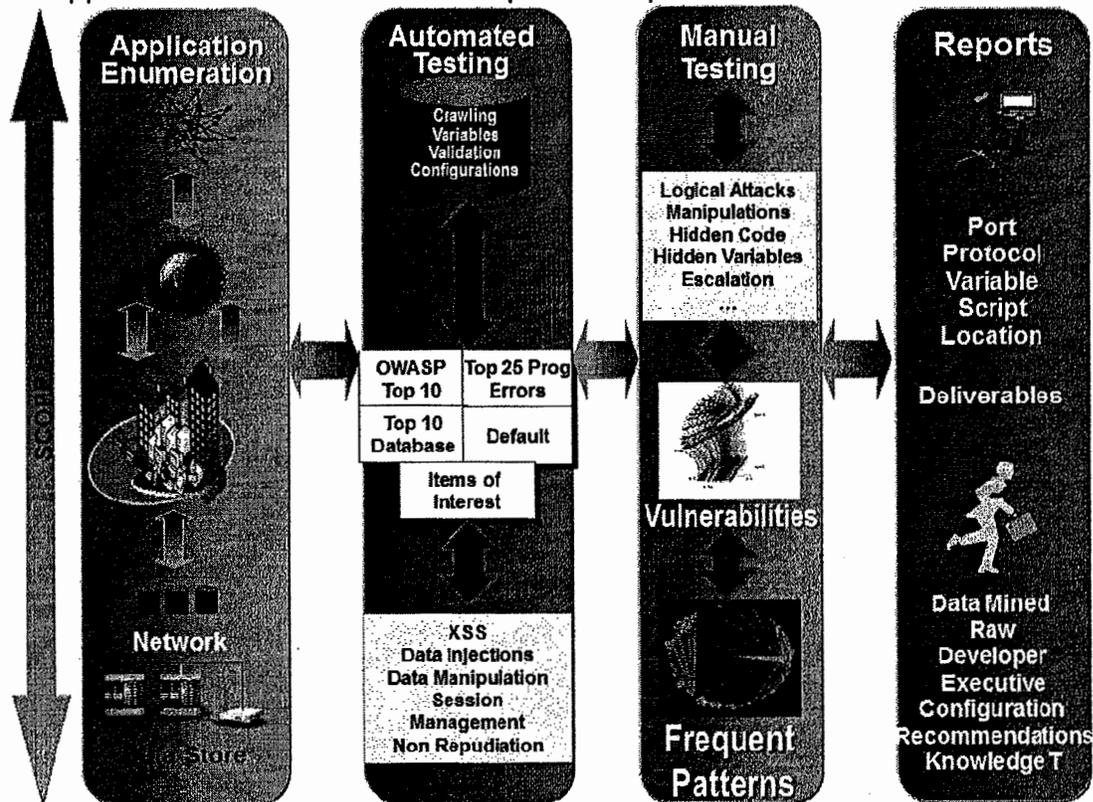


Figure 4: Proprietary Web Application Security Posture Assessment Methodology

Why go beyond automated testing?

Manual testing forays into areas where automated testing fails to make its mark. CAaNES uses its proprietary framework in this phase to overcome limitations of automated tools which CAaNES security experts have identified using their vast web application penetration testing knowledge. This phase is used to test security standards followed in every aspect of a web application; ranging from its internal logic control flow

to any existing misconfiguration issues. CAaNES powered manual testing and penetration phase provides following additional features:

- **Business Logic Testing**

CAaNES security consultants analyze the existing business logic of a web application and find security flaws within the control flow of data. E-commerce and financial applications are targets of attacks, which exploit security flaws in control flow of data within the application. In this testing phase, data flow of hidden variables is analyzed and manipulated to validate security flaws while the application still meets business logic requirements.

- **Privilege Escalation (Grey box testing)**

Target web applications are tested for privilege escalation in which CAaNES security consultants login to the application using a least privileged user account, try to escalate user access level by identifying insecure direct object references and gain access to data items that are restricted to users with higher privilege access levels. During this testing phase, session controls of the application are also validated and session hijacking is performed to gain privilege escalation.

- **Virtual Directory Crawling**

Automated scanners have a serious limitation in crawling virtual directories configured for a web application. Since the virtual directory is not being crawled, all web pages and data within the virtual directory is omitted for testing during the automated phase. CAaNES detects existing virtual directories within a web application and crawls using its proprietary framework **AppSploit** and performs vulnerability testing on pages and data within virtual directory.

- **Web 2.0 Vulnerabilities**

Emerging web 2.0 technologies have increased the leverage users have on web applications. Applications built using web 2.0 technologies like AJAX (Asynchronous JavaScript and XML) enable users to upload and change content existing on web applications. These technologies are capable of querying web service related data directly from the back end.

Considering these advances in web applications, CAaNES consultants test for vulnerabilities related to web 2.0 like AJAX injections and XML injections using proprietary scripts. This stage is used to analyze security standards of different APIs communicating with the target web application.

- **Complex Vulnerability Demonstration**

Automated scanners might find and report vulnerabilities existing in a web application, but they often fail to project the true criticality of these vulnerabilities. CAaNES security consultants combine vulnerabilities found during the automated phase and manual phase, explore and integrate multiple attack vectors possible to prove existence of more complex and critical vulnerabilities in the target web application.

- **Database Vulnerabilities**

CAaNES security consultants detect databases that interact with target web applications and try to penetrate into respective back end databases by exploiting vulnerabilities existing in the database. Web application is used as interface while penetrating into the database. This goes beyond SQL injections performed by automated tools since CAaNES security consultants insert executable code to penetrate into back end database.

- **Security Misconfigurations**

CAaNES security consultants analyze and review the directory structure of a web application based on crawling results obtained during automated testing and virtual directory crawling. This testing stage is used to validate permissions assigned to directories and files within. Communication channels used by the web application are tested for encryption standards.

4.1 Application Penetration Testing

Application penetration testing attack modules consist of payloads that belong to one or more of the four major attack taxonomies (interruption, interception, modification, and fabrication). Attack payloads that exploit common categories of application vulnerabilities are listed below.

Automated Testing

Automated testing is sometimes conducted concurrently with discovery. The automated testing process includes common, off-the-shelf tools, freeware and CAaNES-developed code. Several different scanners and tools are used to ensure that the maximum quantities of vulnerabilities are discovered and that no oversights occur.

The automated testing process is routinely run in an iterative fashion, and each iteration expands upon previously discovered issues. Automated testing is used to determine a baseline and to help the consultant locate potential threat vectors that may require additional manual testing. Automated testing features are highlighted in the following chart.

Automated Testing Features		
Data Injection and Manipulation <ul style="list-style-type: none"> • Reflected Cross-Site Scripting (XSS) • Persistent XSS • Cross-site Request Forgery • SQL Injection • Blind SQL Injection • Buffer Overflows • Integer Overflows • Log Injection • Remote File Include Injection • Server Side Include (SSI) Injection • Operating System Command Injection • Local File Include (LFI) • Custom Fuzzing • Path Manipulation – 	Sessions and Authentication <ul style="list-style-type: none"> • Session Strength • Authentication Attacks • Insufficient Authentication • Insufficient Session Expiration • Brute Force Authentication Attacks • Support For CAPTCHA • Support for Single Sign-On • Support for Two Factor Authentication Mechanisms • Secure Sockets Layer (SSL) Certificate Issues • SSL Protocols Supported 	Server and General HTTP <ul style="list-style-type: none"> • Server Misconfigurations • Directory Indexing and Enumeration • Denial of Service • HTTP Response Splitting • Windows 8.3 File Name • DOS Device Handle DoS • Canonicalization Attacks • URL Redirection Attacks • Ajax Auditing • WebDAV Auditing • Web Services Auditing • File Enumeration • Information Disclosure • Directory and Path Traversal • Spam Gateway Detection • Known Application and Platform Vulnerabilities

<ul style="list-style-type: none"> • Traversal • Path Truncation 	<ul style="list-style-type: none"> • SSL Ciphers Supported • Password Auto Complete • Cookie Security 	<ul style="list-style-type: none"> • Detects Dangerous HTTP
--	--	--

Manual Testing

The ever-changing landscape of technology makes automated scanners difficult to keep updated. Based on the output from the automated testing tools, CAaNES' consultants use their expertise to analyze all potential threats and to conduct proof-of-concept testing where appropriate.

To ensure that the deepest possible analysis is conducted on every engagement, our consultants execute numerous manual-testing processes. These processes use publicly available tools coupled with CAaNES-created code to identify as many issues as possible.

Manual Testing Features		
Data Injection and Manipulation <ul style="list-style-type: none"> • SQL injections • Blind SQL Injections • Translate Encoding Standards • Regex Editing • SOAP Editing • Web Fuzzing/Buffer overflow check 	Sessions and Authentication <ul style="list-style-type: none"> • Brute Force authentications • Cookie crunching 	Server and General HTTP <ul style="list-style-type: none"> • HTTP Request/Response monitoring • HTTP/HTTPS Requests Editing • Mapping applications to ports • Server Analysis

• Injection Flaws

Injection flaw is the exploitation of a vulnerability that is caused when code is injected into a program/script from an external source for execution. The results of code injection can be disastrous; as it can compromise the entire security posture of an enterprise by affecting the security of web applications that can be extended to critical servers. Code injection is actively used by automated attacks and computer worms to propagate.

• Cross Site Scripting (XSS)

A vulnerability that occurs whenever an application takes data that is originated from a user or program and sends it to the browser without validating or encoding the data. An exploited XSS vulnerability can be used by adversaries to bypass access controls, hijack user sessions, deface web sites, insert hostile content, and conduct phishing attacks. XSS attacks are written in a markup language (HTML or XHTML) or client-side scripting language (Java script, Jscript, ActiveX, VB script, flash, and Action script). Most of the document recent security incidents occurred because of the presence of XSS vulnerabilities.

- Document Object Model XSS (DOM based) Vulnerabilities
- Non-Persistent Vulnerabilities

- Persistent Vulnerabilities

- **Insecure Direct Object Reference**

Direct object reference is a file that contains a reference to another object such as a file, directory, database record, and URL or form parameter. Insecure direct object reference occurs when a developer exposes to an internal implementation object and provides access without checking for proper authentication credentials.

- Null Byte Injection

- **Cross-Site Request Forgery**

A web based exploit that occurs when malicious or unauthorized commands or data is sent to a web application on behalf of a trusted user without the trusted user's knowledge or consent. Cross-site forgery exploits the trust that a web application has for a particular user.

- Automatic HTTP Request Execution
- Web Application Performing Security Sensitive Operations without User Validation

- **Canonicalization**

Gaining access to restricted portions of a web application by overcoming its weak canonical rules, using insufficient security validation and sanitization of user-supplied inputs.

- Directory Traversal
- Access to Restricted Pages

- **Additional Testing**

Apart from (Injection Flaws, Cross Site Scripting (XSS), Insecure Direct Object Reference, Cross Site Request Forgery, and Canonicalization) we also test the following exploitable vulnerabilities:

- Information Leakage and Improper Error Handling
- Broken Authentications and Session Management
- Insecure Cryptographic Storage and Weak Ciphers and Session Keys
- Insecure Communications (clear text protocols like Telnet and FTP for sensitive data)
- URL Access
- Regular Expression Checks
- Tainted Parameters
- Header Integrity
- Path Manipulation
- Thread Safety
- Hidden Form Field Manipulation
- Fail Open Authentication
- Weak Session Cookies
- Misconfigurations
- Weak Passwords

- **Detailed Analysis of Application Components**

Using automated and manual means CAaNES will test the additional components of your application presentation. This will consist of testing the following areas as applicable

- Operating System
- Web Servers
- Data Bases

- **Privileged Testing**

Application testing is first conducted with minimal to zero knowledge of your environment, processes, or applications. To be comprehensive in testing, we must consider the capabilities that an authorized user on the systems may have. As such, we will use authorized user accounts - normally a representation of 2-3 user roles - to test what an authorized user may accomplish. This will be primarily a manual exercise and we look to test, at a minimum, the following:

- Authorized User's Ability to Elevate Privileges
- Authorized User's Ability to View Other User/Account Data
- Authorized User's Ability to Add/Modify/Delete Other Account Data
- Authorized User's Existing Access is Appropriate Based Upon Role

Common Tools

Application security assessments are very dynamic in nature and use a wide variety of tools. The following is a sample list of tools that are commonly used during this type of engagement. The specific demands of a test may necessitate additional tools or code to be created.

Application Security Assessment Tools		
• NTO Spider	• CAaNES –AppSploit	• Nessus – Web Plugins
• Acunetix	• Wikto	• NeXpose – Web Plugins

5. Overview of Analytical Tools Used to Conduct Assessment

Our team is familiar with a large host of commercial, open source and proprietary IT security auditing and scanning tools. Our Team is offering the proprietary CAaNES Similarity Analysis of Malicious Executables (SAME®) tool and the CAaNES Mining Vulnerable Patterns (MVP®) tool as part of our service at no additional cost.

Behavioral based Risk Analysis of Vicious Executables (BRAVE®) functionally classifies malware and malicious code by using well-known computational intelligent techniques that goes undetected by traditional security tools and antivirus scanners.

BRAVE uses the latest vulnerability assessment techniques and a collection of proprietary algorithms to identify and report persistent malware indicators that target Confidential, Protected Health Information (PHI) and Personally Identifiable Information (PII).

MVP is a comprehensive analysis and reporting tool which was designed for providing a faster and easier way to assess network vulnerabilities; exploit the vulnerabilities assessed; generate the detailed report together with the remediation of the vulnerabilities, and produce the detailed procedures to patch the exploited vulnerabilities. This tool enables significant efficiencies and automation in producing the report describe above. The report itself is self-explanatory and is very easy to read and understand.

CAaNES **AppSploit** is another proprietary tool that we will use which runs on a laptop as a client application. AppSploit overcomes limitations of automated tools which CAaNES security experts have identified using their vast web application penetration testing knowledge. The tool will only be utilized on the Team's assessment toolkit and is not required to be installed on any End-Client information system.

Our proprietary technology employs well-developed intelligent network penetration techniques that are able to identify vulnerable information systems in a non-intrusive manner. This technique allows the security assessment to be conducted without disrupting End-Client operations or system availability.

Additional features:

- The technology creates assessment projects as sessions which are saved in the tool's database
- The Assessment users have the option to scan selected systems or a range of IP addresses
- The technology has the capability to integrate benchmark security tools and scanners by allowing users to automatically compare and contrast the results from the integrated tools
- Once the discovery and reconnaissance phase is complete, the tool automatically correlates the vulnerabilities with the available exploits in the tool's exploit database and the penetration risks
- Each step of the complete process is logged and the details of each step are included in the comprehensive report generated by the tool

6. Recommendations and Road Map to Achieve Baseline Security

After each individual test is performed, the team will provide an oral summary of the security test performed. Every evening, all of work will be orally summarized to the client. If a critical security issue is discovered, our team will immediately notify the client and work with them to mitigate risk

- At the completion of the assessment, the team provides a report containing summary and detailed information on the findings.
- The documentation covers the technical and business risk results of the performed tests, a high level executive overview of the findings, the recommendations of corrective actions and a detailed prioritization of those actions.
- Additionally, CAaNES' consultants use this phase to discuss the activities performed during the assessment and all other relevant information as part of the knowledge transfer process.
- This process ensures that the client team has all the information they need to take action to remediate any discovered issues.

Information Generated

Our team provides a summary of the network topology, the top 5 most vulnerable machines on the network, top 5 most vulnerable segments of the network, a cyber-intelligence report that maps to the global information security trends, user privilege summary (users never logged on, users that have never changed passwords and users with weak passwords), a summary of default settings (SNMP, FTP, default user names and passwords on computing devices), a port protocol service summary, a summary of the top 25 most dangerous programming errors, and top 10 OWASP vulnerabilities.

Summary of Task Reports

After the engagement is complete, a formal presentation is given with the methodology, findings and recommendations. The full, formal, written report is provided after the presentation and includes an executive summary, web/applications report, system component report, general audit and compliance report, network assessment report and recommendations.

This scope of this project includes the delivery of two separate presentations of the findings for the following customer audiences:

- Information Technology Team
- Senior Management

Next Activities

The presentation and the detailed reports provide a prioritized list of the most critical issues and vulnerabilities that need to be addressed.

7. Detailed SOW Deliverables

1. Information Security Assessment Project Plan & Rules of Engagement

- a. This Project Plan and Rules of Engagement are formed after the contract is finalized and signed. We will schedule an initial consultant introduction via teleconference and conduct a project kickoff meeting to prepare the Project Plan.
- b. During this meeting we will address the following:
 - Stated goals of the project
 - Project scope, methodology and rules of engagement
 - Escalation procedures on each side
 - Expectations for timeline, scheduling, coordination needs, milestones and deliverables
 - Areas of special focus or interest
 - Information specific to your organization
 - Clarification or changes in scope or needs
 - Document exchange
 - Personnel and team roles and responsibilities
 - Organizational risk and security practices
- c. The Project Plan consists of major milestones associated with preparing for and executing vulnerability and penetration tests across the IT infrastructure included in the scope of the contract. The Project Plan will be discussed and finalized with the approval of the End-Client's Chief Information Security Officer, the organizational equivalent, or other point of contact specified in the contract.
- d. The Rules of Engagement is a checklist of End-Client preferences or direction associated with how certain elements of the assessment will be conducted or the exclusion of any activities that are generally performed in an assessment.
 - For example, the Rules of Engagement may identify any exclusion of testing during certain timeframes during business hours or the exclusion or limitation of testing of any specific devices on the network.
 - Once the Project Plan and Rules of Engagement are agreed to, we will schedule and commence the work.
 - It is understood that there may be changes to the Project Plan or Rules of Engagement as the assessment progresses which may be caused by unforeseen circumstances such as the identification of a significant security incident.

2. Security Assessment Executive Summary

- a. The Executive Summary is a high level report of the summary findings from the assessment and is intended for senior managers. It will identify and discuss the top findings from the assessment with the highest potential for risk impact to the End-Client.

3. Security Posture Assessment Approach

- a. The assessment approach and manner in which the findings are uncovered will be described in the respective sections of the Security Posture Assessment Reports. The approach may include details such as the tool or tools used to perform the assessment and analysis performed which resulted in any specific conclusions or recommendations.

4. Security Posture Assessment Reports

- a. The Security Posture Assessment Reports provide a broad view of IT infrastructure elements and functional components with regard to their vulnerabilities associated with internal and external threats.
- b. The findings are determined through scans and penetration tests and provided detailed technical information on the vulnerabilities and remediation approaches. The elements and functional components for this report are as follows:
 - External, internal, and remote security posture
 - Network topology (external, remote and internal)
 - Desktop security
 - Wireless posture assessment
 - Virtualization security posture summary

5. Snapshot of Critical Information Security Risks

- a. This report provides a summary and ranking of the top 5 critical areas of the End-Client's IT security posture that have the greatest risks impact from an information assurance standpoint.
- b. Our risk ranking methodology presents risks as High, Medium, and Low priority based on many factors, including ease of exploitation, business criticality of the host and prevalence of the threat.
- c. Our consultants are familiar with several risk and vulnerability ranking methodologies and use them often. These include the Common Vulnerability Scoring System version 2 (CVSS v2), DREAD, Practical Threat Analysis (PTA) and others. If you would like us to focus on one of these models or your preferred model, we can usually accommodate that request.
- d. The vulnerabilities associated with the identified risks and how they may be compromised is detailed in this report. The report includes the following in terms of findings:
 - Consolidated Network wide Top 5 Vulnerable Subnets
 - Consolidated Network wide Top 5 Vulnerable Machines
 - Consolidated SNMP Summary Report
 - Consolidated anonymous FTP Summary Report
 - Consolidated Unique Port Protocol Service Summary Report
 - Consolidated Network wide list of IP addresses for which password does not expire

6. Penetration Testing Summary

- a. The Penetration Testing Summary provides the details of finding determined from internal and external attempts to compromise IT systems. The vulnerabilities associated with these risks and how they may be compromised is detailed in this report.

7. Web and Application Information Security Posture

- a. The Web and Application Information Security Posture report is a consolidated report includes findings from all of the web and applications scanners including the CAaNES proprietary data mining analysis work.
- b. The report organizes the findings based on the OWASP Top 10 and the CWE/SANS Top 25.
- c. The Open Web Application Security Project (OWASP) is an open community that focuses on improving web application security. OWASP Top 10 is a list of the most critical web application security risks.
 - Intended first as an awareness mechanism, the Top 10 covers the most critical web application security flaws via consensus reached by a global consortium of application security experts.
 - The OWASP Top 10 promotes managing risk via an application risk management program, in addition to awareness training, application testing, and remediation.
- d. Common Weakness Enumeration (CWE)/SANS Top 25 Most Dangerous Software Errors is a list of the most widespread and critical errors that can lead to serious vulnerabilities in software.
 - They are often easy to find, and easy to exploit. They are dangerous because they will frequently allow attackers to completely take over the software, steal data, or prevent the software from working at all.
- e. Within the report, the vulnerabilities found will be categorized as High, Medium or Low risks.

8. Configurations Review Summary with Recommendations

- a. This report provides a summary of recommendations for security controls setting configurations of the various devices in the IT infrastructure found to be at risk. It includes details down to operating system control settings.

9. Summary of Critical Policies and Procedures

- a. This report provides a summary of policies and procedures, which are critical to ensuring or increasing the security posture of an organization. It provides recommendations on any changes to policies such as password settings or use of IT resources, which would increase security posture.
- b. The report also addresses recommendations for any changes to existing procedures or new procedures, which would mitigate the potential for security risks based on roles and responsibilities of the staff performing the procedures, how they are being performed, or the discipline to ensure they are being performed consistently. Additional examples of areas addressed are:
 - Access control lists on network peripherals (firewall, detection devices, etc.)

- User and system level access control procedures
- Application and operating system hardening procedures
- Procedures for access management
- Audit policies and procedures
- Electronic data management policies and procedures

10. Social Media and Blog Mining

- a. Detailed report on internal policy violations, insider data leaks, and misuse of organizational information if found while mining the Web using meta searching

11. Information Security Audit Report per standard federal institutional guidelines and best practices

- a. This report is dependent on the compliance standard being used for the assessment.
- b. This standard establishes best practices for information technology security techniques and code of practice for information security management.
- c. The report provides findings of non-compliance with established institutional or industry guidelines associated with the standard.

12. Security Technical Implementation Guides for Operating Systems and Network Devices

- a. This detailed report provides specific guidance for remediating the vulnerabilities found on network devices and computers running various operating systems.
- b. It provides the options and detailed steps and procedures for making configuration changes or patching to address the specific vulnerabilities identified in the assessment.

13. Recommendations and Executive level presentations summarizing the assessment process and results:

- a. Two presentations are prepared which summarizes of all of reports and the major findings from the assessment. They are written to an appropriate level of detail for Executive Management and for IT Staff and Division Directors.

8. Cost

Assessment Type	Service Description	Estimated Hours/Cost	Cost
Regulatory Compliance Mapping	Identifying Gaps in Required Regulatory Compliance (FISMA and HIPAA) and Best Practices (ISO 27001/27002, COBIT, NIST)	55 Hours for information gathering, interviews, analysis and report writing	\$7,425
Information Security Policy Templates: Risk Management and Disaster Recovery	Provide Templates for Information Security Policies covering Risk Management and Disaster Recovery	40 Hours to develop templates 20 Hours to provide training and guidance	\$8,775
Network and System Vulnerability Assessment and Penetration Testing	Internal and External Network Vulnerability Assessment and Penetration Testing (Up to 1,500 Active IP Addresses)	Assuming Up to 1,500 Active IP Addressable Devices Estimated 92 Hours	\$12,420 (Assuming 1,500 Active IPs) B
Web Application Vulnerability Assessment and Penetration Testing (Automated and Manual) Internal and External	Enterprise wide - Large Web Application Security Posture Assessment and Penetration Testing (This Includes Automated and Manual Testing)	\$4500 Per Application (Varies on the Complexity of the Application under Test) Estimated 70 Hours	\$9,450 (Assumption 2 Enterprise Applications) 4
Total Cost		Not to Exceed \$38,070 + NMGR	

Please note ITSS3 – NM Statewide Price Agreement 135/Hour rate is being used.

Exhibit A

Service Category 5: Security Services

Sub-service Category	Skills	Maximum Hourly Service Rate	Training Rate	Products Supported
IT Security Services	ITSS1	\$75.00	N/A	Please see below table.
	ITSS2	\$105.00		
	ITSS3	\$135.00		

Network Discovery tools	Look@Lan, Angry IP scanner, OpUtilis, 3Com Network
Password Crackers	Cain and Abel, John the Ripper
Sniffers	Wireshark, Kismet, Ntop, NetStumbler
Vulnerability Scanners	Nessus, Nmap, Retina, LANguard, QualysGuard, NeXpose express, Microsoft Baseline Security Analyzer
Wireless Testing tools	Netstumbler, Aircrack, Backtrack
Penetration Testing tools	Metasploit framework, Backtrack, Core Impact, Canvas
Forensic tools	DEFT, Helix, Backtrack
Networking Software	Cisco IOS, Cisco PIX, Cisco ASA, Packet tracer
Networking Hardware	Cisco routers and Switches, Cisco Firewall (ASA, PIX)
Networking Protocols	TCP/IP, UDP, SNMP, RIP, EIGRP, OSPF, IS-IS, ARP, RARP,
Network and Log monitoring tools	Cacti Network monitoring tool, Spiceworks, PRTG, Kiwi Syslog, Logwatch, Solarwinds Orion
Antivirus Software/ Malware Removal tools	Symantec Endpoint Protection, Sophos, Kaspersky Virus Removal Tools, Avira Rescue Disk, Bit Defender Rescue Disks
War Dialers	ToneLoc, THC-Scan, PhoneSweep
Packet Crafting	Scapy, Yersinia, Hping2
VoIP Sniffing Tools	Cain and Abel, SIPVicious Tool Suite
Encryption Tools	Truecrypt, GnuPG

Assessment Frameworks	ISO 27002, HIPAA, PCI DSS, FISMA, FFIEC, New Mexico State Security standards, NIST, Zachman Framework, ITIL, ISACA auditing standards
Operating systems	Microsoft Windows (2000, XP, Vista, 7), Windows Server (2000, 2003, 2008) , Linux (Fedora, Debian), Mainframe



**City of Santa Fe
Summary of Contracts, Agreements, & Amendments**

Section to be completed by department for each contract or contract amendment

1 **FOR: ORIGINAL CONTRACT** or **CONTRACT AMENDMENT**

2 Name of Contractor Computational Analysis and Network Enterprise Solutions

3 Complete information requested Plus GRT

Inclusive of GRT

Original Contract Amount: \$38,070.00

Termination Date: June 30, 2014

Approved by Council Date: _____

or by City Manager Date: _____

Contract is for: Network security posture assessment & gap analysis

Amendment # _____ to the Original Contract# _____

Increase/(Decrease) Amount \$ _____

Extend Termination Date to: _____

Approved by Council Date: _____

or by City Manager Date: _____

Amendment is for:

4 **History of Contract & Amendments:** (option: attach spreadsheet if multiple amendments) Plus GRT

Inclusive of GRT

Amount \$ _____ of original Contract# _____ Termination Date: _____

Reason: _____

Amount \$ _____ amendment # _____ Termination Date: _____

Reason: _____

Amount \$ _____ amendment # _____ Termination Date: _____

Reason: _____

Amount \$ _____ amendment # _____ Termination Date: _____

Reason: _____

Total of Original Contract plus all amendments: \$ _____



City of Santa Fe
Summary of Contracts, Agreements, & Amendments

5 Procurement Method of Original Contract: (complete one of the lines)

RFP# _____ Date: _____

RFQ _____ Date: _____

Sole Source _____ Date: _____

Other SPD# 10-000-00-00051AI _____

6 Procurement History: None
example: (First year of 4 year contract)

7 Funding Source: ITT Professional Services BU/Line Item: 12029.5103

8 Any out-of-the ordinary or unusual issues or concerns:
None
(Memo may be attached to explain detail.)

9 Staff Contact who completed this form: Thomas J. Williams

Phone # 955-5580

10 Certificate of Insurance attached. (if original Contract)

Submit to City Attorney for review/signature
Forward to Finance Director for review/signature
Return to originating Department for Committee(s) review or forward to City Manager for review
and approval (depending on dollar level).

To be recorded by City Clerk:

Contract # _____

Date of contract Executed (i.e., signed by all parties): _____

Note: If further information needs to be included, attach a separate memo.

Comments:

Large empty rectangular box for comments.

CITY OF SANTA FE
PROFESSIONAL SERVICES AGREEMENT

THIS AGREEMENT is made and entered into by and between the City of Santa Fe (the "City") and CAaNES, LLC. (the "Contractor"). The date of this Agreement shall be the date when it is executed by the City and the Contractor, whichever occurs last.

1. SCOPE OF SERVICES

The Contractor shall provide the following services for the City and also described in Exhibit "A attached hereto and incorporated herein:

- A. Information Security Posture Assessment Methodology;
- B. Regulatory Compliance Assessment;
- C. Infrastructure and Technical Controls Assessment;
- D. Application Security Posture Assessment;
- E. Overview of Analytical Tools Used to Conduct Assessment;
- F. Recommendations and Road Map to Achieve Baseline Security;
- G. Deliverables:
 - (1) Information Security Assessment Project Plan & Rules of Engagement;
 - (2) Security Assessment Executive Summary;
 - (3) Security Posture Assessment Approach;
 - (4) Security Posture Assessment Reports;
 - (5) Snapshot of Critical Information Security Risks;
 - (6) Penetration Testing Summary;

- (7) Web and Application Information Security Posture;
- (8) Configurations Review Summary with Recommendations;
- (9) Summary of Critical Policies and Procedures;
- (10) Information Security Audit Report per standard federal institutional Guidelines and best practices;
- (11) Security Technical Implementation Guides for Operating Systems and Network Devices;
- (12) Recommendations and Executive level presentations summarizing the assessment process and results.

2. STANDARD OF PERFORMANCE; LICENSES

A. The Contractor represents that it possesses the experience and knowledge necessary to perform the services described under this Agreement.

B. The Contractor agrees to obtain and maintain throughout the term of this Agreement, all applicable professional and business licenses required by law, for itself, its employees, agents, representatives and subcontractors.

3. COMPENSATION

A. The City shall pay to the Contractor in full payment for services rendered, a sum not to exceed twenty five thousand dollars (\$25,000), plus applicable gross receipts taxes.

B. The Contractor shall be responsible for payment of gross receipts taxes levied by the State of New Mexico on the sums paid under this Agreement.

C. Payment shall be made upon receipt, approval and acceptance by the City of detailed statements containing a report of services completed. Compensation shall be paid only for services actually performed and accepted by the City.

4. APPROPRIATIONS

The terms of this Agreement are contingent upon sufficient appropriations and authorization being made by the City for the performance of this Agreement. If sufficient appropriations and authorization are not made by the City, this Agreement shall terminate upon written notice being given by the City to the Contractor. The City's decision as to whether sufficient appropriations are available shall be accepted by the Contractor and shall be final.

5. TERM AND EFFECTIVE DATE

This Agreement shall be effective when signed by the City and the Contractor, whichever occurs last, and shall terminate on June 30, 2013 unless sooner pursuant to Article 6 below.

6. TERMINATION

A. This Agreement may be terminated by the City upon 30 days written notice to the Contractor.

(1) The Contractor shall render a final report of the services performed up to the date of termination and shall turn over to the City original copies of all work product, research or papers prepared under this Agreement.

(2) If compensation is not based upon hourly rates for services rendered, therefore the City shall pay the Contractor for the reasonable value of

services satisfactorily performed through the date Contractor receives notice of such termination, and for which compensation has not already been paid.

(3) If compensation is based upon hourly rates and expenses, Contractor shall be paid for services rendered and expenses incurred through the date Contractor receives notice of such termination.

7. STATUS OF CONTRACTOR; RESPONSIBILITY FOR PAYMENT OF EMPLOYEES AND SUBCONTRACTORS

A. The Contractor and its agents and employees are independent contractors performing professional services for the City and are not employees of the City. The Contractor, and its agents and employees, shall not accrue leave, retirement, insurance, bonding, use of City vehicles, or any other benefits afforded to employees of the City as a result of this Agreement.

B. Contractor shall be solely responsible for payment of wages, salaries and benefits to any and all employees or subcontractors retained by Contractor in the performance of the services under this Agreement.

C. The Contractor shall comply with City of Santa Fe Minimum Wage, Article 28-1-SFCC 1987, as well as any subsequent changes to such article throughout the term of this Agreement.

8. CONFIDENTIALITY

Any confidential information provided to or developed by the Contractor in the performance of this Agreement shall be kept confidential and shall not be made available to any individual or organization by the Contractor without the prior written approval of the City.

9. CONFLICT OF INTEREST

The Contractor warrants that it presently has no interest and shall not acquire any interest, direct or indirect, which would conflict in any manner or degree with the performance of services required under this Agreement. Contractor further agrees that in the performance of this Agreement no persons having any such interests shall be employed.

10. ASSIGNMENT; SUBCONTRACTING

The Contractor shall not assign or transfer any rights, privileges, obligations or other interest under this Agreement, including any claims for money due, without the prior written consent of the City. The Contractor shall not subcontract any portion of the services to be performed under this Agreement without the prior written approval of the City.

11. RELEASE

The Contractor, upon acceptance of final payment of the amount due under this Agreement, releases the City, its officers and employees, from all liabilities, claims and obligations whatsoever arising from or under this Agreement. The Contractor agrees not to purport to bind the City to any obligation not assumed herein by the City unless the Contractor has express written authority to do so, and then only within the strict limits of that authority.

12. INSURANCE

A. The Contractor, at its own cost and expense, shall carry and maintain in full force and effect during the term of this Agreement, comprehensive general liability insurance covering bodily injury and property damage liability, in a form

and with an insurance company acceptable to the City, with limits of coverage in the maximum amount which the City could be held liable under the New Mexico Tort Claims Act for each person injured and for each accident resulting in damage to property. Such insurance shall provide that the City is named as an additional insured and that the City is notified no less than 30 days in advance of cancellation for any reason. The Contractor shall furnish the City with a copy of a Certificate of Insurance as a condition prior to performing services under this Agreement.

B. Contractor shall also obtain and maintain Workers' Compensation insurance, required by law, to provide coverage for Contractor's employees throughout the term of this Agreement. Contractor shall provide the City with evidence of its compliance with such requirement.

C. Contractor shall maintain professional liability insurance throughout the term of this Agreement providing a minimum coverage in the amount required under the New Mexico Tort Claims Act. The Contractor shall furnish the City with proof of insurance of Contractor's compliance with the provisions of this section as a condition prior to performing services under this Agreement.

13. INDEMNIFICATION

The Contractor shall indemnify, hold harmless and defend the City from all losses, damages, claims or judgments, including payments of all attorneys' fees and costs on account of any suit, judgment, execution, claim, action or demand whatsoever arising from Contractor's performance under this Agreement as well as the performance of Contractor's employees, agents, representatives and subcontractors.

14. NEW MEXICO TORT CLAIMS ACT

Any liability incurred by the City of Santa Fe in connection with this Agreement is subject to the immunities and limitations of the New Mexico Tort Claims Act, Section 41-4-1, et. seq. NMSA 1978, as amended. The City and its "public employees" as defined in the New Mexico Tort Claims Act, do not waive sovereign immunity, do not waive any defense and do not waive any limitation of liability pursuant to law. No provision in this Agreement modifies or waives any provision of the New Mexico Tort Claims Act.

15. THIRD PARTY BENEFICIARIES

By entering into this Agreement, the parties do not intend to create any right, title or interest in or for the benefit of any person other than the City and the Contractor. No person shall claim any right, title or interest under this Agreement or seek to enforce this Agreement as a third party beneficiary of this Agreement.

16. RECORDS AND AUDIT

The Contractor shall maintain, throughout the term of this Agreement and for a period of three years thereafter, detailed records that indicate the date, time and nature of services rendered. These records shall be subject to inspection by the City, the Department of Finance and Administration, and the State Auditor. The City shall have the right to audit the billing both before and after payment. Payment under this Agreement shall not foreclose the right of the City to recover excessive or illegal payments.

17. APPLICABLE LAW; CHOICE OF LAW; VENUE

Contractor shall abide by all applicable federal and state laws and regulations, and all ordinances, rules and regulations of the City of Santa Fe. In any action, suit or legal dispute arising from this Agreement, the Contractor agrees that the

laws of the State of New Mexico shall govern. The parties agree that any action or suit arising from this Agreement shall be commenced in a federal or state court of competent jurisdiction in New Mexico. Any action or suit commenced in the courts of the State of New Mexico shall be brought in the First Judicial District Court.

18. AMENDMENT

This Agreement shall not be altered, changed or modified except by an amendment in writing executed by the parties hereto.

19. SCOPE OF AGREEMENT

This Agreement incorporates all the agreements, covenants, and understandings between the parties hereto concerning the services to be performed hereunder, and all such agreements, covenants and understandings have been merged into this Agreement. This Agreement expresses the entire Agreement and understanding between the parties with respect to said services. No prior agreement or understanding, verbal or otherwise, of the parties or their agents shall be valid or enforceable unless embodied in this Agreement.

20. NON-DISCRIMINATION

During the term of this Agreement, Contractor shall not discriminate against any employee or applicant for an employment position to be used in the performance of services by Contractor hereunder, on the basis of ethnicity, race, age, religion, creed, color, national origin, ancestry, sex, gender, sexual orientation, physical or mental disability, medical condition, or citizenship status.

21. SEVERABILITY

In case any one or more of the provisions contained in this Agreement or

any application thereof shall be invalid, illegal or unenforceable in any respect, the validity, legality, and enforceability of the remaining provisions contained herein and any other application thereof shall not in any way be affected or impaired thereby.

22. NOTICES

Any notices required to be given under this Agreement shall be in writing and served by personal delivery or by mail, postage prepaid, to the parties at the following addresses:

City of Santa Fe:
Thomas Williams
IT Division
P.O. Box 909
Santa Fe, NM 87504

Contractor:
CAaNES, LLC
7801 Academy Rd. NE
Building 1, Suite 202
Albuquerque, NM 87109

IN WITNESS WHEREOF, the parties have executed this Agreement on the date set forth below.

CITY OF SANTA FE:



ROBERT ROMERO,
CITY MANAGER

DATE: 5-24-12

ATTEST:

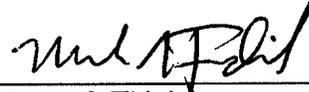

YOLANDA Y. VIGIL
CITY CLERK

CONTRACTOR:
CAaNES, LLC

APPROVED AS TO FORM:



GENO ZAMORA, CITY ATTORNEY
5/18/12

By: 

(Name & Title)
Mark J. Fidle
Title: President

Date: 11 June 2012
CRS#03079518004
City of Santa Fe Business
Registration # 12-00102385

APPROVED:



DR. MELVILLE L. MORGAN, FINANCE DIRECTOR
5/22/12

32784.510300
Business Unit Line Item

CAANES, LLC

Information Security Posture
Assessment

Penetration Testing

&

Regulatory Compliance Mapping
and Analysis



January 6, 2012

CAaNES, LLC™
7801 Academy Rd NE
Building 1, Suite 202
Albuquerque, NM 87109
info@caanes.com
(505) 217-9422 (Main)
(505) 212-0084 (Fax)

Primary Contact:
Mark Fidel
President
mfidel@caanes.com
(505) 241-9669

Contact Information

Customer		City of Santa Fe	
CAaNES Project Executive		Customer Project Executive	
Name:	Srinivas Mukkamala	Name:	Thomas Williams
Address:	CAaNES, LLC™ 7801 Academy Rd NE Building 1, Suite 202 Albuquerque, NM 87109		2651 Siringo Road Building F Santa Fe, NM 87504
Telephone:	505.948.4305	Telephone:	505- 955-5580
Fax:		Fax:	505-955-5581
E-Mail:	smukkamala@caanes.com	E-Mail:	tjwilliams@santafenm.gov
CAaNES Billing/Accounts Payable		Customer Billing/Accounts Receivable	
Name:	Donna Smith	Name:	Same as Above
Address:	CAaNES, LLC™ 7801 Academy Rd NE Building 1, Suite 202 Albuquerque, NM 87109	Address:	
Telephone:			
Fax:			
E-Mail:	dsmith@caanes.com		
CAaNES Organization Information			
Name:	Computational Analysis and Network Enterprise Solutions LLC		
Address:	CAaNES, LLC™ 7801 Academy Rd NE Building 1, Suite 202 Albuquerque, NM 87109	NM Tax ID	03079518004
		NM State Purchasing ID	63360
		NM Statewide Price Agreement	10-000-00-00051 AI
Telephone:	505-217-422	Federal FIN	20-5491219

Table of Contents

Transmittal Letter	15
Introduction	Error! Bookmark not defined.
PROPOSAL	18
1. Information Security Posture Assessment Methodology	18
2. Regulatory Compliance Assessment	20
3. Infrastructure and Technical Controls Assessment	22
4. Application Security Posture Assessment	27
4.1.....	Application Penetration Testing 29
5. Overview of Analytical Tools Used to Conduct Assessment	35
6. Recommendations and Road Map to Achieve Baseline	
Security	37
7. Detailed SOW Deliverables	39
8. Pricing	46

9. Project Team 47

January 6, 2012

Transmittal Letter

Dear Mr. Thomas Williams:

Computational Analysis and Network Enterprise Solutions, LLC® (CAaNES™) is pleased to submit a proposal to City of Santa Fe (CSF-NM) to conduct an Information Security Posture Assessment, Penetration Testing, and a Regulatory Compliance Analysis (HIPAA, NIST, CJIS, ISO 27001/27002, PCI (Snapshot), etc.). CAaNES, as an Independent Information Security Professional Services Provider, believes it is uniquely qualified to meet your goals for these services.

CAaNES, an Information Assurance Research as a Service company, offers independent assessments of information and critical infrastructures, focusing on the malevolent intent of adversaries. These services assist in bolstering security and mitigating damage. CAaNES assisted in securing several governmental entities, including the IT Infrastructures for over 150 public and private organizations in New Mexico, Arizona, Colorado, Nevada, Texas, and New Jersey. CAaNES also provides Incident Response during cyber emergencies and E-Discovery services to entities involved in litigation.

CAaNES cyber Strike Team™ 24/7 concept is comprised of highly qualified security researchers and practitioners assembled to provide preventative and responsive security services to critical infrastructure entities identified by the federal, state, local and private entities. The Strike Team really functions as cyber warriors offering detailed reports of critical vulnerabilities to help eliminate some of the stress that accompanies a cyber-attack, audit flags, or situations that compromise sensitive information.

In a dismal bit of news for organizations trying to protect their Applications, the latest tests on effectiveness of best application security scanners found that only 51 percent of the set of vulnerabilities were detected.

CAaNES, in our recent engagements, was able to detect critical vulnerabilities that were not detected by automated scanning tools. CAaNES goes far beyond automated testing, uses its proprietary framework **AppSploit™** to overcome limitations of automated scanning tools and where automated testing fails to make its mark. CAaNES performs manual testing to test security standards followed in every aspect of a web application; ranging from its internal logic control flow to any existing misconfiguration issues.

CAaNES was one of the first teams in the world to launch a **fragmented RFID malware** that would exploit vulnerabilities in middleware, embedded control systems, and penetrate heavily defended networks. CAaNES performs extensive research on Malware synthesis and analysis and has developed proprietary algorithms that help detect rapid variants which go undetected by most current antivirus technologies.

CAaNES proprietary algorithm Behavioral based Risk Analysis of Vicious Executables (BRAVE™) produces a matrix of similarity scores that can be utilized to determine the likelihood that a piece of code or binary under inspection contains a particular malware or malware variant.

BRAVE™ functionally classifies malware and malicious code by using well-known computational intelligent techniques that goes undetected by traditional security tools and antivirus scanners. MVP results (data mined data from the scanners) will be used by BRAVE to identify malware patterns (vulnerable service | port - protocol | payload) and determine likelihood of a malware and persistent threats.

The following are selected areas of expertise we have highlighted for your consideration:

- Vulnerability Security Assessment and Penetration Testing
- Regulatory and Compliance Assessments and Analysis
- Web Application Security Assessment and Penetration Testing
- Data Mining for Vulnerable Patterns from Complex and Large Scale Networks
- Semantic Web and Blog Mining
- Cloud and Virtual Security Assessment
- Electronic Discovery and Digital Forensics
- Malware Synthesis and Analytics
- Incident Response

For all the identified risks and vulnerabilities identified through our scanning and analysis tools (User | Application | System | Network | Compliance) we follow a four prong approach to measure the risk:

- **Network/System Level:** Port | Protocol | Service (P | P | S) Attack Payload
- **Web/Applications:** Port | Protocol | Service (P | P | S) Script

A vast majority of vulnerabilities found in applications are low hanging fruit for malicious code writers. These vulnerabilities are introduced through poor programming practices or developers are under pressure to bring custom applications online quickly and security can suffer in the process. Most of these vulnerabilities are independent of the programming language used. When applications are not tested and validated sufficiently, they can be left vulnerable to exploitation by both internal and external adversaries.

While other consulting firms will have experience in these areas, we believe that we have a unique level of expertise and world class research that keeps us ahead of the latest threats, adversaries, and malware. CAaNES leverages its access to New Mexico Tech (ICASA) and several other highly qualified professionals from NSA/DHS - CAE-R's (**Information Assurance Centers for Academic Excellence and Research**).

80% of our staff is trained in Information Assurance and has extensively published and practiced Information Assurance. Most of our staff members have received either Masters or Doctoral Degrees from

CAE-R's. Dr. Mukkamala, our proposed Project Director for this assessment, has published over 120 peer-reviewed publications in cyber-security.

Please feel free to contact me or Dr. Mukkamala, our CTO, to discuss any questions you may have. I can be reached at (505) 241-9669 or mfidel@caanes.com, and Dr. Mukkamala can be reached at (505) 948-4305 or smukkamala@caanes.com.

Sincerely,



Mark J. Fidel
President, CAaNES, LLC

PROPOSAL

1. Information Security Posture Assessment Methodology

Our IT Risk Assessment Methodology enables proactive detection and remediation of security vulnerabilities. The assessment is conducted to evaluate (Technical, Operational, and Management) controls in place at the network, system, and application layers that help protect client's systems and data from unauthorized access, use and compromise.

The assessment effort is divided into four major categories:

- Regulatory Compliance Assessment,
- Infrastructure and Technical Controls Assessment,
- Application Security Posture Assessment,
- Road Map to achieve Baseline Security, and

The assessment includes the operations and technologies associated with directly defending against interruption, interception, modification, and fabrication to the client enterprise network. To ensure complete information security posture assessment the assessment includes analysis of information systems, network peripherals, information security devices, and applications. Descriptions of four major categories and an optional category are given below:

- **Regulatory Compliance Assessment:**

CAaNES conducts assessments that are based on multiple best practice frameworks including ISO27001/27002, COBIT, ITIL, Zachman, COSO, NIST, and FSAM. Our assessments are comprehensive, cost effective, and are performed in accordance with customer specified federal, state, and industry regulations which assist organizations to embed a well-defined and compliant framework into their operations

- **Infrastructure and Technical Controls Assessment:**

This is a comprehensive evaluation of current network, applications, systems, and computing environments using best practices and non-invasive methods to identify gaps within CSF-NM's computing environment. To ensure complete information security posture assessment, our team performs assessments based on 100% coverage of every device.

- **Application Security Posture Assessment:**

This is an evaluation of web applications in a distinct and customized approach based on the target web application's features. We provide an in-depth understanding of how an input changes data inside the application. We use a proprietary framework to discover multiple attack vectors by passing or

inputting data to user interfaces, network interfaces, application programming interfaces (APIs), and other places where inputs are processed.

- **Recommendations and Road Map to Achieve Baseline Security:**

CAaNES provides recommendations on how to address the identified gaps within CSF-NM regulatory, infrastructure, and applications.

We provide a detailed analysis on vulnerability/threat pairs and their impact to CSF-NM. We also provide a requirement traceability matrix to mitigate current threats and achieve baseline security for High-Impact systems.

2. Regulatory Compliance Assessment

This is a comprehensive, in-depth security posture assessment based on multiple best practice frameworks including ISO27001/27002, COBIT, ITIL, Zachman, COSO, and FSAM. Our assessments services and audits are comprehensive, cost effective, and are performed in accordance with customer specified federal, state, and industry regulations (HIPAA, NIST, CJIS, ISO 27001/27002, PCI (Snapshot), etc.) which assist organizations to embed a well-defined and compliant framework into their operations.

We utilize a segmented architecture approach for internal auditing, as shown in Exhibit 1, which employs a consistent and iterative assessment and implementation of compliance requirements into each infrastructure element. Application of this methodology encompasses the controls that are required to be implemented by federal, state, local, and industry specific regulations and guidelines. The phases defined are as follows:

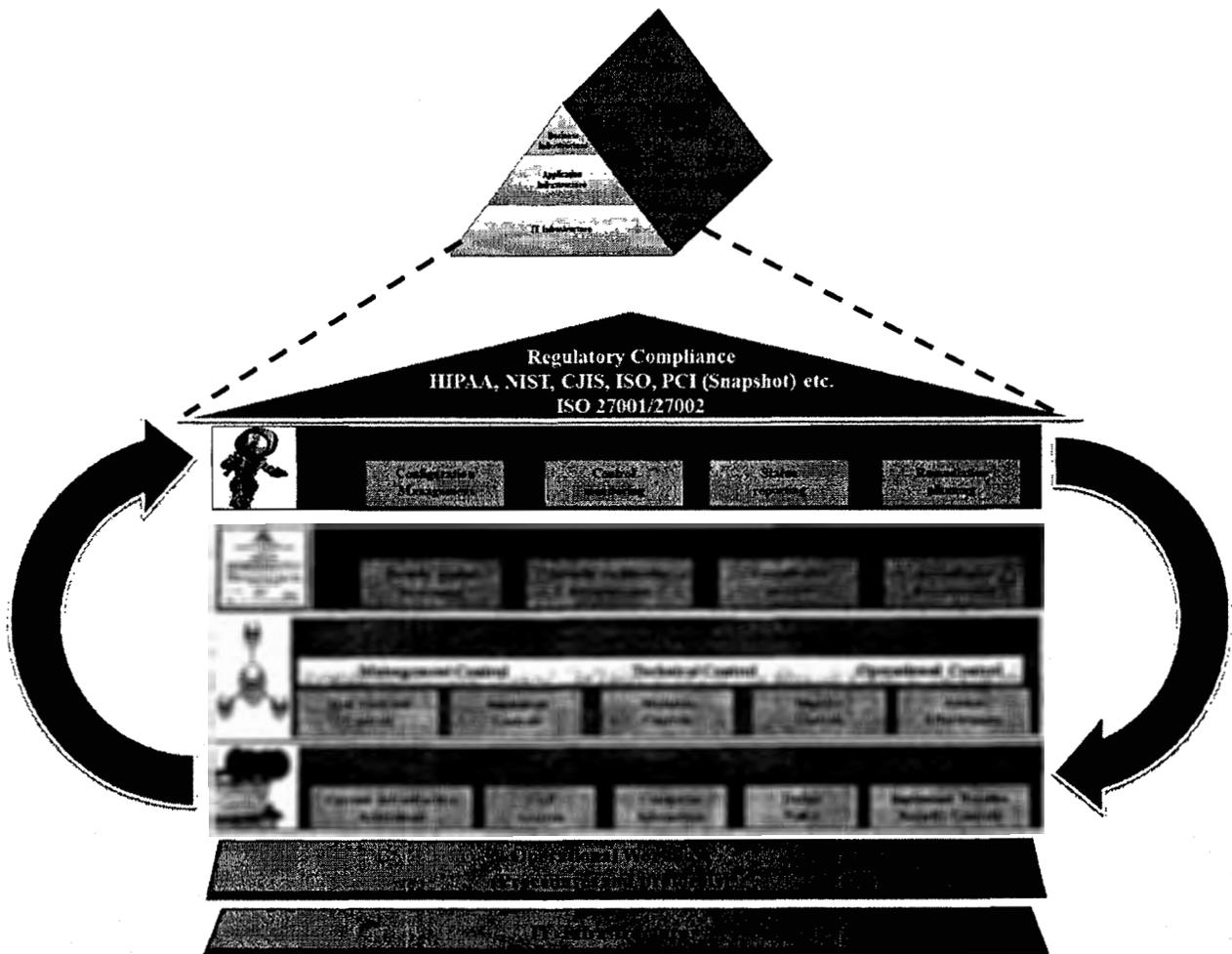


Figure 1: Segmented Architecture Approach for Security Posture Assessment

- **Determine (Compliance Strategy):** During this initiation phase, we work with an organization to identify established procedures which will be assessed. This phase is the first step in completing a strategic gap analysis. The gap analysis provides a vision of the policies and controls to be implemented to achieve required compliance levels. By the end of this phase, a security baseline is established.
- **Establish (Security Control Framework Development):** This phase defines deployment of administrative, technical and operational controls. Previously defined controls are mapped respectively, implemented and assessed for effectiveness.
- **Formalize (Certification & Accreditation):** The Certification phase evaluates the extent to which controls have been established in each of the segments and if implemented controls produce desired outcomes. This phase helps in assessing vulnerabilities and risks associated with systems and applications. The Accreditation phase provides formal authorization for the operation of system and associated applications. By the end of this phase, the risks and vulnerabilities of a system are analyzed and either eliminated or risk accepted which defines the baseline for the assessment of the system.
- **Govern (Manage & Monitor):** Implementing and maintaining regulatory compliance is a process. The management within organizations is required to demonstrate accountability and due diligence in deploying, maintaining and monitoring a compliance framework. During this phase, the continuous auditing and monitoring processes are defined and established for the system controls for the ongoing maintenance of the infrastructure.

3. Infrastructure and Technical Controls Assessment

Our assessments are based on proven, non-intrusive and patent pending methodologies and are the most comprehensive in the industry. Our experts will use proprietary tools and redundant benchmark tools to ensure cross validation and uniformity of process and consistency of results. The assessment effort will be divided into three major categories, internal, external and remote assessment.

Assessments include the operations, processes and technologies associated with directly defending against interruption, interception, modification, and fabrication to the client's network, information systems and information operations. To ensure complete information security posture assessment, our team performs assessments based on **100% coverage** of every device. Every device with an IP address will be assessed for security risks (System, Network, Application, and Compliance).

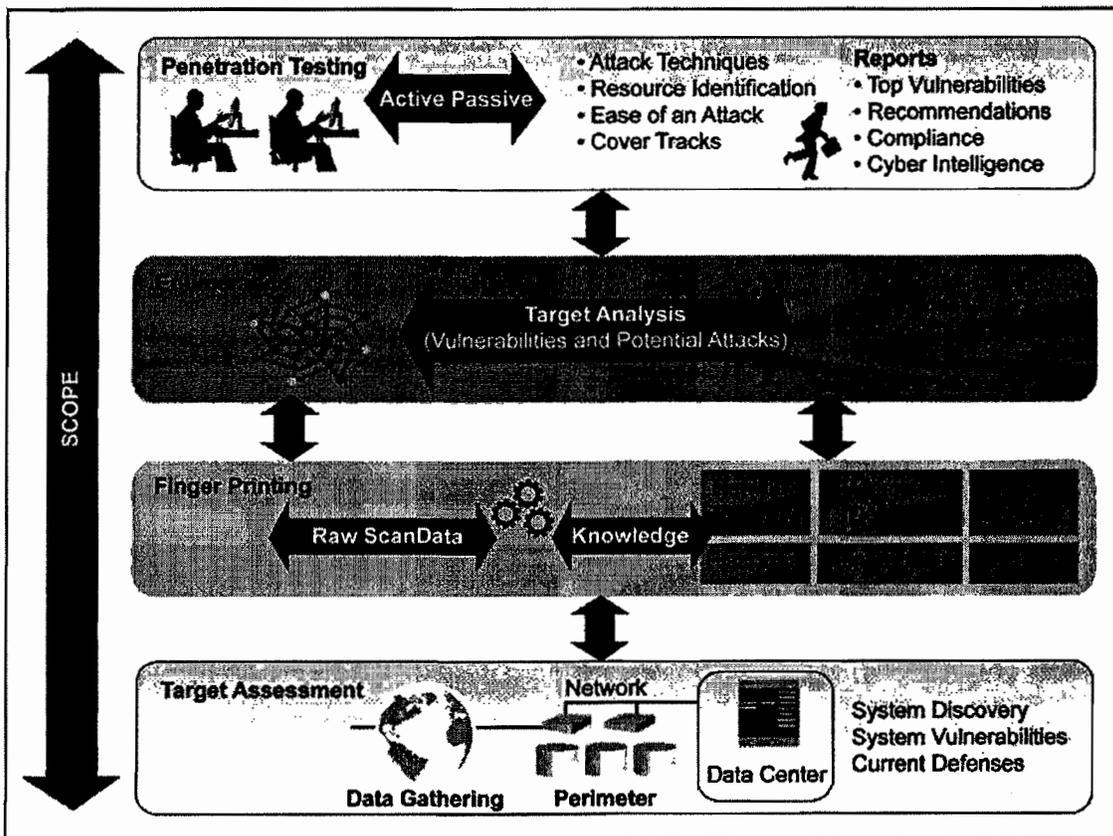


Figure 2: Strike Force Technical Controls Assessment Process and Framework

The assessment will include analysis and review of policies, applications, information systems, network peripherals, information security devices (firewalls, intrusion prevention and detection systems), remote access services, wireless access points, printers, back-up systems, log management systems, voice over IP systems, disaster recovery techniques and physical security. **Figure 2** illustrates the Strike Force Assessment Process and Framework process developed by our Team to perform assessments.

Our security assessments provide a comprehensive evaluation of current network, applications, systems, and computing environments using best practices and non-invasive methods. To ensure a complete information internal security posture assessment, the assessment will include analysis and review of information systems (core components of CSF-NM's infrastructure, routers, firewalls, desktops, and servers), network peripherals, information security devices, printers, back-up systems, log management systems, disaster recovery techniques and physical security.

CAaNES was one of the first teams in the world to launch a **fragmented RFID malware** that would exploit vulnerabilities in middleware, embedded control systems, and penetrate heavily defended networks. CAaNES performs extensive research on Malware synthesis and analysis and has developed proprietary algorithms that help detect rapid variants which go undetected by most current antivirus technologies.

Network Posture Assessment

A review of client's network architecture to determine how it effectively isolates untrusted outside networks from gaining access to client's internal, trusted networks and information.

- Review of current network architecture
- Analysis of individual nodes, servers and peripherals on the network
- Assessment of current authentication methods (user and hardware perspective)
- Network topology review and assessment of current services
- Critical node assessment for fail over analysis

Review all Communication Channels, Protocols, and Data Flow

A review of client network design and implementations to determine how effectively it isolates insiders based on their roles and need to access client's information resources

- Data flow analysis

- Assessment of physical and logical connections
- Network Assets inventory and classification
- Protocols used for communication
- Dial-in and remote connection assessments

Security Posture Assessment

A thorough review of security controls of the client covering policy, processes, procedures, people, access controls, network, communications, systems and compliance from inside, remote and outside.

- Perimeter analysis
- Internal analysis
- Wireless security assessment
- Remote connection analysis
- Remote access services and virtual private network analysis
- Application service providers and trusted networks analysis

System and Application Components Review

Detailed analysis of system and application components using automated and manual means CAaNES will test the additional components of your application presentation. This will consist of testing the following areas as applicable:

- Operating system
- Web servers
- Databases

Within each of these Web components, CAaNES will analyze and test the following security areas:

- Configuration security
- Audit logging
- Security of directory structures and volumes
- Patches and hot-fixes
- Services, ports, and protocols
- Review of endpoint security procedures (HIPS, Antivirus technologies)
- Access, password, and account controls
- Registry settings
- Other areas as necessary

Penetration Testing and Analysis

Penetration Testing - A test designed with an adversarial intent to gain unauthorized access to portions of client's network from the perspective of a trusted user and adversary from inside, remote and outside.

- Perform reconnaissance and penetration testing on the network from internal nodes, remote nodes and external nodes
- Perform analysis on possible secondary exploits
- Red teaming refers to the work performed to provide an adversarial perspective
- Perform analysis and review of remote connection services (remote access servers, virtual private networks, terminal services, etc.)

Analysis of Penetration Test performed

- Basic attack mapping analysis and attack trees
- Analysis of data integrity compromises
- Risk matrix of the discovered vulnerabilities

Virtual Infrastructure Review

A review of policies, procedures, and processes surrounding virtual infrastructure to identify gaps and mitigate risks

- Review virtual infrastructure architecture
- Uncover gaps with DISA/NIST STIGs for virtual infrastructure configuration
- Review access controls
- Review patch management and system separation
- Review virtual network segmentation
- Review logging and audit controls

Verification of Systems Security Requirements

- System access control
- Review client's access control mechanisms
- Access and review the type of software used (commercial, common operating system)
- Review logon failure procedures and policies
- Review and assess access control techniques that utilize personnel identification numbers (PIN) and passwords (or biometrics)

- Review of management controls and oversight of the function of issuing and maintaining access control to PINs and Passwords
- Monitoring and anomaly detection
- Review and assess system design for online access to client's information includes monitoring and anomaly detection capabilities
- Review, access, and test the capability of the monitoring and anomaly detection systems to detect and mitigate unauthorized access to systems and information
- Review and assess reports generated by the monitoring and anomaly detection systems

Recommendations for Security Enhancement

- Internal and external security standards and practices
- Develop requirement traceability matrix and recommend baseline user training
- Assist in developing forms and procedures for incident reporting and response
- Perimeter defense and network performance enhancement
- Map required or preferred tools to current vulnerabilities
- Recommend patches and protection mechanisms for the identified vulnerabilities
- Recommend rules for the new security technologies procured
- Recommend enhanced network architecture

4. Application Security Posture Assessment

CAaNES evaluates web applications in a distinct and customized approach based on the target web application's features. This is achieved using CAaNES' proprietary framework and industry's leading automated tools. We divide a web application security posture into two phases namely:

- Automated Testing Phase
- Manual Testing and Penetration Phase

Automated testing forms the initial layer of web application security posture and reflects black box testing of the web application. In this phase industry's leading web application vulnerability scanners are used to scan and test the web application for critical vulnerabilities. CAaNES' security consultants are proficient in training these tools based on application's architecture and compliance requirements.

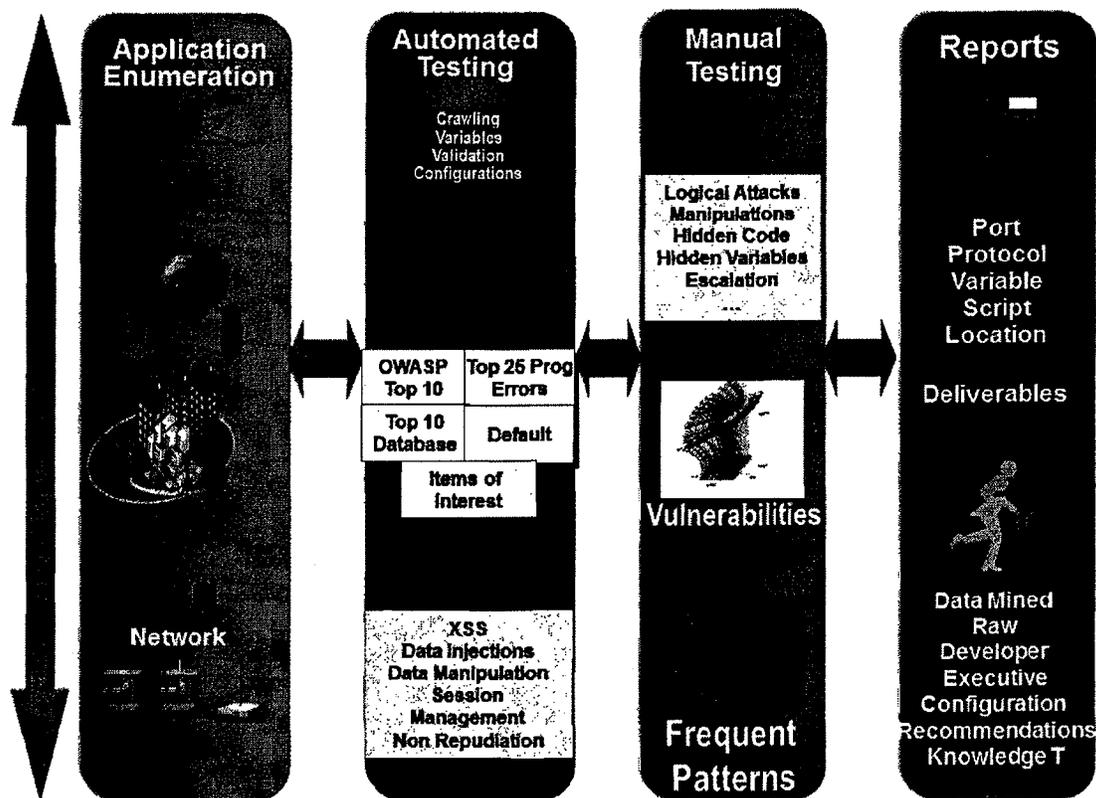


Figure 3: Proprietary Web Application Security Posture Assessment Methodology

Why go beyond automated testing?

Manual testing forays into areas where automated testing fails to make its mark. CAaNES uses its proprietary framework in this phase to overcome limitations of automated tools which CAaNES security experts have identified using their vast web application penetration testing knowledge. This phase is used to test security standards followed in every aspect of a web application; ranging from its internal logic control flow to any existing misconfiguration issues. CAaNES powered manual testing and penetration phase provides following additional features:

- **Business Logic Testing**

CAaNES security consultants analyze the existing business logic of a web application and find security flaws within the control flow of data. E-commerce and financial applications are targets of attacks, which exploit security flaws in control flow of data within the application. In this testing phase, data flow of hidden variables is analyzed and manipulated to validate security flaws while the application still meets business logic requirements.

- **Privilege Escalation (Grey box testing)**

Target web applications are tested for privilege escalation in which CAaNES security consultants login to the application using a least privileged user account, try to escalate user access level by identifying insecure direct object references and gain access to data items that are restricted to users with higher privilege access levels. During this testing phase, session controls of the application are also validated and session hijacking is performed to gain privilege escalation.

- **Virtual Directory Crawling**

Automated scanners have a serious limitation in crawling virtual directories configured for a web application. Since the virtual directory is not being crawled, all web pages and data within the virtual directory is omitted for testing during the automated phase. CAaNES detects existing virtual directories within a web application and crawls using its proprietary framework **AppSploit** and performs vulnerability testing on pages and data within virtual directory.

- **Web 2.0 Vulnerabilities**

Emerging web 2.0 technologies have increased the leverage users have on web applications. Applications built using web 2.0 technologies like AJAX (Asynchronous JavaScript and XML) enable

users to upload and change content existing on web applications. These technologies are capable of querying web service related data directly from the back end.

Considering these advances in web applications, CAaNES consultants test for vulnerabilities related to web 2.0 like AJAX injections and XML injections using proprietary scripts. This stage is used to analyze security standards of different APIs communicating with the target web application.

- **Complex Vulnerability Demonstration**

Automated scanners might find and report vulnerabilities existing in a web application, but they often fail to project the true criticality of these vulnerabilities. CAaNES security consultants combine vulnerabilities found during the automated phase and manual phase, explore and integrate multiple attack vectors possible to prove existence of more complex and critical vulnerabilities in the target web application.

- **Database Vulnerabilities**

CAaNES security consultants detect databases that interact with target web applications and try to penetrate into respective back end databases by exploiting vulnerabilities existing in the database. Web application is used as interface while penetrating into the database. This goes beyond SQL injections performed by automated tools since CAaNES security consultants insert executable code to penetrate into back end database.

- **Security Misconfigurations**

CAaNES security consultants analyze and review the directory structure of a web application based on crawling results obtained during automated testing and virtual directory crawling. This testing stage is used to validate permissions assigned to directories and files within. Communication channels used by the web application are tested for encryption standards.

4.1 Application Penetration Testing

Application penetration testing attack modules consist of payloads that belong to one or more of the four major attack taxonomies (interruption, interception, modification, and fabrication). Attack payloads that exploit common categories of application vulnerabilities are listed below.

Automated Testing

Automated testing is sometimes conducted concurrently with discovery. The automated testing process includes common, off-the-shelf tools, freeware and CAaNES-developed code. Several different scanners and tools are used to ensure that the maximum quantities of vulnerabilities are discovered and that no oversights occur.

The automated testing process is routinely run in an iterative fashion, and each iteration expands upon previously discovered issues. Automated testing is used to determine a baseline and to help the consultant locate potential threat vectors that may require additional manual testing. Automated testing features are highlighted in the following chart .

Automated Testing Features		
Data Injection and Manipulation	Sessions and Authentication	Server and General HTTP
<ul style="list-style-type: none"> • Reflected Cross-Site Scripting (XSS) • Persistent XSS • Cross-site Request Forgery • SQL Injection • Blind SQL Injection • Buffer Overflows • Integer Overflows • Log Injection • Remote File Include Injection • Server Side Include (SSI) Injection • Operating System Command Injection • Local File Include (LFI) • Custom Fuzzing • Path Manipulation - Traversal • Path Truncation 	<ul style="list-style-type: none"> • Session Strength • Authentication Attacks • Insufficient Authentication • Insufficient Session Expiration • Brute Force Authentication Attacks • Support For CAPTCHA • Support for Single Sign-On • Support for Two Factor Authentication Mechanisms • Secure Sockets Layer (SSL) Certificate Issues • SSL Protocols Supported • SSL Ciphers 	<ul style="list-style-type: none"> • Server Misconfigurations • Directory Indexing and Enumeration • Denial of Service • HTTP Response Splitting • Windows 8.3 File Name • DOS Device Handle DoS • Canonicalization Attacks • URL Redirection Attacks • Ajax Auditing • WebDAV Auditing • Web Services Auditing • File Enumeration • Information Disclosure • Directory and Path Traversal

	Supported <ul style="list-style-type: none"> • Password Auto Complete • Cookie Security 	<ul style="list-style-type: none"> • Spam Gateway Detection • Known Application and Platform Vulnerabilities • Detects Dangerous HTTP
--	---	--

Manual Testing

The ever-changing landscape of technology makes automated scanners difficult to keep updated. Based on the output from the automated testing tools, CAaNES' consultants use their expertise to analyze all potential threats and to conduct proof-of-concept testing where appropriate.

To ensure that the deepest possible analysis is conducted on every engagement, our consultants execute numerous manual-testing processes. These processes use publicly available tools coupled with CAaNES-created code to identify as many issues as possible.

Data Injection and Manipulation	Sessions and Authentication	Server and General HTTP
<ul style="list-style-type: none"> • SQL injections • Blind SQL Injections • Translate Encoding Standards • Regex Editing • SOAP Editing • Web Fuzzing/Buffer overflow check 	<ul style="list-style-type: none"> • Brute Force authentications • Cookie crunching 	<ul style="list-style-type: none"> • HTTP Request/Response monitoring • HTTP/HTTPS Requests Editing • Mapping applications to ports • Server Analysis

• Injection Flaws

Injection flaw is the exploitation of a vulnerability that is caused when code is injected into a program/script from an external source for execution. The results of code injection can be disastrous; as it can compromise the entire security posture of an enterprise by affecting the security of web applications that can be extended to critical servers. Code injection is actively used by automated attacks and computer worms to propagate.

• Cross Site Scripting (XSS)

A vulnerability that occurs whenever an application takes data that is originated from a user or program and sends it to the browser without validating or encoding the data. An exploited XSS vulnerability can be used by adversaries to bypass access controls, hijack user sessions, deface web sites, insert hostile content, and conduct phishing attacks. XSS attacks are written in a markup language (HTML or XHTML) or client-side scripting language (Java script, Jscript, ActiveX, VB script, flash, and Action script). Most of the document recent security incidents occurred because of the presence of XSS vulnerabilities.

- Document Object Model XSS (DOM based) Vulnerabilities
- Non-Persistent Vulnerabilities
- Persistent Vulnerabilities

- **Insecure Direct Object Reference**

Direct object reference is a file that contains a reference to another object such as a file, directory, database record, and URL or form parameter. Insecure direct object reference occurs when a developer exposes to an internal implementation object and provides access without checking for proper authentication credentials.

- Null Byte Injection

- **Cross-Site Request Forgery**

A web based exploit that occurs when malicious or unauthorized commands or data is sent to a web application on behalf of a trusted user without the trusted user's knowledge or consent. Cross-site forgery exploits the trust that a web application has for a particular user.

- Automatic HTTP Request Execution
- Web Application Performing Security Sensitive Operations without User Validation

- **Canonicalization**

Gaining access to restricted portions of a web application by overcoming its weak canonical rules, using insufficient security validation and sanitization of user-supplied inputs.

- Directory Traversal
- Access to Restricted Pages

- **Additional Testing**

Apart from (Injection Flaws, Cross Site Scripting (XSS), Insecure Direct Object Reference, Cross Site Request Forgery,

and Canonicalization) we also test the following exploitable vulnerabilities:

- Information Leakage and Improper Error Handling
- Broken Authentications and Session Management
- Insecure Cryptographic Storage and Weak Ciphers and Session Keys
- Insecure Communications (clear text protocols like Telnet and FTP for sensitive data)
- URL Access
- Regular Expression Checks
- Tainted Parameters
- Header Integrity
- Path Manipulation
- Thread Safety
- Hidden Form Field Manipulation
- Fail Open Authentication
- Weak Session Cookies
- Misconfigurations
- Weak Passwords

- **Detailed Analysis of Application Components**

Using automated and manual means CAaNES will test the additional components of your application presentation. This will consist of testing the following areas as applicable

- Operating System
- Web Servers
- Data Bases

- **Privileged Testing**

Application testing is first conducted with minimal to zero knowledge of your environment, processes, or applications. To be comprehensive in testing, we must consider the capabilities that an authorized user on the systems may have. As such, we will use authorized user accounts - normally a representation of 2-3 user roles - to test what an authorized user may accomplish. This will be primarily a manual exercise and we look to test, at a minimum, the following:

- Authorized User's Ability to Elevate Privileges
- Authorized User's Ability to View Other User/Account Data

- Authorized User's Ability to Add/Modify/Delete Other Account Data
- Authorized User's Existing Access is Appropriate Based Upon Role

Common Tools

Application security assessments are very dynamic in nature and use a wide variety of tools. The following is a sample list of tools that are commonly used during this type of engagement. The specific demands of a test may necessitate additional tools or code to be created.

<ul style="list-style-type: none"> • NTO Spider • Acunetix 	<ul style="list-style-type: none"> • CAaNES - AppSploit • Wikto 	<ul style="list-style-type: none"> • Nessus - Web Plugins • NeXpose - Web Plugins
--	---	---

5. Overview of Analytical Tools Used to Conduct Assessment

Our team is familiar with a large host of commercial, open source and proprietary IT security auditing and scanning tools. Our Team is offering the proprietary CAaNES Similarity Analysis of Malicious Executables (SAME™) tool and the CAaNES Mining Vulnerable Patterns (MVP™) tool as part of our service at no additional cost.

Behavioral based Risk Analysis of Vicious Executables (BRAVE™) functionally classifies malware and malicious code by using well-known computational intelligent techniques that goes undetected by traditional security tools and antivirus scanners.

BRAVE uses the latest vulnerability assessment techniques and a collection of proprietary algorithms to identify and report persistent malware indicators that target Confidential, Protected Health Information (PHI) and Personally Identifiable Information (PII).

MVP is a comprehensive analysis and reporting tool which was designed for providing a faster and easier way to assess network vulnerabilities; exploit the vulnerabilities assessed; generate the detailed report together with the remediation of the vulnerabilities, and produce the detailed procedures to patch the exploited vulnerabilities. This tool enables significant efficiencies and automation in producing the report describe above. The report itself is self-explanatory and is very easy to read and understand.

CAaNES **AppSploit** is another proprietary tool that we will use which runs on a laptop as a client application. AppSploit overcomes limitations of automated tools which CAaNES security experts have identified using their vast web application penetration testing knowledge. The tool will only be utilized on the Team's assessment toolkit and is not required to be installed on any End-Client information system.

Our proprietary technology employs well-developed intelligent network penetration techniques that are able to identify vulnerable information systems in a non-intrusive manner. This technique allows the security assessment to be conducted without disrupting End-Client operations or system availability.

Additional features:

- The technology creates assessment projects as sessions which are saved in the tool's database
- The Assessment users have the option to scan selected systems or a range of IP addresses
- The technology has the capability to integrate benchmark security tools and scanners by allowing users to automatically compare and contrast the results from the integrated tools
- Once the discovery and reconnaissance phase is complete, the

tool automatically correlates the vulnerabilities with the available exploits in the tool's exploit database and the penetration risks

- Each step of the complete process is logged and the details of each step are included in the comprehensive report generated by the tool

6. Recommendations and Road Map to Achieve Baseline Security

After each individual test is performed, the team will provide a verbal summary of the security test performed. Every evening, all of work will be verbally summarized to the client. If a critical security issue is discovered, our team will immediately notify the client and work with them to mitigate risk

At the completion of the assessment, the team provides a report containing summary and detailed information on the findings. The documentation covers the technical and business risk results of the performed tests, a high level executive overview of the findings, the recommendations of corrective actions and a detailed prioritization of those actions. Additionally, CAaNES' consultants use this phase to discuss the activities performed during the assessment and all other relevant information as part of the knowledge transfer process. This process ensures that the client team has all the information they need to take action to remediate any discovered issues.

Information Generated

Our team provides a summary of the network topology, the top 5 most vulnerable machines on the network, top 5 most vulnerable segments of the network, a cyber-intelligence report that maps to the global information security trends, user privilege summary (users never logged on, users that have never changed passwords and users with weak passwords), a summary of default settings (SNMP, FTP, default user names and passwords on computing devices), a port protocol service summary, a summary of the top 25 most dangerous programming errors, and top 10 OWASP vulnerabilities.

Summary of Task Reports

After the engagement is complete, a formal presentation is given with the methodology, findings and recommendations. The full, formal, written report is provided after the presentation and includes an executive summary, web/applications report, system component report, general audit and compliance report, network assessment report and recommendations.

This scope of this project includes the delivery of two separate presentations of the findings for the following customer audiences:

- Information Technology Team
- Senior Management

Next Activities

The presentation and the detailed reports provide a prioritized list of the most critical issues and vulnerabilities that need to be addressed.

7. Detailed SOW Deliverables

1. Information Security Assessment Project Plan & Rules of Engagement

- a. This Project Plan and Rules of Engagement are formed after the contract is finalized and signed. We will schedule an initial consultant introduction via teleconference and conduct a project kickoff meeting to prepare the Project Plan.
- b. During this meeting we will address the following:
 - Stated goals of the project
 - Project scope, methodology and rules of engagement
 - Escalation procedures on each side
 - Expectations for timeline, scheduling, coordination needs, milestones and deliverables
 - Areas of special focus or interest
 - Information specific to your organization
 - Clarification or changes in scope or needs
 - Document exchange
 - Personnel and team roles and responsibilities
 - Organizational risk and security practices
- c. The Project Plan consists of major milestones associated with preparing for and executing vulnerability and penetration tests across the IT infrastructure included in the scope of the contract. The Project Plan will be discussed and finalized with the approval of the End-Client's Chief Information Security Officer, the organizational equivalent, or other point of contact specified in the contract.
- d. The Rules of Engagement is a checklist of End-Client preferences or direction associated with how certain elements of the assessment will be conducted or the exclusion of any activities that are generally performed in an assessment.
 - For example, the Rules of Engagement may identify any exclusion of testing during certain timeframes during business hours or the exclusion or limitation of testing of any specific devices on the network.
 - Once the Project Plan and Rules of Engagement are agreed to, we will schedule and commence the work.

- It is understood that there may be changes to the Project Plan or Rules of Engagement as the assessment progresses which may be caused by unforeseen circumstances such as the identification of a significant security incident.

2. Security Assessment Executive Summary

- a. The Executive Summary is a high level report of the summary findings from the assessment and is intended for senior managers. It will identify and discuss the top findings from the assessment with the highest potential for risk impact to the End-Client.

3. Security Posture Assessment Approach

- a. The assessment approach and manner in which the findings are uncovered will be described in the respective sections of the Security Posture Assessment Reports. The approach may include details such as the tool or tools used to perform the assessment and analysis performed which resulted in any specific conclusions or recommendations.

4. Security Posture Assessment Reports

- a. The Security Posture Assessment Reports provide a broad view of IT infrastructure elements and functional components with regard to their vulnerabilities associated with internal and external threats.
- b. The findings are determined through scans and penetration tests and provided detailed technical information on the vulnerabilities and remediation approaches. The elements and functional components for this report are as follows:
 - External, internal, and remote security posture
 - Network topology (external, remote and internal)
 - Desktop security
 - Wireless posture assessment
 - Virtualization security posture summary

5. Snapshot of Critical Information Security Risks

- a. This report provides a summary and ranking of the top 5 critical areas of the End-Client's IT security posture that have the greatest risks impact from an information assurance standpoint.
- b. Our risk ranking methodology presents risks as High, Medium, and Low priority based on many factors, including ease of exploitation, business criticality of the host and prevalence of the threat.
- c. Our consultants are familiar with several risk and vulnerability ranking methodologies and use them often. These include the Common Vulnerability Scoring System version 2 (CVSS v2), DREAD, Practical Threat Analysis (PTA) and others. If you would like us to focus on one of these models or your preferred model, we can usually accommodate that request.
- d. The vulnerabilities associated with the identified risks and how they may be compromised is detailed in this report. The report includes the following in terms of findings:

- Consolidated Network wide Top 5 Vulnerable Subnets
- Consolidated Network wide Top 5 Vulnerable Machines
- Consolidated SNMP Summary Report
- Consolidated anonymous FTP Summary Report
- Consolidated Unique Port Protocol Service Summary Report
- Consolidated Network wide list of IP addresses for which password does not expire

6. Penetration Testing Summary

- a. The Penetration Testing Summary provides the details of finding determined from internal and external attempts to compromise IT systems. The vulnerabilities associated with these risks and how they may be compromised is detailed in this report.

7. Web and Application Information Security Posture

- a. The Web and Application Information Security Posture report is a consolidated report includes findings from all of the web and applications scanners including the CAANES proprietary data mining analysis work.
- b. The report organizes the findings based on the OWASP Top 10 and the CWE/SANS Top 25.
- c. The Open Web Application Security Project (OWASP) is an open community that focuses on improving web application security. OWASP Top 10 is a list of the most critical web application security risks.
 - Intended first as an awareness mechanism, the Top 10 covers the most critical web application security flaws via consensus reached by a global consortium of application security experts.
 - The OWASP Top 10 promotes managing risk via an application risk management program, in addition to awareness training, application testing, and remediation.
- d. Common Weakness Enumeration (CWE)/SANS Top 25 Most Dangerous Software Errors is a list of the most widespread and critical errors that can lead to serious vulnerabilities in software.
 - They are often easy to find, and easy to exploit. They are dangerous because they will frequently allow attackers to completely take over the software, steal data, or prevent the software from working at all.
- e. Within the report, the vulnerabilities found will be categorized as High, Medium or Low risks.

8. Configurations Review Summary with Recommendations

- a. This report provides a summary of recommendations for security controls setting configurations of the various devices in the IT infrastructure found to be at risk. It includes details down to operating system control settings.

9. Summary of Critical Policies and Procedures

- a. This report provides a summary of policies and procedures which are critical to ensuring or increasing the security posture of an organization. It provides recommendations on any changes to policies such as password settings or use of IT resources which would increase security posture.
- b. The report also addresses recommendations for any changes to existing procedures or new procedures which would mitigate the potential for security risks based on roles and responsibilities of the staff performing the procedures, how they are being performed, or the discipline to ensure they are being performed consistently. Additional examples of areas addressed are:

- Access control lists on network peripherals (firewall, detection devices, etc.)
- User and system level access control procedures
- Application and operating system hardening procedures
- Procedures for access management
- Audit policies and procedures
- Electronic data management policies and procedures

10. Information Security Audit Report per standard federal institutional guidelines and best practices

- a. This report is dependent on the compliance standard being used for the assessment.
- b. This standard establishes best practices for information technology security techniques and code of practice for information security management.
- c. The report provides findings of non-compliance with established institutional or industry guidelines associated with the standard.

11. Security Technical Implementation Guides for Operating Systems and Network Devices

- a. This detailed report provides specific guidance for remediating the vulnerabilities found on network devices and computers running various operating systems.
- b. It provides the options and detailed steps and procedures for making configuration changes or patching to address the specific vulnerabilities identified in the assessment.

12. Recommendations and Executive level presentations summarizing the assessment process and results:

- a. Two presentations are prepared which summarizes of all of reports and the major findings from the assessment. They are written to an appropriate level of detail for Executive Management and for IT Staff and Division Directors.

8. Pricing

Assessment Type	Service Description	Estimated Hours/Cost	Cost
Regulatory Compliance Mapping	Identifying Gaps in Required Regulatory Compliance (HIPAA, NIST, CJIS, PCI (Snapshot), etc.) and Best Practices (ISO 27001/27002)	<ul style="list-style-type: none"> 20 Hours for Information Gathering and Interviews with Key Personnel 20 hours for Reports and Recommendations 	\$5,000
Network and System Vulnerability Assessment and Penetration Testing	Internal and External Network Vulnerability Assessment and Penetration Testing (Up to 2,500 Active IP Addresses)	Assuming 2,000 Active IP Addressable Devices	\$10,000 (Assuming 2,000 Active IPs)
Web Application Vulnerability Assessment and Penetration Testing (Automated and Manual) Internal and External	Enterprise wide - Large Web Application Security Posture Assessment and Penetration Testing (This Includes Automated and Manual Testing)	\$5,000 Per ERP Applications (Varies on the Complexity of the Application under Test)	\$10,000 (Assumption 2 Enterprise Applications)

CAaNES, at the client's discretion, will provide a follow-up visit in 3 to 6 months to evaluate improvements. Such a visit will include 4 hours at no charge. Additional hours will be billed at \$135/hour.

9. Project Team

Our approach to staffing is to assemble a highly-skilled group of consultants to deal with the variety of specialties and tasks that must be performed during the course of the project. Our security assessment team is comprised of seasoned professionals with solid backgrounds in IT security audits, penetration testing, operations assessments, information systems evaluations, auditing, network configuration reviews, disaster recovery planning, project management, and implementation assistance.

The team for this engagement will be organized in a hierarchy that defines responsibilities by each individual and provides oversight to all members. Specialists are given roles that match their qualifications and experience. Accordingly, each individual on the team is assigned certain tasks and responsibilities, and given authority and oversight to ensure proper review and management of work performed.

CAaNES provides staff continuity at all phases of the project by balancing workloads and ensuring there is sufficient coverage for each member of our project team. This is accomplished through a combination of factors:

- First, staff schedules are carefully monitored so that conflicts do not arise that pull people away from a project
- Second, multiple people are assigned to individual tasks and support each other throughout the project
- Third, since each consultant possesses specific specialties and experience, we emphasize cross training and diversification of knowledge at all times
- Finally, we conduct regular team meetings to communicate current issues and share information

Our team members are experts in Information Assurance, Network Security, In-depth Security Assessments and Intelligent Penetration Testing. CAaNES provides dedicated professionals who are specialized in providing robust security solutions. CAaNES performs a variety of security tasks such as network security, security posture assessments, penetration testing, incident response, malware and code analysis, knowledge mining, digital forensics and litigation support, discovery management, data management, training and research. CAaNES is uniquely positioned by leveraging the resources of the Institute for Complex Additive Systems Analysis (ICASA).

**CITY OF SANTA FE
AMENDMENT No. 1 TO
PROFESSIONAL SERVICES AGREEMENT**

AMENDMENT No. 1 (the "Amendment") to the CITY OF SANTA FE PROFESSIONAL SERVICES AGREEMENT, dated January 19, 2011 (the "Agreement"), between the City of Santa Fe (the "City") and Computational Analysis and Network Enterprise Solutions (CAaNES) (the "Contractor"). The date of this Amendment shall be the date when it is executed by the City and the Contractor, whichever occurs last.

RECITALS

A. Under the terms of the Agreement, Contractor has agreed to provide system and network hardening and malware removal services to the City.

B. Pursuant to Article 18 of the Agreement, as amended, and for good and valuable consideration, the receipt and sufficiency of which are acknowledged by the parties, the City and the Contractor agree as follows:

1. SCOPE OF WORK.

Article 1 of the Agreement is amended to add the following Scope of Work so that Article 1, paragraph C reads in its entirety as follows:

C. System and Network Hardening and Malware Removal more particularly described in Exhibit "A" attached hereto and incorporated herein.

2. COMPENSATION.

Article 3, paragraph A of the Agreement is amended to increase the amount of compensation by a total of twenty thousand dollars (\$20,000) so that Article 3, paragraph

A reads in its entirety as follows:

A. The City shall pay to the Contractor in full payment for services rendered and deliverables a sum not to exceed forty thousand dollars (\$40,000), plus applicable gross receipts taxes.

3. AGREEMENT IN FULL FORCE.

Except as specifically provided in this Amendment, the Agreement remains and shall remain in full force and effect, in accordance with its terms.

IN WITNESS WHEREOF, the parties have executed this Amendment No.1 to the City of Santa Fe Professional Services Agreement as of the dates set forth below.

CITY OF SANTA FE:

By: Robert Romero
ROBERT ROMERO, CITY MANAGER

Date: 3-22-11

ATTEST:

Yolanda Y. Vigil
YOLANDA Y. VIGIL, CITY CLERK

CONTRACTOR:
CAaNES

M. P. ...
NAME & TITLE SENIOR MANAGER
CTO, MANAGING PARTNER

APPROVED AS TO FORM:

Date: 3/21/11

Judith ... for
GENO ZAMORA, CITY ATTORNEY

3/21/11

APPROVED:


KATHRYN RAVELING, FINANCE DIRECTOR

32758, 520300
Business Unit/Line Item

"System and Network Hardening | Malware Removal | Applications Hardening Assistance"

City of Santa Fe

**Thomas J. Williams
ITT Division Director
2651 Siringo Road
Santa Fe, NM 87504-0909**

Proposal for

Systems and Network Hardening, Applications Hardening and Malware Removal

Prepared by:

**Mark J. Fidel
Computational Analysis and Network Enterprise Solutions**

**10200 Comanche Rd NE
Albuquerque, NM 87111
(505) 948-4305
(800) 339-0140**

February 16, 2011

EXHIBIT "A"

CONTACT INFORMATION

Customer:	City of Santa Fe, New Mexico		
Address:	2651 Siringo Road Santa Fe, NM 87504-0909		
RFQ:	Information Systems and Network Hardening Applications Hardening Malware Removal		
Customer Project Manager		CAaNES Executive:	
Name:	Thomas J. Williams	Name:	Mark J. Fidel
Address:	2651 Siringo Road Santa Fe, NM 87504-0909	Address:	10200 Comanche Rd.NE Albuquerque, NM 87111
Telephone:	(505) 955-5580	Telephone:	505.241.9669
Fax:	(505) 955-5585	Fax:	505.212.0084
Email:	tjwilliams@santafenm.gov	Email:	mfidel@caanes.com

Table of Contents

1. OVERVIEW	3
2. SYSTEMS HARDENING OF PCS, SERVERS, AND PERIPHERALS ..	4
3. APPLICATION HARDENING	7
4. MALWARE (VIRUSES, WORMS, AND TROJANS) REMOVAL	8
5. DELIVERABLES.....	10
6. PRICING	11
7. CHANGE ORDERS	12
8. PROJECT ASSUMPTIONS	12
9. TERMS AND CONDITIONS.....	12
10. APPENDIX A:	13

1. Overview

CAaNES provides Information Assurance, Network Security, in-depth Security Assessments and Intelligent Penetration Testing. CAaNES provides dedicated professionals that are specialized in providing robust security solutions for City of Santa Fe NM. We perform a variety of security tasks such as Network Security, Security Posture Assessments, Penetration Testing, Incident Response, Malware and Code Analysis, Knowledge Mining, Digital Forensics and Litigation Support, Discovery Management, Data Management, Training and Research. CAaNES is uniquely positioned by leveraging the resources of the Institute for Complex Additive Systems Analysis (ICASA).

ICASA is a statutory research division of New Mexico Tech performing work on information technology, information assurance, analysis and protection of critical infrastructures as complex interdependent systems. ICASA is a Center of Academic Excellence in Information Assurance Education and Research (CAE-R/IAE) as designated by Department of Homeland Security (DHS)/National Security Agency (NSA).

CAaNES has an impressive background in Information Assurance, Network Security, Security Posture Assessments, Penetration Testing, Incident Response, Malware Analysis, Digital Forensics, and Knowledge Mining. Independently and collectively, our security subject matter experts (SME) hold numerous certifications and extensive security experience to meet the stringent requirements for the City of Santa Fe NM (CSF-NM) Network and Information Security needs.

Members of our staff have earned the following certifications:

- CNSSI-4016: National Information Assurance Training Standard For Risk Analysts
- CNSSI-4013: National Information Assurance Training Standard For System Administrators (SA)
- NSTISSI-4011: National Training Standard for Information Systems Security (INFOSEC) Professionals
- GCIA – GIAC Certified Intrusion Analyst
- GCFW - GIAC Certified Firewall Analyst
- Certified Information Systems Security Professional (CISSP)
- Cisco Certified Network Associate (CCNA)
- Cisco Certified Network Professional (CCNP)
- Cisco Certified Internetworking Expert (CCIE)
- Cisco Certified Academy Instructor (CCAI)

CAaNES has experience in performing Internal, Remote, and External Security Assessments and Penetration Testing services for several Commercial, Federal, State and Local Municipality clients. Our approach extends beyond the most common practices to include identification of vulnerabilities that may exist within applications, processes, operations, and physical infrastructure.

2. Systems Hardening of PCs, Servers, and Peripherals

CAaNES will use federal and custom security technical implementation guides (STIGs) to perform a comprehensive system hardening via a layered process that assists procuring agency to protect its information assets from internal and external security threats. Hardening process involves, but is not restricted to, removing unnecessary services, installing security patches, strengthening authentication controls and tightening access control security at the operating system level.

The Contractor will provide the following high level services and reports:

- ❖ Identify unused and unnecessary services and remove from client's mission critical machines
- ❖ Disable or remove unnecessary usernames and passwords
- ❖ Fix vulnerabilities in operation systems by applying the latest OS patches, hot fixes and updates
- ❖ Implement and enable native and inbuilt security controls and configure the systems in order to prevent unauthorized access in the form of intruders, hackers, malware and other security vulnerabilities
- ❖ Ensure that critical resources have up-to-date patches and are able to defend against known vulnerabilities in order to reduce the possibility of site outages and performance problems
- ❖ Set access control within applications/services where applicable
- ❖ Configure Access Control Lists (ACL) to eliminate inappropriately powerful rights and permissions (Least Privilege)
- ❖ Enable auditing to track important events

2.4 Operating System Hardening

CAaNES will perform a baseline systems security review (manual) of the Agency's systems to determine how effectively they are protected from gaining unauthorized access to system resources and information stored on the systems

- ❖ Review and Enable required security settings to harden systems that perform different organization roles
- ❖ Build and customize Group Policy objects (GPOs)
- ❖ Adopt least privilege to prevent unauthorized access to data, service disruption, and computer misuse
- ❖ Configure systems so access is limited to approved applications, services, and infrastructure environments
- ❖ Restricted unauthorized network access

- ❖ Strong network protection
- ❖ Restrict administrative groups such as Backup Operators and Server Operators
- ❖ Enforce stronger password requirements
- ❖ Require more strict account lockout policy
- ❖ Require more strict **User Rights Assignments** and **Security Options** policy
- ❖ Limit access to client systems across the network
- ❖ Hide systems from browse lists
- ❖ Control Windows Firewall exceptions
- ❖ Implement connection security, such as packet signing
 - Contractor will enable and implement strong access control policies for all the systems as part of the procuring agency's domain.
 - Password Policy Settings
 - Password policy settings that control the complexity and lifetime of passwords. Configure password policy settings by using Group Policy at the domain level
 - Account Lockout Policy Settings
 - Implement account lockout policy at Active Directory Domain Services (AD DS) that locks a user account. The lock prevents logon after a specified number of failed logon attempts occur within a specified period
 - Contractor will enable and implement native security options:
 - User Account Control
 - User account control reduces the exposure and attack surface of the operating system by requiring that all users run in standard user mode, even if they have logged on with administrative credentials
 - Event Log Security Settings
 - Event log records events on the system, and the security log records audit events
- ❖ Audit Policies
- ❖ Audit policies determine which security events to report to administrators to establish a record of user or system activity based on specified event categories
 - System
 - Logon/Logoff
 - Object Access
 - Privilege Use
 - Detailed Tracking
 - Policy Change

- Account Management
- Directory Service Access
- Account Logon

CAaNES will securely configure systems to minimize impact from adversaries:

- ❖ Enable automatic system updates
- ❖ Remove all unnecessary role services or features from the servers
- ❖ Remove all unnecessary applications and services from each server
- ❖ Remove any unused user accounts
- ❖ Ensure the Guest account is not enabled (it is disabled by default).
- ❖ Rename the default administrator account and establish a strong password for it
- ❖ Ensure strong password policies are enforced
- ❖ Restrict remote logons for standard user accounts
- ❖ Disable Null sessions (anonymous logons)
- ❖ Disable or remove shared administrative accounts
- ❖ Restrict the local administrators group (ideally to two members)
- ❖ Require administrators to log on interactively
- ❖ Ensure that the Everyone group has no rights to folders or shares containing sensitive data
- ❖ Remove unused shares from the server
- ❖ Remove permissions from the everyone group from any server shares

3. Application Hardening

CAaNES service provides an in-depth understanding of how an input, changes data inside the application. We use a proprietary framework to discover multiple attack vectors by passing or input data to user interfaces, network interfaces, application programming interfaces (APIs), and other places where inputs are processed.

CAaNES will perform data sanitization on City of Santa Fe's websites/applications, assist with fixing the discovered vulnerabilities, and secure coding to prevent future attacks.

- Provide fixes and assist City of Santa Fe fix identified vulnerabilities, threats and attacks to City of Santa Fe's Web applications
- Assist with Fixes and perform Analysis of Input validation and access controls
- Assist with Fixes and perform Analysis of HTML TRACE support
- Assist with Fixes and perform Analysis and review of password policies
- Assist with Fixes and perform Analysis of Known application and system vulnerabilities
- Assist with Fixes and perform Analysis of selected code for developer and implementation related vulnerabilities

4. Malware (Viruses, Worms, and Trojans) Removal

The team offers an assortment of proactive, reactive, and responsive information assurance services to organizations of all sizes with a motive of keeping adversaries at arm's length or at bay.

In the event of an incident or incident in progress our team of security experts is adept at stopping attacks in progress and mitigating impact. The team works with your organization to analyze incident data to determine the source, cause and effects of the attacks. Using our proprietary tools and analysis methods we will determine the Port | Protocol | Service | Payload used by the attack and develop customized response plans to minimize the effects of future and similar attacks.

The Team security experts will provide client's executives, managers, and information technology personnel (IT staff) with a comprehensive report on the malware type, attack vectors, eradication and prevention steps.

4.2 Malware Removal

We categorize and examine numerous malware samples in order to identify the parts that cause malicious activities. The premise of the analysis is that malware with similar functions share a common signature. We analyze and extract snippets of API sequences that appear frequently in a number of malicious samples.

❖ Analysis of Compromised Machines

- Extract information from the infected machines and the network
- Review of preliminary forensic and network analysis performed by Presbyterian Healthcare Services
- Compute hash values of executables and compare with the published values (NSRL)
- Analyze the executable or executables for which the hash values don't match

❖ Similarity Analysis of Malicious Executables (SAME)

- Apply CAaNES propriety techniques to identify malware traces
- Determine the malware type
- Analyze the payload for future prevention and containment

❖ If Required Reverse Engineering Executable or Executables of Question

- Identify the communication mechanism
- Identify the payload
- Identify command and control mechanism if possible

❖ Review all Communication Channels, Protocols, and Fata Flow

A review of client network design and implementations to determine how effectively it isolates insiders based on their roles and need to access client's information resources

- Data flow analysis
- Assessment of physical and logical connections
- Network Assets inventory and classification
- Protocols used for communication
- Dial-in and remote connection assessments

❖ **System and Application Components Review (Sampling)**

Detailed analysis of system and application components using automated and manual means CAaNES will test the additional components of your application presentation. This will consist of testing the following areas as applicable

- Operating system
- Web server
- Databases

5. Deliverables

- A. System and Network Hardening | Malware Removal executive summary
- B. Application Security Hardening and Review Report
- C. Security Technical Implementation Guides for Operating Systems and Network Devices
- D. Security Awareness, Identity Management, Social Networking, and Social Engineering Seminar
- E. Map required or preferred tools to current vulnerabilities
- F. Install patches and protection mechanisms for the identified vulnerabilities
- G. Recommendations
- H. Two separate executive presentations to review all findings with the following audiences:
 - a. Information Technology Team
 - b. Senior Management

6. Pricing

The team will consist of: CAaNES's professional staff. All the software and hardware purchased for the project with client's funds will be owned by the client.

Service Performed	No. of Hours
Application Hardening and Revalidation	40
Hardening Peripherals	40
System Hardening and Revalidation	100
Domain Server Configurations Testing	40
Report Preparation and Knowledge Transfer	20
Total No. of Hours	240

Total cost for services delivered per the terms of this Scope of Work is based on a fixed price of:

\$20,000.00 plus applicable NM Taxes

7. Change Orders

Any changes to the scope and/or assumptions will require joint written approval. This may extend the duration of the engagement and/or require additional resources, resulting in additional cost to CSF-NM.

8. Project Assumptions

- CSF-NM will assign a representative to provide project oversight and coordination of all project related tasks.
- CAaNES assigned Consultants will be provided access to current network environment. This includes physical building access and remote VPN access, with password and login credentials as needed to perform assigned tasks.

9. Terms and Conditions

- If the assigned CAaNES Consultants are asked to expand the scope defined herein, this Statement of Work may be amended or, a new Statement of Work may be created to define the expanded scope and additional costs.
- Any pricing quoted within this document is valid for thirty days from the date this document was prepared. Pricing may change if more than thirty days pass before the document is executed.
- Any descriptions of other companies' products in this proposal are provided only as a convenience to the reader. CAaNES cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.
- CAaNES will be provided access, during business hours, on reasonable notice and in conformance with all CSF-NM and other access policies. All information obtained from CSF-NM staff or through access to CSF-NM facilities or systems in connection herewith shall be treated as Confidential Information under the Agreement.
- All work that is created by the CAaNES consultants as part of the regular consulting service will be owned by CSF-NM.

10. Appendix A:

Related Representative Works:

- [1] Electronic Discovery and Information Retrieval System New Mexico Education Retirement Board
- [2] Information Security Assessment and Compliance Audit New Mexico Education Retirement Board
- [3] Infinite Visions Application Security Assessment and Role Bases Access Control Review Infinite Visions Software - Windsor Management (Arizona). Infinite Visions is used in more than 800 K-12 school districts in 29 states as well as 13 County Offices.
- [4] Information Security Assessment and Compliance New Mexico Energy Minerals and Natural Resources Department
- [5] Network and System Hardening New Mexico Workforce Solutions
- [6] Incident Response and Malware Analysis Yavapai College – Arizona (QWEST Corporation)
- [7] Network Maintenance and System Hardening New Mexico Association of Counties
- [8] Centralized Network Monitoring and Information System Hardening New Mexico District Attorneys
- [9] Information Security Assessment and HIPAA Audit Retiree Health Care Authority
- [10] Information Security Posture Assessment and Compliance Audit (HIPAA and Federal Tax Payer Information Compliance) New Mexico Human Services Department
- [11] Information Security Assessment and Compliance Audit Los Lunas Schools
- [12] Information Security Posture and Web Application Security Assessment New Mexico Workforce Solutions
- [13] External Security Assessment and Penetration Testing Bernalillo County
- [14] Information Security Posture Assessment New Mexico Department of Transportation
- [15] Information Security and Internal Audit of Financial Systems on behalf of New Mexico Legislative Finance Committee (Bernalillo School Districts, Aztec School District, Bloomfield District Schools, West Las Vegas School District, and Las Vegas City Schools)
- [16] Information Security Posture Assessment and Penetration New Mexico Association of Counties
- [17] Information Security Posture Assessment and Penetration Testing First Community Bank “Nasdaq: FSNM - First State Bancorp”
- [18] Information Security Policy for New Mexico Department of Homeland Security
- [19] Web and Application Security Assessment Colorado Human Services Department (PEAK System)
- [20] Social Network Analysis and Review “Myths and The Dark-side of Social Networking” New Mexico Department of Homeland Security and New Mexico Governor’s Public Information Office
- [21] Incident Response “ Attack Containment, Mitigation, and Prevention” New Mexico Higher Education Department
- [22] Information Security Assessment New Mexico Administrative Office of District Attorneys
- [23] Web Security Assessment of State of New Mexico Public Facing Websites
- [24] Incident Response (Attack Containment and Mitigation) New Mexico Tourism Department
- [25] Information Security Posture Assessment New Mexico Public Defenders

- [26] Information Security Posture Assessment New Mexico Department of Public Safety
- [27] Information Security Posture Assessment New Mexico Tourism Department
- [28] Application Security Assessment YES New Mexico Project Phase 1 (New Mexico Human Services and New Mexico Department of Information Technology)
- [29] Application and Information Security Posture Assessment New Mexico Judicial Information Systems Division
- [30] Application Code Review, Application and Network Posture Assessment New Mexico Secretary of State
- [31] Application and Information Security Assessment and HIPAA Compliance Mapping for New Mexico Public Regulation Commission
- [32] Information Security Posture Assessment and Secure Network Design New Mexico Higher Education Department
- [33] Security Hardening and Secure Network Design New Mexico Education Retirement Board
- [34] HIPAA Compliance Mapping and Security Hardening New Mexico Retiree Health Care Authority
- [35] Information Security Posture Assessment for New Mexico State Land Office.
- [36] Information Security Posture Assessment for New Mexico Regulation and Licensing Department.
- [37] Information Security Posture Assessment for New Mexico State Records and Archives.
- [38] Information Security Posture Assessment for New Mexico Environment Department.
- [39] Information Security Posture Assessment for the Oil and Natural Gas Administration and Revenue Database (ONGARD) Service Center.
- [40] Information Recovery, Preservation and Forensic Analysis of University of New Mexico Health Sciences (Information Systems) Cause no. D-101-CV-2008-1895 First Judicial District court of Santa Fe.
- [41] Information Security Posture Assessment for New Mexico Education Retirement Board.
- [42] Information Security Posture Assessment and Secure Network Re-design, and Installation of Computer Infrastructure at the NM All Source Intelligence Center (NMASIC) for New Mexico Department of Homeland Security.
- [43] Information Security Posture Assessment for New Mexico Retiree Health Care Authority.
- [44] Information Security Posture Assessment (policies and procedures review) for New Mexico Department of Information Technology, New Mexico Taxation and Revenue Department, and New Mexico Human Services Department .
- [45] Information Security Posture Assessment for New Mexico Economic Development Department.
- [46] Information Recovery, Preservation and Forensic Analysis of University of New Mexico Health Sciences (Information Systems) representing Brown and German and State of New Mexico Risk Management (Ishoo v. UNM, et.al. No. CV-2007-08927, CIV-06-00747).
- [47] System Hardening and Secure Network Redesign of New Mexico Taxation and Revenue Department.
- [48] Web Security Assessment for New Mexico State Domains (100 Unique Web Sites)

- [49] System Hardening, Secure Network Design and Implementation for New Mexico Taxation and Revenue Department
- [50] Information Security Posture Assessment for New Mexico Taxation and Revenue Department.
- [51] Information Security Posture Assessment for New Mexico Corrections Department.
- [52] External Information Security Posture Assessment for Bernalillo County.
- [53] Information Security Posture Assessment for New Mexico Courts (New Mexico Judicial Information Systems Division).
- [54] Information Security Posture Assessment for New Mexico Administrative Office of District Attorneys.
- [55] Incident Response and Information Security Posture Assessment for New Mexico Legislative Council Service (New Mexico Legislature).
- [56] Information Security Review and Vulnerability Analysis of State of New Mexico's Work Force Solutions Department.
- [57] Information Security Review and Vulnerability Analysis of State of New Mexico's Judicial Information Systems Division.
- [58] Information Security Analysis and Performance Analysis of New Mexico SHARE Project
- [59] Information Security Review and Assessment of First State Bank of Socorro Information Systems.
- [60] Information Security Review and Vulnerability Analysis of New Mexico Tech's Administrative Networks.
- [61] Review of Commission on Higher Education's Network and Information Systems.
- [62] Gap Analysis of Department of Public Safety Networks.
- [63] Review on State Wide Security Plan. New Mexico Legislative Finance Committee.
- [64] Security Review of Voter Registration and Election Management System (VERMS) for the New Mexico Secretary of State.
- [65] Secure Network Design and Information Assurance Recommendations, Wagon Mound School Districts.
- [66] A5021 Committee on Critical Transportation Infrastructure Protection (Transportation Research Board).
- [67] Computer and Information Science Forensics Consultant to Modrall Sperling (Eclipse Aviation)
- [68] Information Recovery, Preservation and Forensic Analysis of Albuquerque Public Schools (Networks, Servers and Desktops) representing Bannerman and Williams for Albuquerque Public Schools
- [69] Information Recovery, Preservation and Forensic Analysis of Albuquerque Public Schools (Networks, Servers and Desktops) representing Modrall Sperling
- [70] Incident Response and Forensic Analysis of New Mexico Environment Department Information Systems (Networks, Servers and Desktops)
- [71] Computer and Information Science Forensics Consultant to Modrall Sperling (Medcath)
- [72] Computer and Information Science Consultant to Mr. Prince. Consultant shall provide consulting services as such services apply to the computer and network forensic tasks related to the home

and business computers and networks of Mr. David Prince. Mr. Prince is a client of Laurence J. Brock, PC.

[73] Computer and Information Science Expert for Ron Foss, Brad Walls, and Maranatha Industries, Inc. ("Foss/Walls") for No. CV-2001-618-1 and No. CV-2000-1260-1 (N.M. 11th Jud. Dist Ct.)

[74] Neutral Computer and Information Science Expert for Cause No. CV-2004-00482 appointed by Judge Linda M. Vanzi of (N.M. 2d Jud. Dist. Ct.).

CITY OF SANTA FE
PROFESSIONAL SERVICES AGREEMENT

THIS AGREEMENT is made and entered into by and between the City of Santa Fe (the "City") and Computational Analysis and Network Enterprise Solutions (CAaNES) (the "Contractor"). The date of this Agreement shall be the date when it is executed by the City and the Contractor, whichever occurs last.

1. SCOPE OF SERVICES

- A. The Contractor shall provide the following services for the City:
- (1) Security posture assessment;
 - (2) Progress reporting procedures;
 - (3) Internal infrastructure assessment;
 - (4) External infrastructure assessment;
 - (5) Internal environment assessment;
 - (6) Web and application security posture assessment.
- B. The Contractor shall provide the following deliverables for the City:
- (1) Information security assessment plan;
 - (2) Security assessment executive summary;
 - (3) Security posture assessment approach;
 - (4) Security posture assessment reports;
 - (5) Snapshot of current information security posture;
 - (6) Snapshot of current information security;
 - (7) Penetration testing summary;

- (8) Web and application information security posture;
- (9) Configurations review summary;
- (10) Summary of crucial policies & procedures;
- (11) Information security audit as per standard federal institutions guidelines and best practices;
- (12) Security technical implementation guides for operating systems and network devices;
- (13) Security awareness, identity management, social networking, and social engineering seminar;
- (14) Recommendations;
- (15) Two separate executive presentations to review all findings with the following audiences: information technology team; senior management;

2. STANDARD OF PERFORMANCE; LICENSES

A. The Contractor represents that it possesses the personnel experience and knowledge necessary to perform the services described under this Agreement.

B. The Contractor agrees to obtain and maintain throughout the term of this Agreement, all applicable professional and business licenses required by law, for itself, its employees, agents, representatives and subcontractors.

3. COMPENSATION

A. The City shall pay to the Contractor in full payment for services rendered and deliverables a sum not to exceed twenty thousand dollars (\$20,000), plus applicable gross receipts taxes.

B. The Contractor shall be responsible for payment of gross receipts taxes levied by the State of New Mexico on the sums paid under this Agreement.

C. Payment shall be made upon receipt and approval by the City of detailed statements containing a report of services and deliverables completed. Compensation shall be paid only for services actually performed and deliverables approved and accepted.

4. APPROPRIATIONS

The terms of this Agreement are contingent upon sufficient appropriations and authorization being made by the City for the performance of this Agreement. If sufficient appropriations and authorization are not made by the City, this Agreement shall terminate upon written notice being given by the City to the Contractor. The City's decision as to whether sufficient appropriations are available shall be accepted by the Contractor and shall be final.

5. TERM AND EFFECTIVE DATE

This Agreement shall be effective when signed by the City and terminate on June 30, 2011, unless sooner pursuant to Article 6 below.

6. TERMINATION

A. This Agreement may be terminated by the City upon 30 days written notice to the Contractor.

(1) The Contractor shall render a final report of the services performed up to the date of termination and shall turn over to the City original copies of all work product, research or papers prepared under this Agreement.

(2) The City shall pay the Contractor for the reasonable value of services satisfactorily performed and deliverables, approved of and accepted, through the date Contractor receives notice of such termination, and for which compensation has not already been paid.

7. STATUS OF CONTRACTOR; RESPONSIBILITY FOR PAYMENT OF EMPLOYEES AND SUBCONTRACTORS

A. The Contractor and its agents and employees are independent contractors performing professional services for the City and are not employees of the City. The Contractor, and its agents and employees, shall not accrue leave, retirement, insurance, bonding, use of City vehicles, or any other benefits afforded to employees of the City as a result of this Agreement.

B. Contractor shall be solely responsible for payment of wages, salaries and benefits to any and all employees or subcontractors retained by Contractor in the performance of the services under this Agreement.

C. The Contractor shall comply with City of Santa Fe Minimum Wage, Article 28-1-SFCC 1987, as well as any subsequent changes to such article throughout the term of this Agreement.

8. CONFIDENTIALITY

Any confidential information provided to or developed by the Contractor in the performance of this Agreement shall be kept confidential and shall not be made available to

any individual or organization by the Contractor without the prior written approval of the City.

9. CONFLICT OF INTEREST

The Contractor warrants that it presently has no interest and shall not acquire any interest, direct or indirect, which would conflict in any manner or degree with the performance of services required under this Agreement. Contractor further agrees that in the performance of this Agreement no persons having any such interests shall be employed.

10. ASSIGNMENT; SUBCONTRACTING

The Contractor shall not assign or transfer any rights, privileges, obligations or other interest under this Agreement, including any claims for money due, without the prior written consent of the City. The Contractor shall not subcontract any portion of the services to be performed under this Agreement without the prior written approval of the City.

11. RELEASE

The Contractor, upon acceptance of final payment of the amount due under this Agreement, releases the City, its officers and employees, from all liabilities, claims and obligations whatsoever arising from or under this Agreement. The Contractor agrees not to purport to bind the City to any obligation not assumed herein by the City unless the Contractor has express written authority to do so, and then only within the strict limits of that authority.

12. INSURANCE

A. The Contractor, at its own cost and expense, shall carry and

maintain in full force and effect during the term of this Agreement, comprehensive general liability insurance covering bodily injury and property damage liability, in a form and with an insurance company acceptable to the City, with limits of coverage in the maximum amount which the City could be held liable under the New Mexico Tort Claims Act for each person injured and for each accident resulting in damage to property. Such insurance shall provide that the City is named as an additional insured and that the City is notified no less than 30 days in advance of cancellation for any reason. The Contractor shall furnish the City with a copy of a Certificate of Insurance or other evidence of Contractor's compliance with the provisions of this section as a condition prior to performing services under this Agreement.

B. Contractor shall also obtain and maintain Workers' Compensation insurance, required by law, to provide coverage for Contractor's employees throughout the term of this Agreement. Contractor shall provide the City with evidence of its compliance with such requirement.

C. Contractor shall maintain professional liability insurance throughout the term of this Agreement providing a minimum coverage the amount required under the New Mexico Tort Claims Act. The Contractor shall furnish the City with proof of insurance of Contractor's compliance with the provisions of this section as a condition prior to performing services under this Agreement.

13. INDEMNIFICATION

The Contractor shall indemnify, hold harmless and defend the City from all losses, damages, claims or judgments, including payments of all attorneys' fees and costs on account of any suit, judgment, execution, claim, action or demand whatsoever arising

from Contractor's performance under this Agreement as well as the performance of Contractor's employees, agents, representatives and subcontractors.

14. NEW MEXICO TORT CLAIMS ACT

Any liability incurred by the City of Santa Fe in connection with this Agreement is subject to the immunities and limitations of the New Mexico Tort Claims Act, Section 41-4-1, et. seq. NMSA 1978, as amended. The City and its "public employees" as defined in the New Mexico Tort Claims Act, do not waive sovereign immunity, do not waive any defense and do not waive any limitation of liability pursuant to law. No provision in this Agreement modifies or waives any provision of the New Mexico Tort Claims Act.

15. THIRD PARTY BENEFICIARIES

By entering into this Agreement, the parties do not intend to create any right, title or interest in or for the benefit of any person other than the City and the Contractor. No person shall claim any right, title or interest under this Agreement or seek to enforce this Agreement as a third party beneficiary of this Agreement.

16. RECORDS AND AUDIT

The Contractor shall maintain, throughout the term of this Agreement and for a period of three years thereafter, detailed records that indicate the date, time and nature of services rendered. These records shall be subject to inspection by the City, the Department of Finance and Administration, and the State Auditor. The City shall have the right to audit the billing both before and after payment. Payment under this Agreement shall not foreclose the right of the City to recover excessive or illegal payments.

17. APPLICABLE LAW; CHOICE OF LAW; VENUE

Contractor shall abide by all applicable federal and state laws and

regulations, and all ordinances, rules and regulations of the City of Santa Fe. In any action, suit or legal dispute arising from this Agreement, the Contractor agrees that the laws of the State of New Mexico shall govern. The parties agree that any action or suit arising from this Agreement shall be commenced in a federal or state court of competent jurisdiction in New Mexico. Any action or suit commenced in the courts of the State of New Mexico shall be brought in the First Judicial District Court.

18. AMENDMENT

This Agreement shall not be altered, changed or modified except by an amendment in writing executed by the parties hereto.

19. SCOPE OF AGREEMENT

This Agreement incorporates all the agreements, covenants, and understandings between the parties hereto concerning the services to be performed hereunder, and all such agreements, covenants and understandings have been merged into this Agreement. This Agreement expresses the entire Agreement and understanding between the parties with respect to said services. No prior agreement or understanding, verbal or otherwise, of the parties or their agents shall be valid or enforceable unless embodied in this Agreement.

20. NON-DISCRIMINATION

During the term of this Agreement, Contractor shall not discriminate against any employee or applicant for an employment position to be used in the performance of services by Contractor hereunder, on the basis of ethnicity, race, age, religion, creed, color, national origin, ancestry, sex, gender, sexual orientation, physical or mental disability, medical condition, or citizenship status.

21. SEVERABILITY

In case any one or more of the provisions contained in this Agreement or any application thereof shall be invalid, illegal or unenforceable in any respect, the validity, legality, and enforceability of the remaining provisions contained herein and any other application thereof shall not in any way be affected or impaired thereby.

22. NOTICES

Any notices required to be given under this Agreement shall be in writing and served by personal delivery or by mail, postage prepaid, to the parties at the following addresses:

City of Santa Fe:
200 Lincoln Ave.
Santa Fe, NM 87501

Contractor: CAaNES
10200 Comanche Rd. NE
Albuquerque, NM 87111

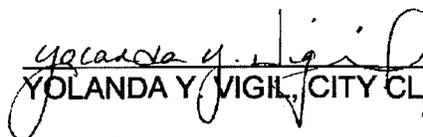
IN WITNESS WHEREOF, the parties have executed this Agreement on the date set forth below.

CITY OF SANTA FE:


ROBERT ROMERO, CITY MANAGER

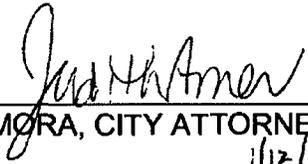
DATE: 1.19.11

ATTEST:

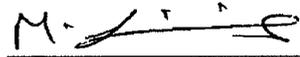

YOLANDA Y. VIGIL, CITY CLERK
JR

CONTRACTOR:
CAaNES

APPROVED AS TO FORM:



GENO ZAMORA, CITY ATTORNEY
1/12/11

By: 

Mark J. Fidel

SR# 11045 MUKKAMAAA 1/20/2011

CRS # 03079518004
City of Santa Fe Business
Registration # 11-00102385

APPROVED:



KATHRYN L. RAVELING, DIRECTOR
FINANCE DEPARTMENT



CERTIFICATE OF LIABILITY INSURANCE

OP ID: LW

DATE (MM/DD/YYYY)
11/17/10

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER The Walker Agency 1501 San Juan Blvd, Ste 201 Farmington, NM 87401 LINDA WALKER	505-326-4952	CONTACT NAME:	
	505-326-5027	PHONE (A/C, No, Ext):	FAX (A/C, No):
		E-MAIL ADDRESS:	
		PRODUCER CUSTOMER ID #:	CAANE-1
		INSURER(S) AFFORDING COVERAGE	NAIC #
INSURED [REDACTED] Mark Fidel 10200 Comanche RD NE Albuquerque, NM 87111	INSURER A : Evanston Insurance Co.		
	INSURER B : First Comp Insurance		
	INSURER C : Colorado Casualty		
	INSURER D : CNA Surety		
	INSURER E :		
INSURER F :			

COVERAGES CERTIFICATE NUMBER: REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSR	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	GENERAL LIABILITY			IT 801403	07/28/10	07/28/11	EACH OCCURRENCE \$ 1,000,000
	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY	<input checked="" type="checkbox"/>					DAMAGE TO RENTED PREMISES (Each occurrence) \$ 100,000
	<input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR						MED EXP (Any one person) \$ 10,000
	GEN'L AGGREGATE LIMIT APPLIES PER						PERSONAL & ADV INJURY \$ 1,000,000
	<input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PROJECT <input type="checkbox"/> LOC						GENERAL AGGREGATE \$ 2,000,000
							PRODUCTS - COMPROP AGG \$ 2,000,000
							\$
C	AUTOMOBILE LIABILITY			BA4002292885	12/15/10	12/15/11	COMBINED SINGLE LIMIT (Each accident) \$ 1,000,000
	<input type="checkbox"/> ANY AUTO						BODILY INJURY (Per person) \$
	<input type="checkbox"/> ALL OWNED AUTOS						BODILY INJURY (Per accident) \$
	<input type="checkbox"/> SCHEDULED AUTOS						PROPERTY DAMAGE (Per accident) \$
	<input checked="" type="checkbox"/> HIRED AUTOS						\$
	<input checked="" type="checkbox"/> NON-OWNED AUTOS						\$
							\$
							\$
	UMBRELLA LIAB						EACH OCCURRENCE \$
	<input type="checkbox"/> EXCESS LIAB						AGGREGATE \$
	<input type="checkbox"/> DEDUCTIBLE						\$
	RETENTION \$						\$
B	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY			UIC0001762-02	07/28/10	07/28/11	<input checked="" type="checkbox"/> WC STATUTORY LIMITS <input type="checkbox"/> OTHER
	ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH)		N/A				E.L. EACH ACCIDENT \$ 1,000,000
	If yes, describe under DESCRIPTION OF OPERATIONS below						E.L. DISEASE - EA EMPLOYEE \$ 1,000,000
							E.L. DISEASE - POLICY LIMIT \$ 1,000,000
A	Professional Liab			IT 801403	07/28/10	07/28/11	Prof Liab 1,000,000
D	Dishonesty Bond			16061986	12/15/10	12/15/11	Bond 100,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (Attach ACORD 101, Additional Remarks Schedule, if more space is required)
Computer forensics and security

CERTIFICATE HOLDER

CANCELLATION

To Whom It May Concern	TOWHOIT	SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.
		AUTHORIZED REPRESENTATIVE <i>Linda G. Walker</i>

© 1988-2009 ACORD CORPORATION. All rights reserved.



City of Santa Fe, New Mexico BUSINESS LICENSE

City Of Santa Fe
PO BOX 909
Santa Fe NM, 87504

Official Document
Please Post

Business Name: CAANES LLC

Location: LINCOLN AVE

Class: BUSINESS REGISTRATION-STANDARD PSA W/CTY

Comment:

Control Number: 0058823

License Number: 11-00102385

Issue Date January 06, 2011

Expiration Date December 31, 2011

CAANES LLC
10200 COMANCHE RD NE

ALBUQUERQUE NM 87111



**City of Santa Fe
Summary of Contracts, Agreements, & Amendments**

Section to be completed by department for each contract or contract amendment

1 **FOR: ORIGINAL CONTRACT** **or CONTRACT AMENDMENT**

2 Name of Contractor Computational Analysis and Network Enterprise Solutions

3 Complete information requested

Plus GRT

Inclusive of GRT

Original Contract Amount: \$20,000.00

Termination Date: June 30, 2011

Approved by Council Date: _____

or by City Manager Date: _____

Contract is for: Network security posture assessment & gap analysis

Amendment # _____ to the Original Contract# _____

Increase/(Decrease) Amount \$ _____

Extend Termination Date to: _____

Approved by Council Date: _____

or by City Manager Date: _____

Amendment is for: _____

4 **History of Contract & Amendments:** (option: attach spreadsheet if multiple amendments)

Plus GRT

Inclusive of GRT

Amount \$ 20,000.00 of original Contract# _____ Termination Date: 06/30/2011

Reason: _____

Amount \$ _____ amendment # _____ Termination Date: _____

Reason: _____

Amount \$ _____ amendment # _____ Termination Date: _____

Reason: _____

Amount \$ _____ amendment # _____ Termination Date: _____

Reason: _____

Total of Original Contract plus all amendments: \$ _____



**City of Santa Fe
Summary of Contracts, Agreements, & Amendments**

5 Procurement Method of Original Contract: (complete one of the lines)

RFP# _____ Date: _____

RFQ _____ Date: _____

Sole Source _____ Date: _____

Other Vendor initiated contact _____

6 Procurement History: None
example: (First year of 4 year contract)

7 Funding Source: ITT Professional Services **BU/Line Item:** _____

8 Any out-of-the ordinary or unusual issues or concerns:
None
(Memo may be attached to explain detail.)

9 Staff Contact who completed this form: Thomas J. Williams
Phone # 955-5580

10 Certificate of Insurance attached. (if original Contract)

Submit to City Attorney for review/signature
Forward to Finance Director for review/signature
Return to originating Department for Committee(s) review or forward to City Manager for review and approval (depending on dollar level).

To be recorded by City Clerk:

Contract # 11-0058

Date of contract Executed (i.e., signed by all parties): 1/21/11

Note: If further information needs to be included, attach a separate memo.

Comments: