

# ORIGINAL

## MEMORANDUM OF UNDERSTANDING #680-M0711

---

This Memorandum of Understanding (MOU) #680-M0711, made and entered into by and between the El Dorado County Information Technologies Department (hereinafter referred to as "County"), and the Monterey County Information Technology Department (hereinafter referred to as "Consultant");

### W I T N E S S E T H

**WHEREAS**, County has determined that it is necessary to obtain a Consultant to provide external and internal vulnerability assessments for County information systems for the Information Technologies Department; and

**WHEREAS**, Consultant has represented to County that it is specially trained, experienced, expert and competent to perform the special services required hereunder and County has determined to rely upon such representations; and

**WHEREAS**, it is the intent of the parties hereto that such services be in conformity with all applicable federal, state and local laws; and

**WHEREAS**, County has determined that the provision of these services provided by Consultant is in the public's best interest, and that these services are more economically and feasibly performed by outside independent Consultants as well as authorized by El Dorado County Charter, Section 210 (b) (6) and/or Government Code 31000;

**NOW, THEREFORE**, it is agreed as follows:

#### ARTICLE I

**Scope of Services:** Consultant agrees to furnish the personnel, equipment and services necessary to provide external and internal vulnerability assessments for County information systems for the Information Technologies Department. Services shall include be in accordance with Exhibit "A", marked "Scope of Services", incorporated herein and made part by reference hereof.

#### ARTICLE II

**Term:** This Agreement shall become effective upon final execution by both parties hereto and shall expire six (6) months from the date thereof.

### **ARTICLE III**

**Compensation for Services:** For services provided herein, County agrees to pay Consultant lump sum upon completion of services and within thirty (30) days following the County's receipt and approval of itemized invoice(s) identifying services rendered. For the purposes of this Agreement, the billing rate shall be in accordance with Exhibit "A". The total amount of this Agreement shall not exceed \$3,067.00.

### **ARTILCE IV**

**Confidentiality of Data:** All data and information relative to the County operations, which is designated confidential by the County and made available to the Consultant in order to carry out this Agreement shall be protected by the Consultant from unauthorized use and disclosure.

Permission, granted by the County, to disclose information on one occasion or at public hearing held by the County relating to the Agreement shall not authorize the Consultant to further disclose such information or disseminate the same on any other occasions.

The Consultant shall not comment publicly to the press or any media regarding this Agreement or the County's actions on the same, except to the County's staff, Consultant's own personnel involved in the performance of this Agreement, at public hearings or in response to questions from the Board of Supervisors.

The Consultant shall not issue any news release or public relations item of any nature whatsoever regarding services performed or to be performed under this Agreement without prior review of the contents thereof by the County and receipt of the County's written permission.

### **ARTILCE V**

**Ownership of Data:** County and Consultant hereby expressly agree that all plans, details, and calculations produced by Consultant, its agents, representatives, employees, or sub-contractors, shall be considered a "work made for hire" within the meaning of 17 USC Sec. 101. County shall have sole ownership of all rights, for all purposes, in each completed work, and unused portions thereof, including the copyrights.

### **ARTICLE VI**

**Changes to Agreement:** This Agreement may be amended by mutual consent of the parties hereto. Said amendments shall become effective only when in writing and fully executed by duly authorized officers of the parties hereto.

## **ARTICLE VII**

**Consultant to County:** It is understood that the services provided under this Agreement shall be prepared in and with cooperation from County and its staff. It is further agreed that in all matters pertaining to this Agreement, Consultant shall act as Consultant only to County and shall not act as Consultant to any other individual or entity affected by this Agreement nor provide information in any manner to any party outside of this Agreement that would conflict with Consultant's responsibilities to County during term hereof.

## **ARTICLE VIII**

**Assignment and Delegation:** Consultant is engaged by County for its unique qualifications and skills as well as those of its personnel. Consultant shall not subcontract, delegate or assign services to be provided, in whole or in part, to any other person or entity without prior written consent of County.

## **ARTICLE IX**

**Independent Consultant/Liability:** Consultant is, and shall be at all times, deemed independent and shall be wholly responsible for the manner in which it performs services required by terms of this Agreement. Consultant exclusively assumes responsibility for acts of its employees, associates, and subconsultants, if any are authorized herein, as they relate to services to be provided under this Agreement during the course and scope of their employment.

Consultant shall be responsible for performing the work under this Agreement in a safe, professional, skillful and workmanlike manner and shall be liable for its own negligence and negligent acts of its employees. County shall have no right of control over the manner in which work is to be done and shall, therefore, not be charged with responsibility of preventing risk to Consultant or its employees.

## **ARTICLE X**

**Fiscal Considerations:** The parties to this Agreement recognize and acknowledge that County is a political subdivision of the State of California. As such, El Dorado County is subject to the provisions of Article XVI, Section 18 of the California Constitution and other similar fiscal and procurement laws and regulations and may not expend funds for products, equipment or services not budgeted in a given fiscal year. It is further understood that in the normal course of County business, County will adopt a proposed budget prior to a given fiscal year, but that the final adoption of a budget does not occur until after the beginning of the fiscal year.

Notwithstanding any other provision of this Agreement to the contrary, County shall give notice of cancellation of this Agreement in the event of adoption of a proposed budget that does not provide for funds for the services, products or equipment subject herein. Such notice shall become effective upon the adoption of a final budget which does not provide funding for this Agreement. Upon the effective date of such notice, this Agreement shall be automatically terminated and County released from any further liability hereunder.

In addition to the above, should the Board of Supervisors during the course of a given year for financial reasons reduce, or order a reduction, in the budget for any County department for which services were contracted to be performed, pursuant to this paragraph in the sole discretion of the County, this Agreement may be deemed to be canceled in its entirety subject to payment for services performed prior to cancellation.

## **ARTICLE XII**

### **Default, Termination, and Cancellation:**

- A. Default: Upon the occurrence of any default of the provisions of this Agreement, a party shall give written notice of said default to the party in default (notice). If the party in default does not cure the default within ten (10) days of the date of notice (time to cure), then such party shall be in default. The time to cure may be extended at the discretion of the party giving notice. Any extension of time to cure must be in writing, prepared by the party in default for signature by the party giving notice and must specify the reason(s) for the extension and the date on which the extension of time to cure expires.

Notice given under this section shall specify the alleged default and the applicable Agreement provision and shall demand that the party in default perform the provisions of this Agreement within the applicable period of time. No such notice shall be deemed a termination of this Agreement unless the party giving notice so elects in this notice, or the party giving notice so elects in a subsequent written notice after the time to cure has expired. In the event of termination for default, County reserves the right to take over and complete the work by contract or by any other means.

- B. Bankruptcy: This Agreement, at the option of the County, shall be terminable in the case of bankruptcy, voluntary or involuntary, or insolvency of Consultant.
- C. Ceasing Performance: County may terminate this Agreement in the event Consultant ceases to operate as a business, or otherwise becomes unable to substantially perform any term or condition of this Agreement.
- D. Termination or Cancellation without Cause: County may terminate this Agreement in whole or in part upon seven (7) calendar days written notice by County without cause. If such prior termination is effected, County will pay for satisfactory services rendered prior to the effective dates as set forth in the Notice of Termination provided to Consultant, and for such other services, which County may agree to in writing as necessary for contract resolution. In no event, however, shall County be obligated to pay more than the total amount of the contract. Upon receipt of a Notice of Termination, Consultant shall promptly discontinue all services affected, as of the effective date of termination set forth in such Notice of Termination, unless the notice directs otherwise.

### **ARTICLE XIII**

**Notice to Parties:** All notices to be given by the parties hereto shall be in writing and served by depositing same in the United States Post Office, postage prepaid and return receipt requested. Notices to County shall be addressed as follows:

COUNTY OF EL DORADO  
INFORMATION TECHNOLOGIES  
360 FAIR LANE  
PLACERVILLE, CA 95667  
ATTN: JACQUELINE NILIUS, DIRECTOR

or to such other location as the County directs.

Notices to Consultant shall be addressed as follows:

MONTEREY COUNTY  
INFORMATION TECHNOLOGY  
DIVISION OF INFORMATION SECURITY  
1590 MOFFETT STREET  
SALINAS, CA 93905  
ATTN: TOM DUNCAN, CHIEF SECURITY AND PRIVACY OFFICER

or to such other location as the Consultant directs.

### **ARTICLE XIV**

**Indemnity:** The Consultant shall defend, indemnify, and hold the County harmless against and from any and all claims, suits, losses, damages and liability for damages of every name, kind and description, including attorneys fees and costs incurred, brought for, or on account of, injuries to or death of any person, including but not limited to workers, County employees, and the public, or damage to property, or any economic or consequential losses, which are claimed to or in any way arise out of or are connected with the Consultant's services, operations, or performance hereunder, regardless of the existence or degree of fault or negligence on the part of the County, the Consultant, subcontractor(s) and employee(s) of any of these, except for the sole, or active negligence of the County, its officers and employees, or as expressly prescribed by statute. This duty of Consultant to indemnify and save County harmless includes the duties to defend set forth in California Civil Code Section 2778.

## **ARTICLE XV**

**Insurance/Self-Insurance:** Each party, at its sole cost and expense, shall carry insurance -or self-insure - its activities in connection with this Agreement, and obtain, keep in force and maintain, insurance or equivalent programs of self-insurance, for general liability, professional liability, workers compensation, and business automobile liability adequate to cover its potential liabilities hereunder. Each party agrees to provide the other thirty (30) days' advance written notice of any cancellation, termination or lapse of any of the insurance or self-insurance coverage.

## **ARTICLE XVI**

**Interest of Public Official:** No official or employee of County who exercises any functions or responsibilities in review or approval of services to be provided by Consultant under this Agreement shall participate in or attempt to influence any decision relating to this Agreement which affects personal interest or interest of any corporation, partnership, or association in which he/she is directly or indirectly interested; nor shall any such official or employee of County have any interest, direct or indirect, in this Agreement or the proceeds thereof.

## **ARTICLE XVII**

**Interest of Consultant:** Consultant covenants that Consultant presently has no personal interest or financial interest, and shall not acquire same in any manner or degree in either: 1) any other contract connected with or directly affected by the services to be performed by this Agreement; or, 2) any other entities connected with or directly affected by the services to be performed by this Agreement. Consultant further covenants that in the performance of this Agreement no person having any such interest shall be employed by Consultant.

## **ARTICLE XVIII**

**California Residency (Form 590):** All independent Consultants providing services to the County must file a State of California Form 590, certifying their California residency or, in the case of a corporation, certifying that they have a permanent place of business in California. The Consultant will be required to submit a Form 590 prior to execution of an Agreement or County shall withhold seven (7) percent of each payment made to the Consultant during term of the Agreement. This requirement applies to any agreement/contract exceeding \$1,500.00.

## **ARTICLE XIX**

**Taxpayer Identification Number (Form W-9):** All independent Consultants or corporations providing services to the County must file a Department of the Treasury Internal Revenue Service Form W-9, certifying their Taxpayer Identification Number.

**ARTICLE XXI**

**County Business License:** It is unlawful for any person to furnish supplies or services, or transact any kind of business in the unincorporated territory of El Dorado County without possessing a County business license unless exempt under County Code Section 5.08.070.

**ARTICLE XXII**

**Administrator:** The County Officer or employee with responsibility for administering this Agreement is Jacqueline Nilus, Director, Information Technologies, or successor.

**ARTICLE XXIII**

**Authorized Signatures:** The parties to this Agreement represent that the undersigned individuals executing this Agreement on their respective behalf are fully authorized to do so by law or other appropriate instrument and to bind upon said parties to the obligations set forth herein.

**ARTICLE XXIV**

**Partial Invalidity:** If any provision of this Agreement is held by a court of competent jurisdiction to be invalid, void or unenforceable, the remaining provisions will continue in full force and effect without being impaired or invalidated in any way.

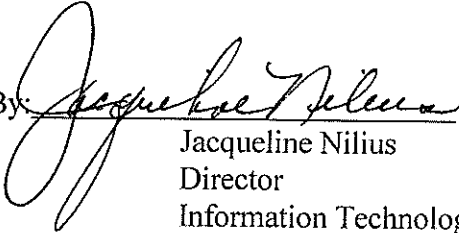
**ARTICLE XXV**

**Venue:** Any dispute resolution action arising out of this Agreement, including, but not limited to, litigation, mediation, or arbitration, shall be brought in El Dorado County, California, and shall be resolved in accordance with the laws of the State of California.

**ARTICLE XXVI**

**Entire Agreement:** This document and the documents referred to herein or exhibits hereto are the entire Agreement between the parties and they incorporate or supersede all prior written or oral Agreements or understandings.

**REQUESTING CONTRACT ADMINISTRATOR/DEPARTMENT HEAD CONCURRENCE:**

By:  Dated: 3/15/07  
Jacqueline Nilus  
Director  
Information Technologies

IN WITNESS WHEREOF, the parties hereto have executed this memorandum of understanding on the dates indicated below, the latest of which shall be deemed to be the effective date of this Memorandum of Understanding.

--COUNTY OF EL DORADO--

Dated: \_\_\_\_\_

By: \_\_\_\_\_  
Chair  
Board of Supervisors  
"County"

ATTEST:  
Cindy Keck,  
Clerk of the Board of Supervisors

By: \_\_\_\_\_

--COUNTY OF MONTEREY--

Dated: \_\_\_\_\_

By: \_\_\_\_\_  
Tom Duncan  
Chief Security and Privacy Officer  
County of Monterey  
"Consultant"



Exhibit "A"  
Scope of Services

# MONTEREY COUNTY

## INFORMATION TECHNOLOGY DEPARTMENT DIVISION OF INFORMATION SECURITY

1590 Moffett Street  
Salinas, CA 93905

(831) 796-1465  
(831) 759-6910 fax



Scope of this effort would focus on Internet (external) assessment specifically related to controls over IP addresses El Dorado County uses for browser, email, and remote services. County of Monterey Information Protection and Security (InfoSec) would test these controls by attempting to access the network from the Internet. I have not included a social engineering component; however, it is something that you may wish to consider and I believe should be part of any independent external or internal network security assessment that you undertake.

### Methodology and Approach Overview

#### *Digital Footprint*

The objective of the Digital Footprint activity is to locate data on the Internet that could assist an attacker in gaining access to the network. While some information placed in the public domain is required by law, regulation, or to assist the organization in conducting business, excess information in the public domain could result in an attacker gaining enough knowledge to conduct a social engineering or other network attack.

With no prior information about an organizations network, InfoSec will gather public information that is available to hackers. This process provides a true perspective of what information a skilled hacker can gather from public sources, and it is potentially the first step in a targeted attack. This test will provide the organization with an analysis of the extent of information available, and, where possible, how to limit information and conceal the organizations identity better. Limiting publicly available information is an essential "first line of defense", and this assessment activity should be part of any independent external network security assessment.

The following information would be gathered from public sources as part of a Digital Footprint assessment:

- Service providers for Internet access, Web Hosting, and Domain Name Service (DNS)
- Whois records
- Internet IP Address Allocation
- Domain Server records from all listed servers
- Common server (www, mail, etc.)
- Mail server (mx) Records
- Routing Summary from Public Internet exchange points
- Header information from public web servers
- Email headers, bounced mails, and read receipts from the server trails

# MONTEREY COUNTY

## INFORMATION TECHNOLOGY DEPARTMENT DIVISION OF INFORMATION SECURITY

1590 Moffett Street  
Salinas, CA 93905

(831) 796-1465  
(831) 759-6910 fax



### *External Scans*

InfoSec then compares the information in the Digital Footprint to actual systems' data. Using information that the organization provides on domain and IP ranges, InfoSec will conduct an automated test from un-trusted locations. The tests are divided into five major components:

- Port Scanning
- Service Identification
- System Identification
- Vulnerability Research and Verification
- Remediation Advice

*Port scanning* is the non-invasive probing of system ports on the transport and network level. This will identify live or accessible Internet services as well as try to penetrate the firewall(s) to find additional live systems. Testing for different protocols will depend on the system type and services it offers.

*Service Identification* is the active examination of the application listening behind the service. In certain cases more than one application exists behind a service where one application is the listener and the others are considered components of the listening application.

*System Identification* is the active probing of a system for responses that can differentiate unique systems to operating system and version level. The focus of the scan is in identification, understanding, and verification of weaknesses, mis-configurations, and vulnerabilities within a host or network.

*Testing for vulnerabilities* using automated tools is an efficient way to determine existing holes and system patch level. Manual verification, however, is necessary for eliminating false positives, expanding the hacking scope, and discovering the data flowing in and out of the network.

### **El Dorado County External Vulnerability Assessment Project**

Our testing methodology closely follows NIST Special Publication 800-42 *Guideline on Network Security Testing*. Each test assignment starts with external scoping and research to understand the Internet footprint of El Dorado County. A semi-automated

# MONTEREY COUNTY

## INFORMATION TECHNOLOGY DEPARTMENT DIVISION OF INFORMATION SECURITY

1590 Moffett Street  
Salinas, CA 93905

(831) 796-1465  
(831) 759-6910 fax



network scan is then performed. This information is used to build up a perimeter network map of each gateway tested, enabling InfoSec to apply tests appropriate to the location of each host.

The proposed project for El Dorado County consists of five phases, each designed to build upon the other;

### Phase 1 – Preparation

This phase consists of contact point determination, emergency communications channels to be used and analysis of documentation provided (maps, IP ranges, etc.)

Phase 2 – Information Gathering (Reconnaissance) includes but is not limited to the determination of;

- IP Address Range
- Owner of IP Range
- Domain Names
- Computing Platforms
- Network Architecture
- Usernames
- Physical Locations
- Active Services
- Technical Contacts
- Business Partners
- Email Addresses
- Phone Numbers
- Routes
- Internet Accessible Data
- DNS Servers
- Web Servers
- SMTP Servers
- Zones and Sub-Domains
- Firewalls and Perimeter Devices
- VPN Access Points

# MONTEREY COUNTY

## INFORMATION TECHNOLOGY DEPARTMENT DIVISION OF INFORMATION SECURITY

1590 Moffett Street  
Salinas, CA 93905

(831) 796-1465  
(831) 759-6910 fax



### Phase 3 – Network Mapping and Firewall Assessments

- Firewall tests, active machine identification and target determination
- Network mapping
- Fingerprinting
- Analysis and determination of services, targets, etc.

### Phase 4 – Vulnerability Assessment

The majority of systems connected to the Internet are at risk from 'hacker attack', due to misconfiguration, lack of security patching or network design. InfoSec's external vulnerability testing is designed to provide an examination of your internet-facing systems from the perspective of a hacker, followed up with sensible 'human-readable' reporting and steps to take to improve security.

This phase includes port scanning and vulnerability assessment tools launched against each host to identify visible services and known software limitations. This allows InfoSec and El Dorado County the ability to identify potential starting points for an attack and can give an indication of the likely success. If default software installs OR insecurely configured services are evident there's a reasonable chance that an attack can be progressed deeper into the network to reach El Dorado County's assets stored in database and file systems. For example, probing the SMTP commands available on El Dorado County's mail server. Can the mail server be forced to give up information that could be useful to an attacker? Can services other than SMTP be tunneled through port 25? Can an attacker telnet to internal machines through the mail server?

Tasks included within this phase;

- Scan of perimeter targets
- Verification of high-risk vulnerabilities found
- Web Application Testing
  - InfoSec will examine what is predominantly accessed over http or https and attempt attacks that the traditional network firewall cannot protect against.

# MONTEREY COUNTY

## INFORMATION TECHNOLOGY DEPARTMENT DIVISION OF INFORMATION SECURITY

1590 Moffett Street  
Salinas, CA 93905

(831) 796-1465  
(831) 759-6910 fax



- Application specific tests against services will be performed to include;
  - Web server assessments
  - Web site scans
  - Web application manipulation
  - SQL tests
  - Password cracking against obtained password databases
  - Enumeration
  - Other services as discovered.
- War Dialing

The objective of war dialing is to identify un-authorized modems connected to El Dorado County systems that could provide a route into the network by an attacker, that is, through any modem or RAS server discovered. This is achieved by using software to dial through the county's telephone PBX range. Once systems are identified, attempts are made to breach the underlying OS and attempt default account password logins.

While it is vital to secure your Internet perimeter, it's equally important to secure potential back-door routes into your network. Unauthorized or poorly configured modems connected to your systems could give an attacker direct access to your internal network. We will not attempt to gain access to the network through this point; however, we will flag the modem(s) so that El Dorado County can investigation and remove if appropriate.

### Phase 5 – External Vulnerability Assessment Project Deliverables

At the completion of the assessment, InfoSec will prepare a final report that will detail our findings to assist El Dorado County with an understanding of its current Internet security posture. The report will identify, prioritize, and justify remediation activities and will be presented in a formal report to include:

- Executive summary
- Statement of Work Performed
- Description of systems & flaws discovered
- A prioritized understanding of the problems
- Grading of risks from High to Low severity
- Recommendations
- Test notes where non-standard behavior has been observed

# MONTEREY COUNTY

## INFORMATION TECHNOLOGY DEPARTMENT DIVISION OF INFORMATION SECURITY

1590 Moffett Street  
Salinas, CA 93905

(831) 796-1465  
(831) 759-6910 fax



The report will be sent to El Dorado County electronically, encrypted during transit, and delivered within 7 to 10 working days from completion of the project.

*Note:* If desired, any serious High Risk security flaws discovered can be reported to El Dorado County immediately, including details of the problem and suggested remedial action.

### Further Advice

Subsequent to the report being issued, InfoSec will be available for advice and further explanation on the specific issues raised in the test and final report by e-mail and phone.

### **Schedule and Cost**

Costs listed below are based on prevailing labor rates in the County of Monterey for fiscal year 2006-07 associated with Information Technology security management and technical/analysis activities.

Objective	Est hrs.	Cost	Activity
Digital Footprint	16	\$ 1,152	Determining hosts and ports that are Internet accessible (incl. web sites).
Risk assessment	4	288	Develop list of targets in coordination w/El Dorado. Identify risks and exposure for each target
External vulnerability audit	16	1,152	Perform the external technical vulnerability audit. Analyze data and results.
Reporting	4	380	Finalize reports.
Presentation	1	95	Provide findings and recommendations
<b>Totals</b>	<b>41</b>	<b>\$ 3,067</b>	

# MONTEREY COUNTY

## INFORMATION TECHNOLOGY DEPARTMENT DIVISION OF INFORMATION SECURITY

1590 Moffett Street  
Salinas, CA 93905

(831) 796-1465  
(831) 759-6910 fax



### Resource Descriptions

InfoSec includes certified Security Professionals on our team. Team members have received formal training on the particulars of ISO/IEC 17799:2005, Forensics Analysis, Network Security Design and Engineering, Incident Response, Vulnerability Assessment and Analysis.

#### **Project Manager** - *Tom Duncan, Chief Security and Privacy Officer*

##### Professional Certifications

- CISSP Certification from (ISC)2
- CISM Certification from ISACA
- SANS GIAC Certified ISO 17799 Specialist (G7799)

##### Summary Experience

Senior level professional with strong leadership skills and extensive Business, Technology, Security and Project Management experience.

##### Experience Areas

Project Management, Strategic Planning, IT Services, IT Security, Security Policy and Strategy, Identity Management and Security Services.

#### **Security Architecture** - *Dan Kern, InfoSec Systems Programmer/Analyst III*

##### Professional Certifications

- SANS GIAC Certified Firewall and Security Architecture Specialist (GCFW)
- SANS GIAC Certified Incident Handler (GCIH)
- Member of the SANS GIAC Advisory Board

##### Summary Experience

Information Security Professional experienced in Network Security Architecture, Intrusion Detection and Analysis, Ethical Hacking and Vulnerability Analysis, Information Security Auditing, Incident Response Team Development and Management, and Staff Development.

#### **Forensics** - *Steve Lucas, InfoSec Systems Security Analyst II*

##### Certifications

- Certified Access Data Forensics Analyst (PSA)
- Degree in Data Processing

##### Summary Experience

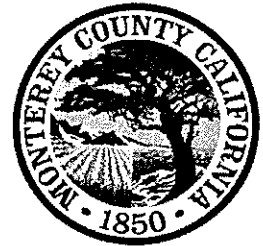
Information Systems and Security Professional skilled in Forensic Investigations including Case Creation, Examination, Analysis, and Classification of Digital Evidence; Information Security Auditing; Malware Operational Process and Procedural Development, Information Security Awareness Training and Education, Data Processing Management.

# MONTEREY COUNTY

## INFORMATION TECHNOLOGY DEPARTMENT DIVISION OF INFORMATION SECURITY

1590 Moffett Street  
Salinas, CA 93905

(831) 796-1465  
(831) 759-6910 fax



### **Technical Security** - *Nathan Wenzler, InfoSec Systems Programmer/Analyst III*

#### Professional Certifications

- SANS GIAC Security Essentials (GSEC)
- Microsoft Certified Professional (MCP)
- Microsoft Certified Systems Administrator (MCSA)
- Microsoft Certified Systems Engineer (MCSE)
- Microsoft Certified Database Administrator (MCDBA)
- QualysGuard Certified Vulnerability Management Specialist

#### **Summary Experience**

Information Systems and Security Professional skilled in Threat and Vulnerability Assessment and Mitigation, Information Security Auditing, Authentication Management, Operational Process, Procedural, and Program Development related to Security Code Correction (Patch Management) and IT Lifecycle Asset Management.