ADVANCED THREAT ANALYSIS

Elections System Security Risk Assessment

Proposal for

SAUK COUNTY

Prepared For

Sauk County
505 Broadway
Baraboo, WI 53913
Steve Pate, MIS Director
Sauk County Clerk
(608) 355-3542 (office)
(608) 355-3526 (fax)
steve.pate@saukcountywi.gov

Technical and Contractual Contact

Advanced Threat Analysis Inc.
8008 Bush Hill Court
Severn, MD 21144
Roger Colón, CEO
(443) 223-8469 (cell)
(410) 969-7509 (office)
roger.colon@atacorporation.com
https://www.atacorporation.com

October 15, 2020

October 15, 2020

Steve Pate, MIS Director
505 Broadway
Baraboo, WI 53913

Dear Mr. Pate,

Advanced Threat Analysis, Inc. (ATA) is pleased to present this technical proposal to Sauk County (the County) to provide the County with an Election System Security Risk Assessment. This proposal discusses how ATA plans to evaluate the security of the County's election system, and related policies and procedures. ATA will conduct vulnerability scanning and penetration testing of the County's internal and external systems related to the election system, and review the County's policies and procedures to identify any gaps.

ATA has proven processes and procedures to protect the County, as we have been providing end-to-end security-related services, to include virtual Chief Information Security Officer (vCISO) as-a-service, implementing the Cyber Security Framework (CSF), and conducting different types of assessments for commercial, federal, state, and local organizations.

We believe that investing in security is investing in the County's future. A secure enterprise is a profitable environment for the businesses, citizens, and employees of the County. We look forward to partnering with Sauk County to develop a plan to meet your security needs, and complete this project within your stated timeframe, meeting your security goals, and exceeding your expectations.

Respectfully,

Roger Colón, Jr.
President/CEO

Table of Contents

Advanced Threat Analysis Corporate Overview

Advanced Threat Analysis (ATA) was organized as a small business in 2012 to provide end-to-end cyber and information security services, and information assurance services to commercial organizations, federal, state, and local governments. Additionally, ATA wanted to take advantage of its eligibility to compete for Federal government contracts reserved for small businesses, owned by service-disabled veterans or minorities, or residing in and employing residents of historically underutilized business zones (HUBZone). ATA currently has **fifteen (15) consultants** supporting different types of contracts and projects. ATA is proposing to dedicate three (3) subject matter experts to deliver on this proposal: Roger Colón, Kristine Titzer, and Mohsan Farid.

ATA has been successful at implementing and securing all types of information technology (IT) at different federal and commercial organizations while providing end-to-end security to large and small organizations for almost eight (8) years, to include the same services being requested by the County. ATA **will begin the work within two weeks** of receiving an award if authorized by Sauk County. These two weeks allow ATA to plan staffing and delivery on the proposal.

As President, CEO, and sole owner of ATA, Mr. Roger Colón, a cyber security Subject Matter Expert (SME), will personally take the lead on this project as he does on many other engagements. He has over 20 years of experience in information technology and information security. He received his initial cyber-security training as a U.S. Navy Cryptologic Technician, and he has subsequently worked with the Office of Naval Intelligence, the National Security Agency, the Defense Information Systems Agency, and the Departments of Homeland Security, Treasury, Justice, and Energy. He is qualified to provide the County with end-to-end security services. He will personally oversee and conduct many of the strategic and tactical services identified in the Request for Proposal (RFP). He is a SME with all the different security frameworks and will assist in mapping any risk identified to the specific frameworks. He frequently maps risks to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, the Open Web Application Security Project (OWASP) Top 10, and Center for Internet Security (CIS) Top 20.

Organizations, such as the Sauk County, have many reasons for taking a proactive and repetitive approach to addressing information security concerns. Legal and regulatory requirements aimed at protecting sensitive or personal data, as well as public security requirements, create an expectation for organizations of all sizes to devote the utmost attention and priority to information security risks. A vulnerability assessment and/or penetration test takes on many names and can vary greatly in terms of method, rigor, and scope, but the core goal remains the same: **identify and quantify the risks to the organization's information assets**. This information is used to determine how best to mitigate those risks and effectively preserve the organization's mission. Some areas of rationale for conducting a security assessment include:

Cost justification—Added security usually involves additional expense. Since this does not generate easily identifiable income, justifying the expense is often difficult. An effective penetration test should educate key business managers on the most critical risks associated with the use of technology, and automatically and directly provide justification for security investments.

Productivity—Vulnerability assessments and penetration tests should improve the productivity of IT operations, security, and audit. By taking steps to formalize a review, create a review structure, collect security knowledge within the system's knowledge base and implement self-analysis features, the penetration test can boost productivity.

Breaking barriers—To be most effective, security must be addressed by organizational management as well as the IT staff. Organizational management is responsible for making decisions that relate to the appropriate level of security for the organization. The IT staff, on the other hand, is responsible for making decisions that relate to the implementation of the specific security requirements for systems, applications, data, and controls.

Self-analysis—Vulnerability assessment and penetration test results must always be simple enough to understand, without the need for any security knowledge or IT expertise. This will allow management to take ownership of security for the organization's systems, applications, and data. It also enables security to become a more significant part of an organization's culture.

Communication—By acquiring information from multiple parts of an organization, an enterprise vulnerability assessment and penetration test boosts communication and expedites decision making.

ATA is proposing to provide Sauk County with security-related services, to include penetration testing, vulnerability scanning, policy, and procedure review, and with a final report and recommendations for correcting any deficiencies.

Experience and Capabilities

The protection of cyber systems and the information they host is of critical importance to every organization's mission success. At ATA, our commitment is to maximize an organization's security with consistent threat monitoring programs and integrated cyber defense solutions that ensure the highest confidence that your network is defended, compliant, and monitored.

ATA focuses on different areas of security, to include Risk Management, Cybersecurity Operations, and Threat Intelligence. Broken down even further, ATA conducts:

- Security requirements selection
- Implementing security controls
- Assessing the implementation of security controls which include:
  - Security controls assessments
  - Vulnerability scanning
  - Penetration testing
- Continuous monitoring

ATA currently provides security architecture and engineering support, security controls assessments, vulnerability management, and penetration testing of federal general support systems and major applications. ATA also provides continuous monitoring for local organizations. Services provided are primarily vulnerability scanning, penetration testing, and the monitoring of security controls.

ATA provides security architecture, engineering, implementation, and vulnerability management services to a broad range of clients. Below are some of our past and current clients:

Internal Revenue Service (IRS)	Bureau of Engraving and Printing (BEP)
Veterans Affairs (VA)	Armstrong Flooring, Inc. (AFI)
M&T Bank	US Bank
EMC Corporation	DTXT Corporation
Virtustream	Lancaster Hospice and Community Care
Community First Fund	Charles County, MD

ATA's current customers include the IRS, BEP, AFI, and the VA. ATA currently provides security architecture and engineering support, security controls assessments, vulnerability management, and penetration testing of general support systems and major applications. ATA also provides continuous monitoring for local organizations to include Lancaster Hospice and Community Care, and Community First Fund. Services provided are primarily vulnerability scanning, penetration testing, and the monitoring of security controls.

ATA's Technical Response

ATA begins every assessment with a confirmation of scope. By reading Sauk County's (the County) RFP, we understand the scope to be penetration testing, vulnerability scanning, and a policy and procedure review. We have organized this proposal to align into logical groupings of assessing and conducting this assessment.

Each part of the technology infrastructure should be assessed for its risk profile. From that assessment, a determination should be made to effectively and efficiently allocate the County's time and money toward achieving the most appropriate and best employed overall security policies. The process of performing a penetration test can be quite complex and should consider secondary and other effects of action (or inaction) when deciding how to address security for the various IT resources.

Depending on the size and complexity of the County IT environment, it may become clear that what is needed is not so much a thorough and itemized assessment of precise values and risks, but a more general prioritization. Determination of how security resources are allocated should incorporate key business managers' risk appetites, as they have a greater understanding of the County' security risk universe and are better equipped to make that decision.

Each organization is different, the County is not a hospital or a federal agency, so the decision as to what kind of penetration test should be performed depends largely on you. If it is determined what your organization needs now is general prioritization, a simplified approach to a penetration test can be taken and, even if it already has been determined that a more in-depth assessment must be completed, the simplified approach can be a helpful first step in generating an overview to guide decision making in pursuit of that more in-depth assessment.

If one is unsure what kind of assessment the organization requires, a simplified assessment can help make *that determination. If one finds that it is impossible to produce accurate results in the process of completing a simplified assessment—perhaps because this process does not consider a detailed enough set of* assessment factors—this alone can be helpful in determining the type of assessment the organization needs. ATA understands the objectives of the engagement to be the following:

PENETRATION TESTING

Provide penetration testing for the County's internal and external networks with access to the County's election system.

VULNERABILITY SCANNING

Provide vulnerability scanning for the County's internal and external networks with access to the County's election system.

POLICY AND PROCEDURE REVIEW

Review the County's processes, policies, and procedures, related to those specific items identified in Part Two of the RFP, regarding the County's election system and related infrastructure.

FINAL REPORT AND RECOMMENDATIONS

Provide a comprehensive final report detailing the findings identified during the penetration testing, vulnerability scanning, and policy and procedure review. This report will include a listing of specific items identified along with suggested corrective actions.

Preliminary Activities

As soon as possible after the contract award has been communicated, a project kickoff meeting will be scheduled. The kickoff can be conducted via teleconference. During the kickoff meeting the following items are typically covered:

- Review terms of the project
- Verify project scope and deliverables
- Arrange for necessary access permissions (ID badges, system access authorization, etc.) – if needed
- Always arrange for letters authorizing the tests (to be carried by ATA consultants during the testing) – if needed
- Review the work plan to finalize the timing of external tests, on-site visits – if needed
- Agree upon reporting and communications methods
- Finalize rules-of-engagement
- Discuss anticipated impact (if any) of the testing
- Identify technical and other documents required by ATA – if needed
- Introduce client and ATA project staff and review roles
- Exchange contact information
- Discuss automated tools to be used in engagement
- Other logistics

Planning

ATA will outline the logistics of the test, expectations, legal implications, objectives, and goals the County would like to achieve. ATA will capture the planning in a Rules of Engagement or a Test Plan.

Specifically, for the penetration testing and during the planning, ATA will work with the County to fully understand any risks, the organizational culture, and the best pen testing strategy for the County. The County may want to perform a white box, black box, or gray box penetration test. It's at this stage when the planning occurs along with aligning the County' goals to specific pen testing outcomes. ATA is proposing an **"Eyes-Shut"** and **"Eyes-Open"** approach for the External and Internal networks.

This means that we will perform an examination, beginning with recon, discovery, enumeration, and scanning, from outside, through the Internet with no organization originated UserIDs or information; rather, we will operate initially utilizing only the predetermined IP ranges provided by the County to avoid disturbing other organizations. The "**Eyes-Shut**" approach is described below. Potential target hosts are identified, and screen prints taken during the testing to document the vulnerabilities identified and verified.

While "**Eyes-Shut**" testing could go on for weeks (i.e., a real hacker who wanted to penetrate the environment could spend as long as it would take to gather the information needed), from a cost/benefit standpoint, we believe a limited engagement is more appropriate. A limited engagement will still provide a realistic hacker's eye view of systems; it will *not* yield information about the obscure pathways into the systems, nor will it simulate the view that might be gained by those who already have some information (such as a disgruntled employee). It will, however, reveal many issues.

We will also request you to be cognizant of what activity your incident response team observes. We will "step up" the level of activity – from stealthy to more obvious – to try to determine how your incident prevention system works and at what level our activities are observed and we will report this information in our deliverables. To prevent being blocked from testing, we will work with those Organization staff members whom you designate.

Once the "**Eyes-Shut**" portion of the assignment is complete, typically, a second phase of the assessment begins. This is the "**Eyes-Open**," credentialed segment of the review and seeks to identify ports and services enabled on the cyber assets within the perimeter surrounding a specific County system or application. Our staff takes the perspective of an authorized user attempting to circumvent controls through the firewall. After the initial analysis with no credentials we will request a basic UserID and password, like what an employee or casual vendor might possess. Our engineers draw on information gleaned in "**Eyes-Shut**" testing and attempt to determine passwords and circumvent controls methodically as we move about the network and attempt to reach the target application, and document what can be accessed. This is completed from ATA locations. The Rules of Engagement and/or Test Plan will be developed once the proposal is approved and will include the technical details for the scope.

Exploitation of Identified Vulnerabilities

During the testing ATA will have put together a map of all possible vulnerabilities and entry points into the County' enterprise. ATA will begin to test the exploits found within the County' network, applications, and data. The goal for ATA is to see exactly how far we can get into the County' environment, identify high-value targets, and avoid any detection. Where possible, we will also seek to address the following (among other items), if they can be determined as posing as an external penetration tester:

- Implementation flaws/code bugs that could open a vector to attack downstream application software
- User authentication security
- Access control mechanisms
- Data communications integrity and confidentiality protections
- Session management protections against attacks such as man-in-the-middle, session hijacking or session replay
- Cryptographic module integrity
- Adequate input validation protections against attack
- Presence of adequate auditing/logging of system events to preserve non-repudiation integrity and assess the capabilities present to detect/alert on targeted attacks or malicious activities

In addition, if we discover additional areas that we believe need attention, we will also include them as either risks or observations, depending on the method that the County wishes, since they may be considered out-of-scope. The Rules of Engagement and/or Test Plan will be developed once the proposal is approved and will include the technical details for the scope.

ATA will collaborate with the County to determine if a security control is not applicable from the list provided above and document the exception in the Rules of Engagement and/or Assessment Plan.

Sauk County Project Description

For this Sauk County assessment ATA will leverage the information gathered discussed during the planning and exploit stages above, but also use proven technologies and methodologies to role-play an attacker against the County's Internet accessible, and internal systems and services. ATA understands that the following information systems are in-scope for the penetration test:

- Election System External Wireless WAN
- The County's Public Internet Connection
- Election System Communications Server
- Election System File Server
- Election System User PCs
- Election Results Web Page

A review of this nature is a practical demonstration of the extent of access that could be gained within a limited timeframe, as well as discovery of common security weaknesses, which might be used to launch further targeted attacks. The following testing objectives are covered as an unauthenticated and/or unauthorized user:

- Verify the perimeter and internal technical security controls, to include Firewall, anti-virus, etc.).
- Scan, or use manual techniques on, identified information systems for any weaknesses or vulnerabilities.
- Identify any gaps, vulnerabilities, or missing patches that may exist in the technical controls.
- Map vulnerabilities to known exploits identified in Bugtraq ID, or MITRE's Common Vulnerabilities and Exposures (CVE) database.
- Attempt to bypass system, application, or architecture controls, to acquire privileged access to systems and services within the environment.
- Acquire access to information relating to other users and customers or which is not publicly accessible.
- Identify and attempt to exploit vulnerabilities to compromise a system, service, or the environment.
- Where relevant, test the responsiveness of detection controls, response and subsequent management of security incidents related to the environment.

ATA will document the status of the technical controls as Satisfied, Partially Satisfied, or Not Satisfied, and any identified weaknesses in the Security Assessment Test Plan.

Table 1 describes the implementation plan with a high-level methodology we will apply to discover, and with permission, exploit common security weaknesses.

Table 1: ATA's Implementation Plan

Project ID	External and Internal Vulnerability Scanning and Penetration Test	Timeline and PoC
1.1	**Penetration Testing** With County permission, ATA will attempt to validate any identified vulnerability or technical control through penetration testing or through administrator support. Based on the analysis completed during the vulnerability analysis phase, the security tester attempts to exploit identified weaknesses to compromise a system, service, or gain a foothold in the County environment for further exploitation. ATA will utilize the following to validate vulnerabilities identified, to include: Kali Linux, Metasploit, and manual techniques. ATA will assess any available management, technical, and operational controls during this phase.	**Week 1 and 2** **Roger Colon and Mohsan Farid**
	Reconnaissance ATA will gather as much information about the County's external and internal environments as possible. ATA expects information to also come from the County as this will not be considered a Black Hat assessment. The information assists in profiling the County' Internet presence and security posture. This allows the security tester to take a focused and informed approach when targeting the environment, its systems, and services. ATA will also attempt to identify active devices, and communication paths not already provided by the County. ATA will utilize several technologies to perform reconnaissance, to include Google, Foca, Netcraft, SamSpade, Kali Linux, and others. In addition, ATA will review the Technical Controls and a few Operational Controls, to include: Access Controls, Audit and Accountability Controls, Configuration Management, Identification and Authentication Controls, System Communications and Boundary Protection Controls, and System and Information Integrity Controls as described in NIST 800-53 Revision 4.	**Week 1** **Roger Colon and Mohsan Farid**

	Asset Discovery and Enumeration ATA will identify any accessible systems, network ports, running services and technologies used. A list of the County' systems and services are mapped for testing with prioritized targets based on initial profiling. ATA will utilize several technologies during this phase, to include: Nmap, Hping, Burp Suite Pro, Nessus, Wireshark, Kali Linux, and nCircle. ATA will also use manual techniques to identify systems. ATA will assess any available management, technical, and operational controls during this phase.	**Week 1** **Roger Colon and Mohsan Farid**
1.2	**Vulnerability Scanning** ATA will probe the County' information systems and services for known weaknesses using technologies such as Nessus and Netsparker. Any discovered vulnerabilities are reviewed, analyzed, and prioritized. In addition, ATA will assess the Technical Controls and Operational Controls, to include: Access Controls, Audit and Accountability Controls, Configuration Management, Identification and Authentication Controls, System Communications and Boundary Protection Controls, and System and Information Integrity Controls. ATA will assess any available management, technical, and operational controls during this phase.	**Week 1 and 2** **Roger Colon and Mohsan Farid**
1.3	**Conduct a Policy and Procedure Review** ATA will review the policies and procedures provided by Sauk County. ATA will examine the documentation, conduct interviews, and identify any deficiencies or gaps in the documentation. Findings or deficiencies will be discussed with Sauk County and documented in the assessment report.	**Week 2** **Kristine Titzer**
1.4	**Develop a Detailed Report** ATA will report all management, technical, and operational weaknesses identified and prioritize those vulnerabilities that were validated through exploitation in the assessment report.	**Week 2 and 3** **Kristine Titzer, Roger Colon**

	ATA will also identify any gaps from the documentation review. In addition to reporting the findings, ATA will map the vulnerabilities back to NIST 800-53 Revision 4, OWASP Top 10, and CIS Top 20 security controls.	**and Mohsan Farid**

Conduct External and Internal Penetration Testing

In this testing, ATA will use its **"Eyes-Shut"** approach to seek to gain as much knowledge about the County's Internet presence (as it pertains to the target components) using resources available to any technical person via the Internet. ATA has an exhaustive checklist for finding open entry points and vulnerabilities within an organization, and for Sauk County will focus its penetration efforts on Sauk County's:

- Election System External Wireless WAN
- Public Internet Connection
- Election System Communications Server
- Election System File Server
- Election System User PCs
- Election Results Web Page

First, ATA will conduct Google searches and Google hacks, using different tools and technologies to conduct reconnaissance to identify County emails, hosts, subnets, etc. that are Internet-facing. ATA will identify targets and map the different attack vectors. Any information gathered during this phase will be used during the penetration test. ATA will also use various vulnerability scanners to complete a discovery and inventory on the security risks posed by identified vulnerabilities. ATA will then validate if the vulnerability is exploitable. To accomplish this phase, we anticipate that the testing will encompass at least the following:

- Evaluation of IP address ranges
- Internet vulnerability scanning using Tenable Nessus and Netsparker
- Lateral motion within the network
- Potential compromise of Internet firewalls
- Potential compromise of web server(s)
- Other devices identified during testing

It should be noted that ATA testers might veer from their test plan to explore unexpected routes into the network (and/or focus area) that may surface during the testing. From this testing, we will determine where exploitation can occur and begin to document those possibilities. The list of vulnerabilities will be included in the final report.

At the end of the Discover stage, activities and findings are documented, results analyzed to determine the level of risk, and appropriate mitigation strategies developed. These are then integrated into the final report.

ATA will build upon the activities completed during the vulnerability scanning, and use best practices, our experience, and follow OWASP, NIST, and other guidance to assist the County in securing their information systems and information. We will leverage vulnerabilities identified during the scanning phase to identify exploitable weaknesses. As a part of our regular process, we will begin with research about the target environment. We will focus on:

- ***Identifying and Validating*** specific threats and risks to your organization to:
  - Understand the actual risk to the organization posed by the specific vulnerabilities
  - Test the security of the environment
  - Identify vulnerabilities that are exploitable
  - Determine if current security measures are detecting or preventing potential attacks
- ***Recommending*** actions for mitigation
- ***Assigning*** a "risk rating"
- ***Calculating*** the effect of the threat or risk
- ***Documenting*** the problems
- ***Prioritizing*** findings by the damage you might sustain if the vulnerability was exploited.

While our tests include validating known vulnerabilities through penetration testing, we will utilize where possible, automated tools, and if necessary, manual ethical hacker techniques. Additionally, ATA will also seek to go far beyond these steps by looking at complex interactions between the applications, infrastructure, and the network components. Hacker methodologies are will be examined carefully, and used as necessary, to determine the likelihood of unauthorized exploitation by external and unauthorized users, past and present employees, and other personnel. However, the ability for authorized individuals to circumvent processes is also a major focus area where analysis will occur.

At a time to be mutually agreed upon, as soon after the kickoff as possible, ATA will begin the penetration testing of the County public information systems. The penetration test includes three steps (or more phases): Plan, Discover, and Exploit to get the results necessary to meet the requirement. The planning and discovery are all about identify the vulnerabilities, and the exploitation is where ATA will validate any County weaknesses through penetration testing.

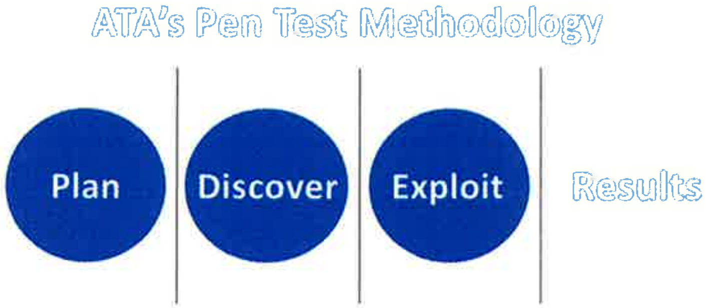

Figure 1 – ATA's penetration test methodology.

Network Penetration Test

A network penetration test is the process of identifying, but specifically validating and/or exploiting vulnerabilities identified in the County' IT logical and physical IT infrastructure, to include network devices, operating systems, and different types of platforms. This type of test may include various malicious techniques to evaluate the County network's security, or lack of, responses.

ATA will use automated tools and manual ethical hacker techniques to validate as many vulnerabilities and/or weaknesses and test to ensure the vulnerabilities are real. The normal process is as following:

- Review and research vulnerabilities identified during the vulnerability assessment.
- Identify vulnerabilities that have an exploit available or are low hanging fruit.
- Validate the vulnerability without exploiting the vulnerability.
- Exploit the vulnerability to gain unauthorized access to a system, and access County information.

ATA will take every measure to not impact the availability of the system or its data or alter any data.

During the network penetration test, ATA may identify vulnerable web applications; therefore, web application penetration testing could be leveraged to exploit web application vulnerabilities to also gain access to the County's systems and/or data.

Web Applications Penetration Test

If vulnerabilities are identified on the County web applications, ATA will all attempt to validate vulnerabilities through penetration testing. Web applications play a vital role in every modern organization. If the County does not properly test and secure its web apps, attackers can compromise these applications, damage business functionality, and steal data. Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems. ATA will use the OWASP Top 10 testing methodology to conduct non-credentialed and if required, credentialed penetration testing of the County web applications. The testing will include validating and/or exploiting risks that are associated with:

- Injection attacks
- Broken authentication
- Sensitive data exposure
- XML External Entities
- Broken access controls
- Security misconfiguration

- Cross-site scripting
- Insecure deserialization
- Using components with known vulnerabilities
- Insufficient logging & monitoring

Figure 2 provides a high-level visual of how ATA will assess the County 's web applications.

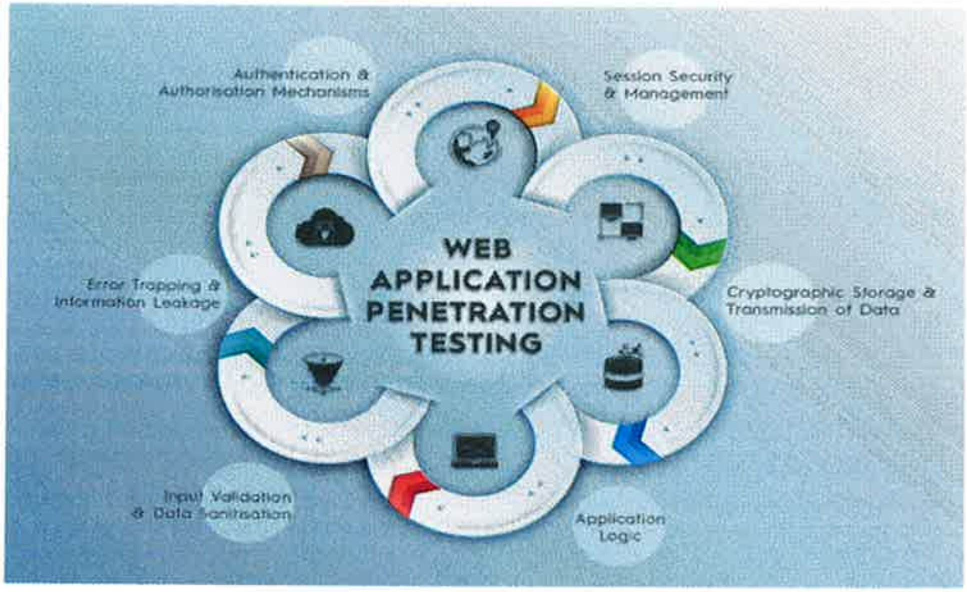
Authentication & Authorisation Mechanisms
Session Security & Management
WEB APPLICATION PENETRATION TESTING
Error Trapping & Information Leakage
Cryptographic Storage & Transmission of Data
Input Validation & Data Sanitisation
Application Logic

Figure 2: A visual on ATA's methodology for web application penetration testing.

ATA will utilize the following steps when conducting the web applications penetration testing:

1. Test the application/web servers for vulnerabilities
2. Map the different application's content
3. Test the client-side controls
4. Test the authentication process
5. Test the session security and management
6. Test the access controls
7. Test for input-based vulnerabilities
8. Test for function-specific input vulnerabilities
9. Test for application logic flaws
10. Test for shared hosting issues

The above steps will include automated techniques using known vulnerability assessment solutions, and manual ethical hacking techniques. ATA will validate vulnerability management efforts, test the effectiveness of existing security controls, and identify gaps in the IT risk management strategies. The results of this exercise will be used to inform plans for the County'

IT risk management program. Specific testing will be captured in the Rules of Engagement and/or Assessment Plan.

Conduct Vulnerability Scanning

For this portion of the assessment, ATA will work internally and begin non-credentialed testing of the County' internal and external logical and physical IT infrastructure, to include applications, databases, end point devices, network devices, and servers with access to the County's election system. We will utilize **Tenable Nessus** and **Netsparker** to scan the network and web application systems. We draw on information gleaned from any previous steps and use both automated technologies and manual techniques to identify vulnerabilities for systems identified in the Rules of Engagement or Assessment Plan. This testing forms the first step in reporting on the status and state of security from inside, both for a non-authorized user and of an authorized user exceeding authority.

To begin the process, we request a short introductory session delivered by the most appropriate County staff members. This provides our engineers with an overview of the County' methods and structure. We also request a presentation of organizational structure, overall network components, and the network/security structure in place. Also beneficial is information about your security objectives, risk tolerance/risk aversion profile, anticipated growth/needs, etc.

To ensure that a wide variety of vulnerabilities are addressed, not simply those that can be discovered via scans, ATA will also examine the following, utilizing ethical hacker techniques:

Operating Systems and Network Weaknesses – This step encompasses a detailed investigation of in-scope operating systems and network weaknesses related to the infrastructure (e.g., DNS spoofing), including analytical findings, recommendations, prioritization, and mitigation or closure needs. We examine firewall/router ports, and services enabled (remote access) to permit external access and the security configuration of the operating systems that permit this access as compared to that recommended by the vendor (along with why variances exist). Upon completion, the consultants evaluate the implementation of the boxes, their by-pass capabilities, and other vulnerabilities.

Databases – We will examine the security surrounding databases to determine their susceptibility to unauthorized access. We will also determine how they inter-connect with other elements of the infrastructure and present the security weaknesses surrounding their structure and usage.

Control Functions – Proposed control functions are reviewed to discern which might be at risk or allow errors. ATA will examine security-related documentation (security policies, standards, and procedures) to assess and determine if the documentation meets the industry controls; interview stakeholders to ensure they understand what is in the security-related documentation; and test the County's information systems to ensure they are compliant with the security-related documentation. Examination of logical areas for operating platforms will involve manipulation of "other-than-regular" logical network computing paths. These paths may lead through convoluted passages and other network segments that may not be accessible initially. ATA engineers look for other information depending on the pattern of results, and the remaining assignment requirements. Following this, a series of probing exercises are performed. These seek to determine:

- Discrepancies in actual controls vs. intended controls (per appropriate client policy and regulations).
- Weak implementation of policy per industry security controls and best practices.
- Security exposures that could result from the way multiple boxes are connected (particularly network routers with other boxes) or used together.
- Within this area we will focus on System Management Controls such as Problem and Change Management and the patching process along with the adequacy of documentation and controls.

Inter-Connectivity – In evaluating inter-connectivity, ATA examines how the components touch the operating system, what the security weaknesses are, and what type of problems procedural tasks incur. Recommendations for risk mitigation are gathered.

Target Server Business Processes – Determination of the business processes within the scope of work. During this step, ATA gains an understanding of the relative importance of various servers to the organization. The engineers utilize this information to better target business risk and opportunities for exploitation.

Other areas are also tested, based both on other needs we observe as we conduct the testing and on knowledge gained from ATA engineers' experiences at other sites. ATA will report on exploitable processes, hosts, devices, and vulnerabilities and their level of risk along with known fixes, recommendations, and resource estimates to correct or mitigate risk.

This portion of the internal assessment will focus on the items requested within the request including:

- In-scope Servers
- Network Devices
- Operating Systems

In addition, if we discover additional areas that we believe need attention, we will also include them as either risks or observations, depending on the method that the County wishes, since they may be considered out-of-scope. The Rules of Engagement and/or Test Plan will be developed once the proposal is approved and will include the technical details for the scope.

Conduct a Policy and Procedure Review

ATA will conduct a comprehensive review of their security-related policies and procedures to stay current with applicable federal, state, and local laws. ATA uses the following process to review security-related documentation (policies, standards, procedures, etc.).

1. Prepare. ATA will request the policies and procedures in advance to examine them, and then come prepared with an understanding of policies and procedures and a list of items to be reviewed by the County.
2. Examine. Once the policies and procedures are received by ATA, information assurance subject matter experts will examine each documentation to ensure the following:
   A. If the documentation is still necessary and accurate.
   B. If a policy should be combined with another policy or if it should be rescinded.
   C. If the policy is up to date with current laws and regulations, and if a specific procedure is written to enforce the policy.
   D. If changes are required to improve the effectiveness or clarity of the policy or procedure.
3. Interview. ATA will interview the County employees and ask them to explain their work process. ATA will then compare the process, as the employee explained it, to what the written policy and/or procedure says. This step is necessary to gain an understanding of the County employee competence and identify areas that need additional training.
4. Document. ATA will document the results and any differences in practice to how the policies are written, when policies are complied with, and when they are not. This may also include other information that is gathered from the interview process. ATA will provide recommended updates to the documentation where needed.
5. Report. ATA will create an easy to read audit report detailing the identified findings, and recommendations for an improvement plan that have gaps.

Develop a Detailed Report

ATA will draft and provide a detailed assessment report capturing all the activities conducted during the assessment. This report will include an Executive Summary, with a high-level summary of the findings, a narrative on what was tested and how, the results of the policy and procedure analysis, and any deviations from the Wisconsin Elections Commission standards. Once the draft report is delivered to Sauk County, ATA will schedule a briefing to discuss the draft report and listen for any mitigation to the findings being presented. ATA will then update and finalize the report before sending the final version to Sauk County.

Deliverables

The following Table contains the proposed deliverables for Sauk County.

Table 2: Deliverables

	Deliverable	Description
1	Kick-off Presentation	A PowerPoint presentation describing the approach to the engagement and the necessary information and interrelationships to ensure engagement success. A PDF version of this document will be delivered by ATA to the County at the onset of the project. **NOTE: If not necessary, please inform us.**

2	Signed Confidentiality Agreement	Non-disclosure agreement form (provided by the County or optionally, by ATA).
3	Rules of Engagement or Assessment Plan	A detailed work breakdown structure and schedule prepared in Microsoft Project and/or Word. A PDF version of this document will be delivered by ATA to the County at the onset of the project. **Also known as a Statement of Work, Rules of Engagement/Assessment Plan to supplement this proposal.**
4	Final Review Presentation	A PowerPoint presentation that summarizes the secure implementation of the County technologies. A PDF version of this document will be delivered to the County at the completion of the project.
5	Final Engagement Report	Draft report shall be issued within one (1) week of the completion of the assessments. The final report shall be issued within four (4) weeks of the assessment. The formal presentation shall be scheduled to be held within three (3) weeks of the final report being delivered.

Options

Although not specifically discussed in the RFP, ATA added **Web Application Vulnerability Scanning and Penetration Testing** in this proposal (see above). This assessment is already included in the pricing. However, if Sauk County does not want ATA to assess the security of its web applications, please let us know as we develop the Rules of Engagement.

In addition to a web application penetration test, and policy and procedure review, ATA can review other security-related documentation, to include the County's **Business Impact Analyses (BIAs)** to ensure that they address impacts and criticality. We will confirm that each BIA addresses: critical functions and services; resources to support each critical function or service; relationships and interdependencies among the impacted functions and services; estimated decline in effectiveness over time that a critical function or service can be inoperable without a catastrophic impact; estimated maximum amount of information or data that can be lost without a catastrophic impact to a critical function or service; interim or workaround procedures to perform critical functions or services critical events or services that are time-sensitive or predictable and require a higher than normal priority critical non-electronic media required to support critical functions or services.

We can also review all **information technology contingency plans (ITCP)**, or backup and recovery plans to ensure that their strategy is implementable and known by all personnel who perform backup or recovery. We will evaluate strategies to ensure that the plans address the type of incident, type of system, and its operational requirements. Sample strategies include commercial contracts with cold, warm, or hot site vendors, mobile sites, mirrored sites, reciprocal agreements with internal or external organizations, and service level agreements (SLAs) with equipment vendors. In addition, we will consider Redundant Arrays of Independent Disks (RAID), automatic fail-over, uninterruptible power supply (UPS), and mirrored systems. We will confirm that the strategy includes a combination of methods to provide recovery capability over the full spectrum of incidents.

We will review each contingency test plan element to confirm the accuracy of individual recovery procedures and their overall effectiveness. We will verify that the test plan includes system recovery on an alternate platform from backup media; coordination among recovery teams; internal and external connectivity; system performance using alternate equipment; restoration of normal operations; and notification procedures. We will review contingency test reports to confirm that they include the deficiencies to be addressed and have recovery actions with completion schedules.

Finally, ATA can conduct a **Static Application Security Test (SAST)** of a specific Sauk County application. By looking at the source code, ATA can identify vulnerabilities on an application before it is promoted into Production.

Pricing

ATA is proposing the following price for the Election System Security Risk Assessment: **$15,500** for **three (3)** full-time subject matter experts over a **three-week period**. See Table 4. Options can also be added on if desired by Sauk County. NOTE: All prices quoted in Table 3 Cost Proposal shall be good for 180 days from the date signed.

Table 3: Cost Proposal

DESCRIPTION	COST
1. Voting System SRA:	
a. Penetration Testing	$7,500
b. Vulnerability Scanning	$3,500
c. Policy and Procedure Review	$4,500
Total cost for solution (Add items above) in Item 1	**$15,500**
2. Optional Services	
a. BIA and ITCP Review	$2,500
b. Source Code Review (per application)	$2,500
3. Total cost for solution (Add items above): Items 1 and 2	$20,500

For the Vendor:

AUTHORIZED SIGNATURE

October 13, 2020
Date

Roger Colón, Jr.
PRINTED NAME

President & CEO
Title

Advanced Threat Analysis Inc.
COMPANY NAME

For the County:

AUTHORIZED SIGNATURE

11/11/20
Date

Steve Pate
PRINTED NAME

MIS Director
Title

References

Past Performance 1 – SIN *132-45 Highly Adaptive Cybersecurity Services (HACS)*

Offeror's Name	Advanced Threat Analysis Inc. (ATA)
Client/Customer Company Name and Address:	Internal Revenue Service, 5000 Ellin Road, Lanham, MD 20706 through VariQ Corporation
Title of Contract or Agreement plus Contract and other Identification Numbers, if any:	Security Risk Management, Subcontract Agreement No: 2013-ATA-TIPSS4, Task Order No: 02
Client Project Manager Name, telephone number, fax number, and E-mail Address:	Greg Dimmie Enterprise Database Scanning Lead/Manager Phone: (240) 602-0200 Fax: (304) 264-5491 Greg.a.dimmie@irs.gov
Client COTR or TPOC Name, telephone number, fax number, and E-mail Address:	Olin Green, Treasury Program Manager Phone: (571) 338-1037 Olin.green@variq.com
Client Contracting Officer Name, telephone number, fax number, and E-mail Address:	Janelle Meredith, CO Phone: (240) 613-8243 Janelle.m.meredith@irs.gov
Period of Performance:	03/31/2016 - 03/20/2020
Description of Service(s) or Product(s): ATA provides Subject Matter Expertise to Security Risk Management for Enterprise Database Scanning, Penetration Testing, and Security Controls Assessments. ATA is a valued partner on the SRM contract under TIPSS-4, providing subject matter expertise with vulnerability identification, review, analysis, and reporting for all IRS databases. ATA collaborates with the different IRS business units to analyze and validate the vulnerabilities and support the remediation process, or to mark vulnerabilities as false positives. ATA also provides SRM with critical vulnerability management training using Guardium. In addition to the SME support, ATA also provides SRM with Security Controls Assessments for IRS information systems. ATA conducts security controls assessments by collecting IRS-related artifacts, interviewing stakeholders, and testing information systems for any potential risks. ATA has been supporting this contract since 2016.	
Total Contract Value	$1,035,822.40
SIN Value	$1,035,822.40

Past Performance 2 – SIN *132-45 Highly Adaptive Cybersecurity Services*

Offeror's Name	Advanced Threat Analysis Inc. (ATA)
Client/Customer Company Name and Address:	Bureau of Engraving and Printing (BEP) through VariQ Corporation
Title of Contract or Agreement plus Contract and other Identification Numbers, if any:	Security Risk Management, Subcontract Agreement No: 2013-ATA-TIPSS4, Task Order No: 01
	Scott Graf, Bureau of Engraving and Printing (BEP) 300 14th St SW Washington, DC Scott.graf@variq.com 202-292-4236
Period of Performance:	3/25/2015 – 10/31/2019

Description of Service(s) or Product(s):

ATA provides security engineering support to BEP through VariQ Corporation, to include

1. The risk management framework
2. Categorize BEP information systems
3. Support the selection of security controls
4. Assesses the information systems for risk
    a. Vulnerability Scanning
    b. Penetration Testing
5. Support the authorization to operate
6. Support continuous monitoring of BEP information systems

ATA has been supporting this contract since 2015.

Contract/Cost Type (firm fixed price, cost reimbursement, user fee, or other):	Cost Plus Fixed Fee (CPFF)
Total Contract Value	$638,039.20
Total SIN Value	$638,039.20

Past Performance 3 – SIN *132-45 Highly Adaptive Cybersecurity Services*

Offeror's Name	Advanced Threat Analysis Inc. (ATA)
Client/Customer Company Name and Address:	Hospice & Community Care of Lancaster County 685 Good Drive Lancaster, PA 17601
Title of Contract or Agreement plus Contract and other Identification Numbers, if any:	Security Assessment
Client Project Manager Name, telephone number, fax number, and E-mail Address:	Krista Kae Hazen (717) 391-2402 (Direct) khazen@HospiceCommunity.org 685 Good Drive Lancaster, PA 17601
Period of Performance:	4/29/2017 Renewed Annually Just completed 2019 work on 5/20/2019
Description of Service(s) or Product(s): Services included: Penetration testing, analyzing policies and configurations, evaluation of compliance with regulations and directives, and guidance related to security controls to mitigate risk. The engagement is to analyze and evaluate the IT risk management infrastructure as it applies to the Hospice IT environment, which is comprised of the physical IT environment and the operational IT environment as defined below. The assessment is applicable within the context of the IT business drivers. • **IT risk management infrastructure** (i.e. policy, procedure, organization, governance structure, and controls pertaining to IT security, as well as continuity of operations plans and disaster recovery plans). • **Physical IT environment** (i.e. the FCC LAN/WAN infrastructure and all connected IT systems, equipment, devices, software applications, utilities, services, physical or wireless interfaces to other networks, externally hosted nodes, information stores, and managed services. • **Operational IT environment** (i.e. key IT operations, processes, and routines, key data information flows, and new and on-going IT initiatives). • **IT business drivers** (i.e. organization mission, major business operational capabilities, facilities, staff and other stakeholders).	
Contract/Cost Type (firm fixed price, cost reimbursement, user fee, or other):	Firm Fixed Price
Total Contract Value	$12,000 Annually
Total SIN Value	$12,000 Annually

Resumes of Proposal Personnel

Each ATA employee is carefully screened, and our pre-employment background process includes criminal record checks, tax, and financial checks. ATA members are trained in our services that we provide to customers in the commercial, federal, international, financial, and healthcare sectors. Finally, ATA provides in-depth consulting specifically tailored to secure the diverse elements of our clients' enterprise. ATA affirms that no employee working on this engagement has ever been convicted of a felony.

The ATA value proposition delivers expert capability at attractive prices with low risk. Our approach for providing highly qualified staff will give the County the best return on its investment. Our staff has deep experience and expertise in information security, cloud security, application security, network security, secure application development, and is backed up by numerous industry certifications that include:

1. Certified Ethical Hacker (C|EH)
2. Offensive Security Certified Professional (OSCP)
3. Licensed Penetration Tester (LPT)
4. Certified Penetration Tester (CPT)
5. Qualified Ethical Hacker (QEH)
6. Certified Network Defense Architect (C|NDA)
7. Certified Information System Security Professional (CISSP)
8. Certified Software Security Lifecycle Professional (CSSLP)
9. Certified Information Security Manager (CISM)
10. Certified Information Security Auditor (CISA)
11. Amazon Web Services (AWS) Solutions Architect
12. Certified Cloud Security Knowledge (CCSK)
13. GIAC System and Network Auditor (GSNA) Certified Professional
14. Information Technology Infrastructure Library (ITIL) Certified Professional

ATA's employees are subject matter experts (SME) in cyber security, information security, and information assurance. All SMEs are educated and certified in information technology, information security, and business information systems.

Mr. Roger Colón, a cyber security SME and certified ethical hacker, will personally take the lead on this project as he does on many other engagements. He has over 20 years of experience in information technology and information security. He started penetration testing in 2003 when he worked for KPMG. He then began working as a pen tester at the IRS. He became the Chief of Penetration Testing and Source Code Analysis at the IRS. He was promoted to Associate Director of Cybersecurity Operations and oversaw the vulnerability management program. Eventually he decided to start his own company providing vulnerability management and penetration testing services. He leverages frameworks such as NIST 800-53 Rev 4, OWASP Top 10, and CIS Top 20 to help organizations build security.

Mrs. Kristine Titzer is an information assurance SME and will support this engagement by with the policy and procedure review. She will leverage NIST 800-53 to conduct the security assessment. They will also support the development of the different artifacts to include a final assessment report.

Mr. Mohsan Farid is a certified ethical hacker with experience in certifications in different areas of penetration testing and red teaming. He will be tasked with conducting the external and internal penetration testing. He will leverage different frameworks to assess the County's information systems, such as OWASP Top 10, and NIST 800-115.

This gives ATA the corporate capability and capacity to staff, plan and manage engagements effectively and efficiently, and individual competency required to execute on those plans.

(see resumes beginning on next page)

Roger Colón, Jr.
8008 Bush Hill Court, Severn, MD 21144
Roger.colon@atacorporation.com, 443.223.8469
Subject Matter Expert
Senior Security Architect and Engineer

Cyber Security Consultant Professional

Professional Summary

An information technology, information security, and cyber security subject matter expert (SME) with over 20 years of strategic and tactical experience. Primary areas of expertise include security architecture, security engineering, vulnerability management, program management, security assessments, and continuous monitoring of federal government and commercial information systems. Additionally, develop, and implement business, technical, and security requirements for technologies that are on premise or in the cloud. A technical SME in vulnerability scanning, penetration testing, and ethical hacking. Finally, a very successful Program Manager overseeing IT and security-related programs and projects.

Education

Master of Science Certificate, IT Project Management, George Washington University, June 2010
Master of Science, IT Management, American Intercontinental University, April 2004
Bachelor of Science, Business Information Systems, University of Phoenix, February 2002
Associate of Arts, Spanish, Anne Arundel Community College, June 2000

Professional Certifications

Certified Secure Software Lifecycle Professional (CSSLP); Certified Ethical Hacker (CEH); Certified Cloud Security Knowledge (CCSK); Certified FISMA Compliance Practitioner (CFCP); Certified Information Security Manager (CISM); Certified Information Systems Security Professional (CISSP); Information Technology Infrastructure Library (ITIL) v3.0; GIAC System and Network Auditor (GSNA); GIAC Pen Tester (GPEN); CheckMarx Certified Engineer (CxCE), CyberArk Level 1; Splunk Core Certified User; Solaris 7 Systems Administrator; Six Sigma Green Belt; and CompTIA A+ and Security+

Clearances

Public Trust with Department of Veterans Affairs (VA), 2015; Department of Treasury, Internal Revenue Service (IRS), 2019; Department of Homeland Security, U.S. Customs and Immigration Services (USCIS), 2018; Consumer Financial Protection Bureau (CFPB), 2015; and the Center for Medicare and Medicaid Services (CMS), 2013

Experience

Advanced Threat Analysis, Inc. November 2012 – Present

Senior Information Systems and Cyber Security Architect/Senior Security Engineer/Senior Security Controls Assessor/Virtual Chief Information Security Officer/Program Manager

- As Subject Matter Expert (SME) in information technology, cyber security, and information security, successfully provide SME support to some of the largest federal, financial, and healthcare organizations in the United States.
  - All work is mapped back to different compliance and security frameworks, to include: the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 (Rev 4), Payment Card Industry Data Security Standard (PCI-DSS), Minimum Acceptable Risk Standards for Exchanges

  - (MARS-E), International Organization for Standardization (ISO) 27001 Information Security Management, and Center for Internet Security (CIS) Top 20 Critical Security Controls.
  - Provide end-to-end security, to include developing requirements, capturing the implementation or implementing requirements, assessing the requirements, and monitoring the implementation of those security requirements.
  - Build information security programs, and implement on cloud, virtual, and on-premise enterprise technologies.
  - Major organizations successfully supported include Optum, CMS, CFPB, IRS, M&T Bank, Virtustream, Department of Justice, Department of Homeland Security, the VA, USCIS, and others.
- Successfully architected RSA AA, Affordable Care Act Information System (ACA IS), Splunk Enterprise, SailPoint IdentityIQ, CyberArk, Tenable Security Center, and other technologies for federal and commercial organizations.
  - Design, build, and oversee the implementation of network and computer security technologies for a federal agency and a major healthcare organization leveraging NIST 800-53 and MARS-E frameworks.
  - Create complex security structures – and ensure they work.
  - Partner with all business units to guide and inspire teams to address security risks.
  - Develop and maintain security architecture deliverables and artifacts for reference and use by IT project teams.
  - Provide fraud analytics support for bank customers accessing their online accounts. Analysis includes exploring data, preparing data for modeling, creating logistic regression models, and validating models.
- Conduct security controls assessments and security risk assessments on new technologies and existing information systems in the cloud and on premise.
  - All work is mapped back to different compliance and security frameworks, to include NIST, PCI, MARS-E, ISO, and CIS Top 20.
  - Gather evidence, interview stakeholders, and test the controls through automated and manual processes.
  - Assessed the implementation of Amazon Web Services (AWS) and Microsoft Azure at different federal organizations as they leveraged these technologies for Software and Platform as a Service.
  - Assessed multiple technologies for the Optum FISMA Environment (OFE), to include Splunk Enterprise, SailPoint IDIQ, CyberArk, BlueCoat Proxy, F5 Load Balancers, InfoBlox, IronPort, Ixia, ServiceNow, Symantec Data Center Security, SevOne, and RSAM. Additionally oversaw the remediation of findings.
  - Conducted security controls assessments for different customers, to include the IRS, CMS, M&T Bank, Virtustream, USCIS, and other federal and commercial organizations.
  - Develop security assessment reports, and present those findings to C-level stakeholders.
- Conduct successful red team exercises, to include social engineering, phishing attacks, man-in-the-middle attacks, and other types of attacks against large companies and organizations.
  - Use phishing technologies, such as the Social Engineering Toolkit (SET) and other technologies to trick users into providing potentially sensitive information, used to pivot to internal systems.
  - Collaborate with C-Level's to report social engineering trends, and where their organization may have gaps that need to be addressed. Support retesting of security awareness and training security controls.

  - Develop reports that discuss the risk, and remediation.
- Manage a $9 million dollar Information Technology Security Implementation (ITSI) program, to include the planning and governance, and oversee the successful delivery of ITSI and Continuous Diagnostics (CDM) technologies at the IRS, to include Splunk Enterprise, CyberArk, SailPoint IdentityIQ, Return Review Program, Customer Account Data Engine, Account Management System, and others.
  - Manage the ITSI portfolio of projects and programs. Develop position descriptions, interview, hire, and onboard candidates. Coordinate internal resources and third party vendors for the flawless execution of projects. Assist in the definition of the project scope and objectives, involving all relevant stakeholders and ensuring technical feasibility.
- Support all technologies and applications across all phases of the system and software development life cycle (SDLC) to include defining, implementing, assessing, and monitoring security requirements.
  - Successes include the integration with Development Operations (DevOps) and Development Security Operations (DevSecOps) for end-to-end services.
  - Follow SDLC processes, to include Waterfall, while also working with Agile processes.
  - Collaborate with developers to test and implement different Google and Mozilla Firefox extensions, to include Cookie Manager, Scraper, Websecurify, Inspector, Debugger, and WebIDE.
- Work for small, mid-size, and large organizations as a Virtual CISO, to include overseeing the enterprise security program, capturing metrics, developing security-related documentation, overseeing the security operations and maintenance for the security architecture, and keeping the CIO's informed on all things security.
  - Leverage the Cyber Security Framework (CSF) to include tracking the different milestones.
- Supported a DHS contract as an Information System Security Officer (ISSO) for several information systems.
  - Work included the daily security operations for three different major applications and their general support systems, to include reviewing events and vulnerabilities in Tenable Security Center and Splunk Enterprise; conducting security controls assessments, developing and/or updating the System Security Plans for each information systems; and attending various meetings to support security objectives.
- Support the requirements gathering and implementation of security architecture and identity access management technologies for Optum to include Splunk Enterprise, SailPoint IdentityIQ, CyberArk, and ServiceNow.
  - Map all requirements to NIST and MARS-E.
  - Develop implementation statements for how the technologies are addressing the security requirements identified by the organization, NIST, or federal mandates.
  - Support the security controls assessments by providing details on the implementation of the security requirements.
  - Support the daily maintenance and operations of various technologies.
  - Leverage ServiceNow for reviewing, working on, and approving tickets for different changes. Also used Remedy in the past to track and monitor tickets.

- Provide information and system security engineering and assurance consulting services to the Federal and Commercial sectors by providing design recommendations, developing security-related documentation, providing project management support, and risk management for critical security initiatives. Work is in relation to the Federal Information Security Management Act (FISMA), PCI, MARS-E, Sarbanes Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), and the Department of Homeland Security (DHS) Continuous Diagnostic and Mitigation (CDM) initiative which includes the enterprise wide implementation of Splunk Enterprise, SailPoint IDIQ, CyberArk, BigFix, Forescout, Tenable Security Center, and other CDM-related technologies.
  - Considered a Subject Matter Expert (SME) to ensure compliance and security requirements are being met by the different technologies, and/or organizations.
  - Provide technical support for various technologies to include implementation, and operations and maintenance.
- Develop and deliver architecture and engineering documents to include design documents, security requirements, baselines, system security plans, and audit and accountability plans in accordance with NIST 800-53 Rev 4 for Amazon Web Services, webMethods, Red Hat Enterprise Linux 6, Oracle 12, RSA AA, Linux, Greenplum, VMWare, and JBoss.
- Conduct manual penetration testing of dynamic applications and general support systems (GSS) leveraging known frameworks, to include OWASP Top 10, CIS Benchmarks, and NIST.
  - Over 20 years of experience in UNIX, Red Hat Enterprise Linux (RHEL), and Windows system administration. Well versed in using the shell and powershell command line interfaces to test systems.
  - Experienced with web application configurations using RHEL, Apache, MySQL, and PHP.
  - Experienced with Industrial Control Systems (ICS), and Supervisory Control and Data Acquisition (SCADA) information system vulnerability management and penetration testing for electric, water and sewage organizations. Tested Programmable Logic Controllers (PLC) which managed the valves and sensors. Exploited vulnerabilities in systems supporting the ICS to gain access to the Local Human-Machine Interface.
  - Well versed in software exploitation for web and client-server systems. Use SQL injection attacks and/or Cross-Site Scripting attacks to exploit vulnerabilities in web applications.
  - Test applications regularly to ensure encryption is implemented and that customer clients trust the digital certificates to protect both from sensitive data exposure.
  - Able to leverage automated technologies and manual techniques to exploit injection, access controls, and security misconfigurations.
  - Manage advanced technical testing teams to include static code analysts, vulnerability scanners, and penetration testers.
  - Develop Python and BASH scripts to automate some of the validation of vulnerabilities, while also downloading and editing other scripts as necessary.
- Conduct vulnerability assessments on static and dynamic applications, general support systems (GSS), cloud systems, and other information system types.
  - Successfully tested hundreds of applications and/or general support systems with automated tools. Validated and/or exploited hundreds of vulnerabilities using automated technologies.

ADVANCED THREAT ANALYSIS

Mohsan Farid

PROFESSIONAL SUMMARY

Mr. Farid has fifteen years of technical, security, and customer service experience within Government and commercial industries. He currently uses his technical experience to develop, test, and engineer security assessments for various DOD and commercial entities. His engineering skills allow for an in-depth understanding of system security and posture with respect to today's exploits.

- Information Assurance Mgt.
- Firewall/Routers/Switch Security & Mgt.
- Systems Hardening
- Active Directory Mgmt.
- Exploit Development
- Implementation of IA plans, Solutions and Auditing
- Penetration Testing & Web Application
- TCP/IP Architecture
- NIST, DIACAP,FISMA,DITSCAP
- Certification and Accreditation
- Mobile Security
- Web App Testing
- PPSM, Packet Analysis
- Application Security
- IPS/IDS/HBSS/VPN Mgmt.
- Malware Analysis & Antivirus Mgmt.
- Development of IA plans
- Security Assessments
- Security Awareness Development
- Vulnerability Assessments
- Systems Administration
- DoD 8500.1/.2, 8570.1, CJCSM
- Reverse Engineering
- Source Code Review

Clearance:

- Department of Defense, SECRET
- Department of Homeland Security, SECRET
- Department of Interior SECRET
- Department of Treasury SECRET
-

Technical Skills/Tools:

- OS/Applications: Windows, OS X, Linux: Redhat Enterprise, CentOS, Debian, Kali Ubuntu, Fedora, Suse, Slackware, Mandrake, Enigma, Red Hat, Beehive, Knoppix STD, NST, BackTrack, Samurai, VMware ESXi Unix: Solaris, FreeBSD/Open BSD ,Open VMS, Novell
- Forensic Software: Autopsy, SleuthKit, dd/dc3dd, PTK, DD, Pasco
- GOTS scripts: DISA Unix SRR, Oracle SRR, SQL SRR, WebSRR, and Gold Disk.
- Penetration and Vulnerability scanning software: Metasploit, Responder, Empire, Bloodhound, DeathStar, CrackmapExec, Mimikatz, Core Impact, Nmap, Nessus, AppDetective, FoundStone, WebInspect, Retina, Nikto, NTOSpider, Netscan, Retina, X-Scan, AIX, Unicornscan, Sshmitm,Webmitm, Arpspoof, Hydra, Cain and Able, TCP DUMP, Netcat, Cryptcat, Hping, Xscan, AutoScan, Firewalk, DNSwalk, Fport, HttpPrint, Immunity Canvas, OpenVaus, admsnmp, Cisco Global Exploiter, Fierce, Maltego, Mantra, SQL Ninja, snmpenum, one sixty one, Karmetasploit,

ADVANCED THREAT
ANALYSIS

Mohsan Farid

Social Engineering Tool kit(SET), WCE Windows credential editor, Nexpose, Browser exploitation framework.

- Sniffers: Ethereal, Etherape, Ettercap WireShark, Dsniff, Kismet, tcpdump
- Debug/Reverse Engineering: Peach Fuzz, FileFuzz,!Exploitable, DebugDiag, Spike, Immunity Debugger, IDA Pro, Ollydbg, windbg
- Web Application: Burp Suite Pro, SQLMap,AppScan, ZAP proxy, Tamper Data, Acunetix, Paros, WebScarab, w3af, , Wfuzz, Web Inspect, Nikto, NTO Spider, Net Sparker.

Certifications:

Certified Information Systems Security Professional (CISSP) #303425
Federal Information Technology Security Professional (FITSP-A) #00260
Certified Ethical Hacker and Countermeasures V6 (C|EH) #ECC938952
Certified Secure Software Lifecycle Professional (CSSLP) #303425
Certified Network Defense Architect (C|NDA) #ECC938952
Certified Expert Penetration Tester (CEPT) #100218
Certified Security Analyst (E|CSA) #ECC950306
Licensed Penetration Tester (LPT) # SM11 – 404
Certified Penetration Tester (CPT) #100218
Qualified Ethical Hacker (QEH)

Education:

Virginia Commonwealth University
Bachelor of Science in Business

Publications:

Metasploit: EMC Alphastor Device Manager Opcode 0x75 Commnad Injection
Penception: Countering Countermeasures Pentest Magazine April 2013

PROFESSIONAL EXPERIENCE

Pervade Security June 2013 to Current

Mr. Farid performs mobile, internal, and web penetration testing for various clients. As a pen tester for the IRS Penetration Test Code Analysis team, Mr. Farid's responsibilities include managing all aspects of assessment and response engagements from launch to completion. Mr. Farid leveraged the MITRE ATTACK framework and to reproduce and map out advance persistent threat attack scenarios and responsibilities include internal/external penetration testing, vulnerability assessments, and web application pen testing.

As a Mobile Security Penetration tester for various clients, Mr. Farid's responsibilities include pen testing mobile applications and platforms such as IOS, Android, Windows Mobile, while leveraging the OWASP Mobile Top 10.

Vector Detectors, December 2012 to June 2013
Mr. Farid was an independent security consultant and cofounder of Vector Detectors. Vector Detectors provides security consulting services ranging from internal/external penetration testing, vulnerability assessments, and web application pen testing.

Knowledge Consulting Group, March 2012 to December 2012
As a Senior Penetration Test Engineer for Knowledge consulting group, Mr. Farid's responsibilities include internal/external penetration testing, vulnerability assessments, and web application pen testing. Mr. Farid leads pen testing engagements in support of the KCG Cyber Attack & Penetration Division for customers such as Rapid7, Akamai, Stratfor, Intelligence, Metlife, DC WASA, Empire State NYC, BPD, DHS, DOI, FMS, and FRB. In addition to penetration testing, Mr. Farid conducts ST&E for Federal information systems in accordance with NIST standards and oversees and manages the delivery of security assessment services to commercial and Federal customers. Mr. Farid led the FEDRAMP initiative as a 3PAO technical lead for Akamai. Mr. Farid manages all aspects of assessment and response engagements from inception to completion.

Telos Corporation, February 2008 to March 2012
As a Senior Security Engineer, Mr. Farid's responsibilities include conducting vulnerability assessments, penetration testing, and web application assessments. Mr. Farid performs multi-scaled analysis ranging from large scale vulnerability to automated and manual penetration testing in addition to web application testing. Vulnerability assessments are in accordance with the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP, DITSCAP, AR 25-2, and NIST SP 800 series. Mr. Farid manages all aspects of assessment and response engagements from inception to completion.

Mr. Farid leverages the Application Security and Development Security Technical Implementation Guide and OWASP to provide security guidance for use throughout the application development lifecycle. Mr. Farid provides the guidance needed to promote the development, integration, and maintenance of secure applications. Mr. Farid utilizes VMware ESXi server to develop a lab environment for application security and penetration testing. Mr. Farid leverages multiple tools in Back Track distro to perform penetration testing and web application testing. Mr. Farid performs vulnerability testing leveraging tools such as Defense Information System Agency (DISA) Security Readiness Review (SRR) scripts, Nessus/Newt, AppDetective, NTO Spider, Nikto, ISS, FoundStone, WebInspect. Mr. Farid consolidates and analyzes the output from the findings tools and presents them in the form of a vulnerability matrix consisting of a POA&M, DIP, SIP, and DIACAP scorecard. Mr. Farid concludes projects by developing an Appendix Q and Appendix F for each respected assignment.

Security University, August 2010 to December 2010

As an intern, Mr. Farid immerses students into an interactive environment where they're shown how to scan, test, hack and secure their own systems. The lab intensive environment gives each student in-depth knowledge and practical experience with the current essential security systems. Students begin by understanding how perimeter defenses work and then lead into scanning and attacking their own networks. Students then learn how intruders escalate privileges and what steps can be taken to secure a system. Students also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, and Buffer Overflows.

IntelliDyne, LLC, October 2006 to February 2008

As a Security Engineer, Mr. Farid's responsibilities include performing vulnerability assessments and application testing in accordance with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). Mr. Farid is responsible for evaluating application security within the Software Development Life Cycle (SDLC) of clientele. Mr. Farid assisted in the design, development, testing, deployment, and maintenance of secure applications. Vulnerability assessments are derived by identifying and understanding information systems. Said duties are accomplished by the evaluation of system documentation such as System Security Authorization Agreements (SSAA), Security/System Design Documents (SDD), in addition to conducting technical interviews with developers and program security personnel. Through the employment of such accomplished multifaceted approach, Mr. Farid develops detailed test plans for identifying the system accompanied by its components, security requirements, in addition to testing methodologies and tools. Mr. Farid facilitates negotiations with all Points of Contact (POC) for system testing in order to establish testing time, location, and to provide those who are to be tested with an understanding of what to expect during the auditing phase. Mr. Farid performs vulnerability and application testing using tools such as Defense Information System Agency (DISA) Security Readiness Review (SRR) scripts, Nessus/Newt, AppDetective, ISS, FoundStone, WebInspect, John the Ripper, Nmap, and Cain and Able. Mr. Farid consolidates and analyzes the RAW data from the findings tools and presents them in the form of a vulnerability matrix with recommendation for mitigation or elimination of the identified risks for both technical and managerial audiences.

AcquireSoft, April 2002 to October 2005

As a Technology Officer for a fast paced startup company AcquireSoft, Mr. Farid managed a team of engineers in Information Security evaluation, design and implementation of AcquireSoft's technical infrastructure. Mr. Farid was the director of the AcquireSoft Risk Management process. He performed regular data hygiene activities in addition to creating and administering internal and client databases. Additionally, Mr. Farid was responsible for the development and maintenance of the IT Audit mission, strategy, procedures, secure application development, and risk assessments. Mr. Farid focused on secure application development conducting code reviews for security flaws for various customers. Mr.

Farid trained developers on secure development standards. In addition to training, Mr. Farid helped development teams with their information security/information assurance concerns. He also performed routine data encryption for internal security purposes along with clientele data, and installed and configured ERP solutions.

Item Inc., April 2000 to December 2002

As the Systems Engineer and Sr. Network Administrator, Mr. Farid designed, tested, and implemented systems that focused on the infrastructure components. This included network switches, routers, LAN/WAN connectivity, remote access, Windows NT and Active directory domain design and implementation, network management design and implementation. In this capacity, Mr. Farid performed network security/information assurance activities including active audits, firewall, and Intrusion Detection System (IDS) configurations. Mr. Farid exercised defense in depth by utilizing multiple layers of security. In addition, Mr. Farid was responsible for installing and maintaining networks on-site and off-site. In this capacity his duties included the configuration of client systems including server and workstation operating systems, configured customer databases to custom specifications to best meet needs, and performed upgrades to products with optimum security settings/permissions.

RCN Internet, May 1999 to March 2000

As a member of Help Desk support staff, Mr. Farid analyzed and diagnosed Internet and operating system related errors while providing client with superior customer service. This position required exceptional skills in problem solving and diagnostics. Typical tasks of this position included removing Internet related viruses through dos, connecting into mail servers, troubleshooting modems, installing and re-installing drivers, com ports, configuring receive and transmit buffers, communicating and running diagnostics, and resetting modems with initiation strings. In addition, Mr. Farid performed advanced operating system trouble shooting such as extracting Winsock's and manually uninstalling DUN, manual repairing and uninstalling IE 4 & 5. In this capacity Mr. Farid's tasks included editing registry settings, scanning critical system files and replacing them if they were corrupt. He optimized Internet connections; power cycled cable modems and tweaked registry settings for optimal performance.

Kristine Titzer
CISSP | PMP | CRISC

Professional Summary

Results-driven IT professional with over 25 years of experience demonstrating notable success managing a broad range of complex business, IT and IT security programs and initiatives. Hands-on experience leading and supporting system development, PMO, network operations, acquisition management and IT security efforts. Recent experience with TIPSS and CDM tasks; familiar with CDM phases and associated tools. Able to work effectively in a variety of roles. Excellent written and verbal communication skills.

Professional Certifications

Certified in Risk and Information Systems Controls (CRISC), 2011
Certified Information Systems Security Professional (CISSP), 2010
Project Management Professional (PMP), 2004

Clearances

Internal Revenue Service, Minimum Background Investigation – Interim, 2018
Previous clearances range from MBI to Secret from 1990 to present

Professional Experience

Advanced Threat Analysis Inc. (ATA), June 2017 – Present
Senior Consultant
Support public and private customers in the areas of project and security management, technical and security documentation, training, security assessment and authorization, and continuous monitoring.

- Developed draft requirements for COTS tools – business, technical, functional and security.
- Researched malware issues/customer tool capabilities and drafted remediation plan; developed plan and interview questions for security assessment following remediation.
- Developed vulnerability scanning and management metrics to determine if current processes and tools allowed customer to meet goals.
- Revised audit and accountability guidance to align with current processes and tools.
- Drafted training/presentations for a variety of COTS tools.
- Drafted CONOPS for security operations reviews, as customer moved IT platform, infrastructure and software to the cloud.
- Developed draft CONOPS to demonstrate updated data collection tool and dashboard functionality.
- Developed policies, standards and artifact tables for high-level systems that encompassed SOC, NIST and CSA guidance.
    - Created table of NIST 800-53 Rev. 4 controls in Excel and overlaid SOC controls.
        - Created additional entries where matches did not exist.
        - Added basic artifacts required to comply with each control.
    - Updated draft information security policy in accordance with NIST 800-53 Rev. 4.
        - Added policies and standards for all NIST control families.
        - Added SOC guidance to policies and standards.
- Developed security standards for high-level system for NIST control families based on corporate policies and NIST 800-53 Rev. 4.

Support corporate teaming and partnerships related to task orders and IDIQs to include NDAs, subcontracts, proposals, staffing and pricing. This includes TIPSS and CDM tasks, as well as cloud IAM implementation. Manage corporate efforts related to HUBZone, SDVOSB and GSA schedule. Develop and maintain corporate documents related to capabilities, processes, best practices, staffing, pricing, labor categories, customers and past performance.

Torii LLC, August 2007 – June 2017
Consultant
Responsible for corporate initiatives, contract performance, and business development. Support public and private customers in the areas of full lifecycle acquisition, project and security management; financial analysis and costing; business process reengineering; technical and security documentation; proposal development and marketing; performance measurement and reporting; training; security assessment and authorization; and continuous monitoring activities.

Worked with team of small businesses to obtain contracts from 2014 – 2016. Contracts ranged from PMO analysis and training to implementation of online recruiting platforms and defining components and boundaries for complex IT systems. Served as senior consultant on contracts awarded.

- Reviewed RFPs, developed proposals and pricing, drafted and led presentations.
- Oversaw project teams, led customer meetings, guided staff, developed technical/analytical content, monitored progress and prepared monthly reports.

Managed security compliance and risk mitigation support for government customer in accordance with corporate, NIST and FISMA requirements for 10+ major applications that were authorized in 2007 and 2008 and reauthorized in 2012 and 2013.

- Developed and maintained System Registration documentation, Privacy Impact Assessments, System Security Plans, and Risk Assessments.
- Supported SA&A efforts to include providing and updating requested documentation, reviewing and providing feedback on the SAP, attending and documenting SA&A interviews; reviewing scan data and reports to determine false positives; reviewing the SAR and providing feedback on SA&A package.
- Worked with ISOs to determine appropriate access and roles for system testing, and reviewed test plans and results.
- Developed COOP test plan for remote users of government systems; walked users through plan and reviewed results.
- Developed continuous monitoring (CM) strategy and plans and updated annually.
- Managed Plan of Action and Milestones (POA&Ms) and reported progress in Quarterly Memos to the AO and CISO.
- Provided guidance/clarified artifacts necessary to address POA&Ms, as well as required CM controls.
- Used ASSERT and customized templates to ensure that system security information was properly recorded and reported.
- Worked with ISOs, AOs and department management to ensure that quarterly briefings on system status and inherent risks were conducted.
- Reviewed quarterly system scanning reports and worked with ISOs and technical teams on remediation plans.
- Worked with ISSO and ISOs to develop, review and update MOUs and ISAs.
- Conducted independent assessments of NIST controls selected by the ISO and reported results at quarterly briefings.
- Worked with ISO and ISSO to develop and implement risk mitigation plans to address IG audit findings related to legacy system and potential data breaches.
- Developed physical security inspection plans, procedures and templates required for system data housed at off-site, non-government facilities.
- Supported plan implementation via inspection of contractor sites quarterly to ensure the security of the facility and the government data housed therein.
- Worked with ISO and ISSO on complex legacy system to identify system weaknesses, develop risk mitigation strategies and activities, and estimate resources needed to implement them.

- Coordinated artifact preparation, collection and delivery to support internal audits of system security.

IT Consulting Division, Zen Technology, Inc, February 2005 – August 2007
Division Director

Oversaw multiple contracts providing: business process, requirements, configuration and project management; COTS product evaluations; and security planning and certification studies.

- Reviewed and refined requirements for agency COOP plan software; solicited COOP COTS products from vendors, installed software, tested products and recorded test results in Test Director; presented findings to COTR, COOP experts and system specialists.
- Provided briefings on the certification and accreditation (C&A) process.
- Developed guide for C&A, identifying phases, processes, inputs/outputs, and samples and forms; integrated guide with customer SDLC to illustrate the steps required at each phase of the development process.
- Implemented guide and assisted customer in managing the C&A phases for systems in development.
- Worked with customer security team to ensure system information was properly entered in Xacta.
- Worked with Federal agencies to gain information about platforms and secure hosting facilities for system implementation.
- Outlined the C&A process and the resources, documentation and timeframes necessary to achieve authorization for a customized COTS product that was being operated on behalf of the government; helped customer to understand and establish criteria for a secure facility; collaborated with customer on secure login and authentication, documenting the accreditation boundary for the application, and defining interconnections with other government systems.
- Worked with Government COTR and agency security officer to develop security requirements for statement of work (SOW) for system services. Developed a requirements matrix, drafted text for tasks in the SOW, defined associated deliverables and expected delivery dates, and provided specifications for the general requirements to address NIST, agency and OMB requirements.

IntelliDyne, LLC, February 2003 – February 2005
PMO Manager
Supervised configuration, quality, facility, project, engineering design, and security management functions and personnel at multi-state locations for DoD contract. Developed program management planning, tracking and reporting mechanisms to demonstrate adherence to contract service levels for supporting over 2,000 users.

- Established PMO, standardizing processes and tools across projects, to include risk identification, tracking and reporting.
- Facilitated monitoring, communicating and reporting risks, by making information available via the intranet.
- Developed COOP scenarios for planning purposes to include threat identification, impact and response.
- Met with users seeking to add software/applications to the network and briefed them on the security requirements and associated process.
- Provided organization-wide briefings on security requirements, resources and timing for process implementation.
- Addressed special security requests, such as adding systems that housed HIPAA and PII to the network:
    - Oversaw team of mechanical and telecommunications engineers tasked with reengineering the server room to provide separate connectivity, UPS and COOP capabilities for the system.

    - Managed the security testing process where system developers and testers port applications to approved hardware and test them in approved network facilities to ensure that they are secure prior to bringing them on the network.
- Ensured that external connecting systems were certified and accredited, and internal systems and CPUs were scanned and complied with approved configurations monthly.
- Worked with IAO and Program Manager to analyze and address certifications and security incidents; defined appropriate actions, briefed the customer and implemented approved fixes.
- Collaborated with IAO to ensure that network security documentation was current, accurate, and could be produced when requested by network assessment team; worked with facility manager to ensure that systems were tested according to schedule and security requirements were met.

Interimage, Inc, September 2001 – September 2002
Project Director
Managed major contracts for the Chief Counsel, Internal Revenue Service, to design, develop and add systems to their intranet. Developed and implemented schedules and staffing, negotiated contract change requests and modifications, and adhered to strict security requirements. Served as the primary contact with clients and ensured a clear delineation of requirements and customer satisfaction with recommended solutions. Developed deliverables via a web platform, conforming to C2-level security and allowing customers to access files via online modules developed using SQL Server 7.0, HTML, DHTML, ASP, JavaScript, MS Access and associated tools.

Data Systems Division, Vector Research, Inc, September 1997 – September 2001
Operations Director
Oversaw the quality of deliverables for task orders, including program and project planning, requirements analysis, data and process modeling, business case analysis, prototype software development for electronic filing of tax and wage information, web site and application development and maintenance, security planning and risk assessment. Adhering to the IRS security process for prototype software development and the SDLC, developed system security documentation, met with IRS security personnel to review and answer questions regarding documentation, updated the documentation, underwent an external security audit of the facility and prototype software, and worked to remediate audit findings. System was approved for testing with IRS test group.

Federal Trade Commission, May 1992 – September 1997
Team Leader & Branch Manager for Information Management
Served as branch manager and team lead, planning and directing data management activities for a 1,000+ staff legal agency with a $1+ million annual budget. Oversaw agency records, forms, document management, publications; court reporting, automated case management; and data administration programs. Implemented FTC records management policies and procedures and developed electronic records schedules. Conducted impact analysis on FTC systems for Y2K and ensured OMB and regulatory compliance. Provided training and documentation for the case management system, developed technical specifications for data and records management contracts and served on technical evaluation panels.

Education

M.A. Russian Studies, Monterey Institute of International Studies (MIIS), 1987
M.A. International Policy Studies, MIIS, 1987
B.A. Russian (Management &Economics, 41 credits), Purdue University, 1985

Client Responsibilities

1. The County must be aware that ATA will not intentionally negatively affect any system where possible, but nothing can ensure this will not happen.
2. The County has created a full backup of all systems to be tested and has verified that the backup procedure will enable the County to restore their systems to pretest state.
3. The County has requested that their Internet facing network be assessed and will defend and hold ATA harmless from any liability or damage arising from the ATA team's performance under this penetration test.
4. will communicate to ATA if one of ATA's Internet Protocol (IP) addresses is flagged.
5. The County understands and agrees that the performance of these services may improve your security posture.
6. The County will collaborate with ATA if it is compromised, and will create test accounts for any additional testing, as necessary, or requested.

Potential System Outages

ATA consultants do everything they can to ensure that there are no system outages caused during our penetration testing. However, there is always a risk that testing could impact a system that is vulnerable to multiple security exploits. Due to this, ATA can accept no responsibility for any outages caused because of our testing.

This scope definition will describe the consulting services being delivered by this proposal. If any of the assumptions in this scope definition are not met by ATA or are proven to be inaccurate, then the scope, timing or fees for this engagement may be changed at ATA's discretion. These changes will be managed through the project change control process and may affect the project schedule and cost.

This proposal contains confidential and proprietary information of Advanced Threat Analysis, Inc. ("ATA"). The County may not disclose the confidential information contained herein to any third party without the written consent of ATA. As a condition of receiving this document, the County agrees to treat the confidential information contained herein with at least the same level of care as it takes with respect to its own confidential information, but in no event with less than reasonable care. This confidentiality statement shall be binding on the parties for a period of three (3) years from the issue date stated on the front cover unless superseded by confidentiality provisions detailed in a Master Services Agreement or a subsequent agreement.

This proposal will be void after 120 days unless a signed complete copy of this document is provided to ATA by that date. ATA reserves the right to vary the terms of this document in response to changes to the specifications or additional information made available by the County. Submission of this document by the County in no way conveys any right, title, interest, or license in any intellectual property rights (including but not limited to patents, copyrights, trade secrets or trademarks) contained herein. All rights are reserved. This proposal is based on

ATA's current understanding of the County's project requirements. ATA's offer specified herein is not binding except as specified in the Acceptance section of this document.

ATA does not assume liability for any errors or omissions in the content of any referenced third-party document. ATA reserves the right to correct any typographical errors, inaccuracies, or outdated information, and will notify the County of any changes required by such corrections. Any communication required or permitted in terms of this document shall be valid and effective only if submitted in writing.

Acceptance Criteria

ATA will deem the following to reflect the acceptance criteria of the deliverables:

1. **Kick off Presentation** – The Kickoff Presentation will be provided to the County at least 72 hours before the kickoff meeting. The Deck will be considered accepted after presented to the County. If revision is requested in writing, 24 hours must be given for ATA to correct and provide back to the County for review.
2. **Penetration Test Report** - The Penetration Test Report will be deemed accepted by the County after the final Document is supplied to the client unless revisions are requested within 96 hours of delivery. If no revision is requested for a period of 96 hours following the assets distribution to the client, the asset is deemed accepted.
3. **Final Review Presentation** – The Final Review Presentation will be provided to the County at least 72 hours before the final presentation meeting. The presentation will be considered accepted after being presented to the County If revision is requested in writing, 24 hours must be given for ATA to correct and provide back to the County for review.

Table 4: Acceptance criteria

Milestone	Acceptance Criteria
1 Initiate	The project kick-off meeting is completed. The County has been presented with ATA's testing methodology, team roles and responsibilities; and the County has been given a baseline MS Project Plan or Schedule.
2 Discover	Completion of testing scope and compilation of the County requirements.
3 Construct	The County has reviewed and approved the initial assessment findings.
4 Recommend	Delivery of the Final Summary Presentation to the County.

Proposal Acceptance

By signing below, the parties hereby confirm acceptance of and agreement to this proposal. Please return this entire document along with the signed proposal Acceptance Sheet via email to:
roger.colon@atacorporation.com

Advanced Threat Analysis, Inc.

Signature

Roger Colón, President/CEO

Date

Sauk County

Signature

Steve Pate / MIS Director
Print Name and Title

11/11/20
Date