ERIE COUNTY WATER AUTHORITY
INTEROFFICE MEMORANDUM

July 26, 2021

To: Jerome D. Schad, Chair
Peggy LaGree, Vice Chair
Michele Iannello, Treasurer

From: Terrence D. McCracken, Secretary to the Authority

Subject: Request for Proposal
Cybersecurity Risk & Vulnerability Assessment
Project No. 202100195

Commissioners:

As you are aware, on May 13, 2021 the Board of Commissioners (the "Board") authorized the issuance of a Request for Proposal (the "RFP") to qualified firms to provide the Erie County Water Authority with a Cybersecurity Risk and Vulnerability Assessment. The RFP was issued to five firms with a deadline of June 11, 2021. The RFP was also posted on the Authority's website. Eleven valid responses to the RFP have been submitted.

Senior Systems Engineer John Weider, Security Officer Matt Barrett, General Counsel Mark Carney, Senior Associate Attorney Margaret Murphy, Chief Executive Officer Russ Stoll, Chief Financial Officer Karen Prendergast and myself reviewed the submitted proposals (the "Committee").

A scoring matrix and points system was developed referencing each of the consultant's business structure, consultant's team, scope of services, insurance, registered to do business in New York State, references and pricing.

After a thorough review of the proposals, the Committee is recommending that the Board approves awarding a contract to GlobalSecurityIQ ("Global"). Global is a local company that the Committee feels is best fit to carry out the needs to perform a Cyber Security Risk and Vulnerability Assessment. With those thoughts in mind, the Committee respectfully requests consideration of awarding a contract to Global for the above referenced project.

Budget Information:
O&M Budget
Unit: 7510: General Expenses
Item No.: 20 – Miscellaneous

TDM:tf

# Erie County Water Authority

## Cybersecurity Risk & Vulnerability Assessment Summary

**Brief Background:**

- On May 13, 2021, the Board of Commissioners approved and authorized a Request for Proposal for a Cybersecurity Risk & Vulnerability Assessment. (Item #6).

- The Office of Secretary posted the RFP on the Authority's website and mailed the RFP to the following five companies:

    - Bonadio Group (Amherst, NY)
    - Dopkins & Co. LLP (Buffalo, NY)
    - Freed Maxick (Buffalo, NY)
    - GlobalSecurityIQ (Amherst, NY)
    - Sedara Security (Buffalo, NY)

- On June 11, 2021, **twelve companies** submitted proposals in response to the RFP:

    - Only **three of the five companies solicited by the Authority** responded to the RFP:

        - Freed Maxick CPAs P.C. (Buffalo, NY)
            - New York public corporation formed in 2011, formally Freed Sachs & Murphy, P.C. incorporated in 1958
            - Closed corporation
            - No related corporation listed.
            - No principal place of business listed, but indicates its has headquarters in Buffalo, Rochester and Batavia
            - Insurance Coverage
            - Consultant Team
            - Scope of Service

        - GlobalSecurityIQ, LLC (Amherst, NY)
            - Title indicates an LLC, but response states a Partnership
            - New York entity formed on July 3, 2017
            - Closed corporation
            - No related corporation listed

        - Principal place of business:  Amherst, NY
        - Insurance Coverage
        - Consultant Team
        - Scope of Service

    - Sedara (Buffalo, NY)
        - No proper corporate name given
        - New York corporation formed on November 7, 2013
        - Closed corporation
        - No related corporations
        - Principal place of business: Buffalo, NY
        - Insurance Coverage
        - Consultant Team
        - Scope of Service

- One company, **All About IT, Inc. (dba AAITPRO**), failed to submit a proper proposal and should be deemed **non-responsive**.

    - This company is foreign corporation based in India, but has a USA office in Houston, Texas (based on a Google search).

- **Eight companies outside of New York State** also submitted proposals:

  **NOTE:  We could not access the business search website of the New York Secretary of State.  NYSOS is updating the business search engine.  We have called NYSOS to check when the website will be back up, but they have no date when the website will be operational.**

  **CAUTION:**  An out-of-state entity must be registered to do business in New York State.

    - AESI-US, Inc.
        - Georgia Corporation formed on July 15, 1997
        - Closed corporation
        - Related corporation: AESI Acumen Engineered Solution International Inc.
        - Principal place of business: Tucker, GA
        - Insurance coverage
        - Consultant Team
        - Scope of Service

- Dean Dorton Allen Ford PLLC
    - Professional Limited Liability Corporation formed under the laws of Kentucky in 1921
    - Principal place of business: Lexington, KY
    - Insurance coverage
    - Consultant Team
    - Scope of Service

- Janus Software, Inc.(dba Janus Associates)
    - Florida Corporation formed on February 26, 1990
    - Closed corporation
    - No related corporations
    - Principal place of business: Stamford, CT
    - Insurance coverage
    - Consultant Team
    - Scope of Service

- O'Connor & Drew, P.C. (dba OCD-Tech)
    - Massachusetts Corporation formed on March 1, 1998
    - Closed corporation
    - No related corporations
    - Principal place of business: Braintree, MA
    - Insurance coverage
    - Consultant Team
    - Scope of Service

- Securance Consulting (Securance LLC) (password protected)
    - Florida LLC formed on March 4, 2002
    - Closed corporation
    - Principal place of business: Tampa, FL
    - Insurance Coverage
    - Consultant Team
    - Scope of Service

- Softchoice Corporation
    - Nonresponsive
    - Publicly traded
    - Related corporations:  Softchoice LP (Canada)
    - Principal place of business: Chicago, IL
    - Insurance Coverage
    - Consultant Team
    - Scope of Service

- Sleath-ISS Group® Inc.
    - Florida Corporation formed October of 2002
    - Closed corporation
    - No related corporation
    - Principal place of business: Arlington Virginia
    - Insurance Coverage
    - Consultant Team
    - Scope of Service

- True North Consulting Group, LLC
    - Texas LLC with inconsistent dates of formation
        - In business for 37 years
        - Date and State of Formation: 2014/Texas
        - Changed to an LLC in 2018
    - Principal place of business: Waco, TX
    - Insurance Coverage
    - Consultant Team
    - Scope of Service

- Minority/Women-Owned Business Enterprises – **Only one qualified MWBE**.
    - **GlobalSecurityIQ, LLC** (Amherst, NY)
        - MWBE Certifications from Erie County, State of New York, and U.S. Small Business Administration

    - Janus Software, Inc.(dba Janus Associates)
        - No County or State MWBE certificates
        - National MWBE Certification
        - Can supply NYC MWBE Certification

    - Sleath-ISS Group® Inc.
        - Has applied for WOBE to U.S. Small Business Administration, but not certification from U.S. SBA

- References: Each proposed Consultant has provided at least three references for entities for which they performed work. Some proposed Consultants did not submitted references for work relating to Cybersecurity Risk & Vulnerability Assessment. Below are relevant references for certain sectors involving a Risk & Vulnerability Assessment:

    - Public Water Systems
        - Janus Software, Inc.(dba Janus Associates)
            - Southern Central Connecticut Regional Water Authority
            - Massachusetts Water Resources Authority

        - Securance Consulting (Securance LLC)
            - Boston Water and Sewer Commission (Massachusetts)
            - Warren Co. Water District (Kentucky)

- Erie County Entities
    - GlobalSecurityIQ, LLC (Amherst, NY)
        - Town of Cheektowaga
        - Town of Orchard Park
        - Northtown Auto

    - Sedara (Buffalo, NY)
        - West Herr Automotive Group (but no indication as to the type of work)

- Public Utilities
    - AESI-US, Inc.
        - Lakeland Electric (Florida)
        - EPCOR Utilities (Canada)
        - New Brunswick Power (Canada)

    - Janus Software, Inc.(dba Janus Associates)
        - Norwich Public Utilities (Connecticut)

    - Securance Consulting (Securance LLC)
        - City of Fort Collins (Fort Collins Utilities – Colorado)

- Governmental Entities:
    - Dean Dorton Allen Ford PLLC
        - Jefferson Co. Public Schools (Kentucky)
        - Louisville Metro Government (Kentucky)

    - O'Connor & Drew, P.C. (dba OCD-Tech)
        - Bridgewater State University (Massachusetts)

    - Sleath-ISS Group® Inc.
        - Town of North Kingston (Rhode Island)
        - U.S. Department of Transportation

    - True North Consulting Group, LLC
        - Bi-State Development (Missouri)
        - City of Palm Beach Gardens (Florida)
        - Town of Dudley (Massachusetts)

- Pricing Structure:

    - Freed Maxick CPAs P.C. (Buffalo, NY)
        - Two Options
            - Option A: a Chinese menu of specific services, individual priced
                - Total Service Bundle: $71,000
                - On-going quarterly monitoring: $35,000 (not clear whether the price is for a year or a quarter)
            - Option B: three-year plan for specific services, totaling $85,000

    - GlobalSecurityIQ, LLC (Amherst, NY)
        - NIST-based Cybersecurity Risk Assessment: $24,975
        - Full internal/external vulnerability scan including a domain controller configuration audit: $8,900
        - Additional consulting: $389 per hour purchased in blocks of 20 hours: $7,780
        - Total with 20 additional hours: $41,655 ($33,875 + $7,780)

    - Sedara (Buffalo, NY)
        - $37,000 plus licensing fees in excess of $100,000

    - AESI-US, Inc.
        - Four pricing options, ranging from $47,000 to $55,800

    - Dean Dorton Allen Ford PLLC
        - $30,000 based on stated assumptions

    - Janus Software, Inc.(dba Janus Associates)
        - Chinese menu of specific services, individual priced
        - Total Service Bundle: $120,188

    - O'Connor & Drew, P.C. (dba OCD-Tech)
        - $16,500 for a defined list of services

    - Securance Consulting (Securance LLC)
        - $53,816

    - Softchoice Corporation
        - $79,645

  - Sleath-ISS Group® Inc.
    - $62,026.02

  - True North Consulting Group, LLC
    - $58,500

- **Consultants with Proposed Consulting Agreements and/or NDA**

  - Freed Maxick CPAs P.C. (Buffalo, NY)
    * Sample Network Security Authorization Agreement
    * General Business Terms

  - GlobalSecurityIQ, LLC
    * Standardize Agreement

  - Sedara (Buffalo, NY)
    *Standardize Agreement Terms

  - AESI-US, Inc.
    *Standard Contract
    *Non-Disclosure Agreement

  - Janus Software, Inc.(dba Janus Associates)
    * Standard Consultant Agreement

  - True North Consulting Group, LLC
    * Sample TNCG Consultant Agreement

JUNE 11, 2021

# ERIE COUNTY WATER AUTHORITY

Proposal for Cybersecurity Risk and Vulnerability Assessment Services

Trust earned.

FreedMaxick®

Trust earned.
FreedMaxick®

June 11, 2021

Terrence D. McCracken, Secretary to the Authority
Erie County Water Authority
295 Main Street, Room 350
Buffalo, New York 14203
Email: tmccracken@ecwa.org

Dear Terrence:

We appreciate the opportunity to propose on comprehensive IT Cybersecurity Risk and Vulnerability Assessment services for the Erie County Water Authority ("the Authority"). Freed Maxick CPAs P.C. ("Freed Maxick" or the "Firm") is enthusiastic about the prospect of supporting your cybersecurity program.

We understand that the Authority needs to adhere to regulatory standards and complex privacy regulations, maintain effective controls throughout the company, and protect the security of its information assets. Our dedicated Risk Advisory Services team has extensive experience leveraging our understanding of client risks and providing tailored services to large, complex organizations across many highly-regulated industries, including utilities We believe the following are our distinct advantages:

- **Extensive risk management and utility industry expertise**

  We have dedicated significant resources to develop leading edge expertise in Risk Management, with a depth of focus in both cybersecurity and privacy. The professionals in our Risk Advisory Services practice have extensive experience in information technology, information security, and business consulting. We have a proven methodology that we have executed successfully for public companies in numerous industries, including yours.

- **We've delivered proven results**

  Our assessment reports and deliverables were reviewed by the Public Service Commission of the State of New York in 2019, 2020, and 2021. We know we deliver quality, and we've backed that up by providing services that have been reviewed and noted as being satisfactory by regulators

- **Value for fees paid**

  Our collaborative approach to cybersecurity engagements results in a foundation for an overall security strategy that is scaled to meet your needs. Our proactive approach allows for strategic spending to achieve your cybersecurity goal as opposed to a massive unplanned spend resulting from a breach.

- **Partnership approach**

  We take the time to understand your business environment and associated risks. We strive to be a resource you can turn to for all your cybersecurity needs. Our technical knowledge combined with our depth of cybersecurity experience will allow for the development of strategies and tactical plans that will fit your organization's unique culture.

- **Strong project management**

  Our team has experience running large projects, creating and reporting against project plans, and coordinating resources to meet objectives. Our collaborative approach emphasizes communication and will help drive completion of the project so that you can achieve your compliance requirements.

We are committed to demonstrating the reasons we believe we are the best and most qualified firm to suit your needs. We have provided the details necessary to show how we can provide the greatest value to the Authority now and in the future.

Please contact us if you have additional questions.

Sincerely,

Freed Maxick CPAs, P.C.

David Hansen, QSA, CISA, CPA, CISSP
Director, Risk Advisory Services
david.hansen@freedmaxick.com
585-360-1481

Sam DeLucia, CISA
Risk Advisory Services Senior Manager
samuel.delucia@freedmaxick.com
585-360-1405

# Table of Contents

**PART 1** .......... **5**

**PART 2** .......... **6**

Item 1 - Consultant Business Form .......... 6

Item 2 - Consultant Team .......... 7

**PART 3** .......... **9**

Item 1 - Proposed Scope of Service .......... 9

Proposed Engagement Services .......... 10

NIST Cybersecurity Framework Assessment .......... 10

Penetration Testing Services .......... 10

Information Technology Process Review .......... 11

Assessment Services Detail .......... 11

Item 2 -Hardware and Software Requirements .......... 11

Item 3 -Timeframe for Deliverables .......... 12

Sample Engagement Timeline .......... 13

Item 4 -Price Structure .......... 14

Fees .......... 14

Proposed Pricing Options .......... 14

Pricing Option A: Bundled Service Listing—Select Desired Options .......... 15

Pricing Option B: Flex Pay Offering .......... 16

**Exhibits**

Exhibit A	Assessment Services Detail
Exhibit B	Sample Network Authorization Agreement
Exhibit C	Security Tools Listing
Exhibit D	General Business Terms
Exhibit D	Professional Biographies
Exhibit E	Certificate of Insurance

# PART 1

**Item 1 - Name of Individual or Organization**

Freed Maxick CPAs P.C.

**Item 2 - Name and Title of Contact Person**

David Hansen, QSA, CISA, CPA, CISSP, Director, Risk Advisory Services

**Item 3 -  Business Address**

424 Main Street, Suite 800 Buffalo NY 14202

**Item 4 - Telephone No.**

716.847.2651

**Item 5 - Email Address**

david.hansen@freedmaxick.com

**Item 6 -  Fax No.**

716.847.0069

# PART 2

## ITEM 1 - CONSULTANT BUSINESS FORM

1. **Identify the Consultant's business or corporate structure:**
   **(a) If a Corporation, including the following:**
   - **Date and State of Incorporation**
   - **List Name and Title of Executive Officers**
   - **Principal Place of Business**
   - **List all Related Principal or Subsidiaries Corporations**
   - **Closed or Publicly Traded**
   - **EIN**
2. **Identity the number of years your entity has been in business.**
3. **Identity whether your business/corporate structure has changed in the past fiveyears and if yes, describe the change.**

Freed Maxick CPAs, P.C. ("Freed Maxick", EIN 454051133 ) was founded as Freed Maxick Sachs & Murphy, P.C. in 1958. Freed Maxick was incorporated in 2011 but has been under consistent management of the Firm's Directors since its inception in 1958. Freed Maxick is one of the largest providers of professional services in Upstate New York, with over 320 professional and administrative staff. We are listed in the Public Accounting Report's annually updated list of the 100 largest accounting firms in the United States. We are headquartered in Buffalo, NY and have additional offices in Rochester, NY and Batavia, NY.

Freed Maxick operates as a professional corporation and is a privately owned and managed Certified Public Accounting firm. It is headed by a Managing Director and an executive committee provides additional oversight. Key executive officers are Henry Koziol, CPA, Managing Director; Mark Stebbins, CPA, Vice Chairman; Tom Berical, CPA, Treasurer, and Howard Epstein, CPA, Secretary. Internal department heads include a CFO, CMO, CIO, COO, and CHRO. Our corporate structure has not changed in the past five years.

4. **Identity the type and coverage amount of all insurance policies.**

We have attached a Certificate of Insurance showing our coverage types and amounts.

5. **Identify the name, address, and contract information for three (3) companies that the Consultant has performed similar services to those being sought by theAuthority.**

We attribute our success to our ability to attract and retain high quality clients like AVANGRID. As we hope you would agree, we have committed ourselves to growing to keep up with the service needs of our clients. The end result of these efforts has led to the development of a diverse client base across and within numerous industries, including yours. The following clients represent organizations with operating environments or engagements similar in nature to yours and would happily discuss their experiences with Freed Maxick and your engagement team.

**AVANGRID**
**Jen Spencer – Manager Privacy and Security**
jennie.spencer@avangrid.com | Cell 585.284.9388
Services Provided: Compliance with State of New York Public Service Commission (PSC) Order 13-M-0178 "Review of Security for the Protection of Personally Identifiable Customer Information" / Cybersecurity Assessments for NYS SHIELD and NIST

**IDI Billing Solutions**
**Patrick Talty – Vice President, Operations & Chief Security Officer**
ptalty@idibilling.com I 888.924.4110
Services Provided: PCI Compliance / Security Consulting / SOC Reporting
**Frontier Communications Corp I Ticker: FTR**
**David A. Keech – Vice President of Information Technology**

David.keech@ftr.com I 585.777.6932
Services Provided: PCI DSS Reporting, SOC Reporting

**Arizona Public Service Company I Ticker: PNW**
**Nick Petrishin – Manager, Audit Services**
nicholas.petrishin@pinnaclewest.com I 602.250.4838
Services Provided: Security and Privacy Internal Audit

**NOCO Energy Corp**
**Scott Ernst – Vice President, Corporate Operations**
Sernst@noco.com I 716.614.1150
Services Provided: IT Business Process Optimization and Redesign Consulting

Hearthstone Utilities, Inc. (Formerly Gas Natural, Inc.)
**Jed D. Henthorne – President and General Manager**
jhenthorne@egas.net I 406.791.7500
Services Provided: Sarbanes-Oxley Consulting / IT Controls

**6. If you are a certified, minority and/or women owned business, submit a copy ofthe certification.**

The Firm is not designated as an MWBE enterprise.

## ITEM 2 - CONSULTANT TEAM

**Identify the individuals whose professional services will be utilized to undertake a comprehensive IT Cybersecurity Risk and Vulnerability Assessment, including thoroughly reviewing the current state of the Authority's information technology security, developing a vulnerability mitigation plan, and developing a prioritized road map of activities to enhance the Authority's future Cybersecurity position. Please provide the following information for each identified individual:**

**(a) Relevant qualifications and experience, including educational degrees and any applicable licenses orcertifications (e.g., CISSP, CISM, CGEIT, CRISC), and**
**(b) State and county of residence, and**
**(c) Scope of responsibility, and**
**(d) Length of time working for Consultant.**

Freed Maxick is uniquely qualified to implement and oversee security programs due to our staff's extensive experience in information technology, information security, and business consulting. Freed Maxick staff is focused on applying their extensive technical knowledge and experience to provide independent verification and validation, technical assistance, and security oversight. Freed Maxick staff regularly provide subject matter expertise on security audits, reviews of technical system design documentation, deliverables, and performance.

The most critical element in the successful completion of any engagement of this nature is the personnel assigned to carry out the responsibilities. David Hansen, CPA, CISA, QSA, CISSP, Director, and Sam DeLucia, CISA, CISSP in progress, a Senior Manager with 20+ years of experience, will manage the project and provide overall quality control for this engagement. He will be supported by experienced professionals from our Risk Advisory Services Department—Alex Bliss and Tiffany Williams-- who have cybersecurity expertise and have the benefit of previously working on similar engagements. Justin Bonk, CIA, CISA, CFE, QSA, CISSP, CIPP/US, is available as a subject matter specialist, lending industry insight and technical expertise surrounding security and privacy. The core engagement team will be supported by senior and staff consultants from our Risk Advisory Services Practice.

Full professional biographies for each member of the engagement team that further address the above required criteria are attached as Exhibits. All staff assigned to this engagement are internal staff of Freed Maxick and reside in Western New York; including Erie County, NY and Monroe County, New York.

## STAFF TRAINING, PROFESSIONAL AND TECHNICAL CERTIFICATIONS

Our Firm is focused on its people and their personal and professional development. Our goal is to attract and retain the best people and provide them with superior development opportunities. We believe our people are our greatest asset; this philosophy guides our activities internally and externally, influencing how we serve clients while encouraging industry expertise and community involvement. This philosophy has been embedded into the firm’s talent management processes and systems. Our talent management process is designed to support our people throughout their employment cycle with Freed Maxick which starts at an entry-level Associate level and culminates with being promoted to Director. Our focus is to develop well-rounded business advisors to serve our clients’ business needs. We do this by providing educational opportunities through seminars, conferences, self-study, computer-based training, and the internet. We strive to make learning easy, convenient and effective.

We have an extensive training program covering a broad array of subjects that is designed to provide continuous learning and growth opportunities for our professionals, as well as to comply with various Continuing Professional Education ("CPE”) requirements. Each individual’s CPE is monitored by the firm on an annual basis. Web-based platforms are widely used to bring professionals up-to-date in an efficient and interactive manner on a variety of topics. In addition, we supplement our internal training with numerous conferences and seminars sponsored by the AICPA, IIA, MIS Institute, ISACA and ACFE.

A number of important factors contribute to collaborative and productive working relationships between companies and their service providers. These factors include the skills and personalities of the persons assigned to an engagement, the quality of the services delivered, experience, cost and more. We believe that we have unique qualities that distinguish us from other firms, including:

- Qualified personnel that specialize in risk management and auditing will staff this project. Therefore, the engagement will be performed efficiently and on a timely basis;

- Consultants who hold various professional certifications such as Certified Public Accountant (“CPA”), Certified Internal Auditor (“CIA”), Certified Information Systems Auditor (“CISA”), Certified Six Sigma Black Belt (“CSSBB”), Certified Information Systems Security Professionals (“CISSP”), Certified Information Privacy Professional (“CIPP”), in progress) or others;

- Employees whom all subscribe to the American Institute of Certified Public Accountants' (“AICPA”) Code of Ethics, and security consultants whom subscribe to the Information Systems Audit and Control Association's (“ISACA”), International Information Security Certification Consortium's (“ISC2”), and System Administration, Networking and Security (“SANS”) Institute's Codes of Ethics; and

- A mission and client service philosophy based on helping our clients succeed - providing services of the highest quality is a basic tenet of our Firm and we believe this fundamental strength is enhanced by our orientation to help clients anticipate future needs

# PART 3

## ITEM 1 - PROPOSED SCOPE OF SERVICE

**Working in consultation with the Authority's IT staff, the Consultant will be required to develop comprehensive IT Cybersecurity Risk and Vulnerability Assessment. Describe the scope of service, which the Consultant would recommend to the Authority, to undertake a comprehensive IT Cybersecurity Risk and Vulnerability Assessment. The scope should include the following elements, along with such elements will be performed on-site or off-site:**

*A detailed scope of services follows; below, we have indexed your requirements to the pertinent following sections.*

(a) **Review of current state of the Authority's information technology security,** *Included in the Cybersecurity Assessment*

(b) **Development of  a vulnerability mitigation plan, Included in vulnerability mitigation plan**

(c) **Development of a prioritized road map of activities to enhance the Authority's future Cybersecurity position,** *Included in the deliverables*

(d) **Best practice methodologies to ensure a standardized risk mitigation approach that will offer the highest risk reduction potential, complementing the "Framework for Improving Critical Infrastructure Cybersecurity", developed by the National Institute for Standards and Technology (NIST),** *Included in NIST CSF*

(e) **Assessment that includes but not limited to:**

- **Test for susceptibility to Advanced Persistent Threats (APTs) such as viruses, malware, Trojan horses, botnets, and other targeted attack exploits.** *Included in the Vulnerability Assessment*
- **Evaluate the Authority's current threat posture including antivirus and Intrusion Detection and Prevention (IDP) capabilities.** *Included in the System Maintenance and Management process review*
- **Evaluate the Authorities planned changes and improvements to the threat surface and assist identifying and addressing security concerns.** *Included in cybsecurity strategy and remediation - consultation*
- **Review the Authority's current Supervisory Control and Data Acquisition (SCADA) water systems for security vulnerabilities.** *Included in the Vulnerability Assessment*
- **Review wireless network system components for security vulnerabilities, validating system-specific operating systems and firmware versions for known exploits and recommend upgrades, updates, and mitigations.** *Included in process review – network management & vulnerability management & remediation*
- **Review current system-specific operating systems and firmware versions for known exploits and recommend upgrades, updates, and mitigations. This includes firewalls, switches and routers, Microsoft Active Directory, email and file servers, web servers, wireless routers, WAN, VPN, VoIP, and CCTV systems.** *Included in the Vulnerability Assessment*
- **Assess VoIP network system components for security vulnerabilities, validating system-specific operating system and firmware versions and reviewing for known exploits.** *Included in the Vulnerability* **Assessment, also included** *in process review – network management & system configuration/maintenance*
- **Review existing IT policies and procedures and make recommendations for changes and/or additional policy and procedure development.** *Included in process review-policy procedure*
- **Execute and review internal network vulnerability scans and external vulnerability and penetration scans and make recommendations to reduce the threat attack surface.** *Included in the vulnerability assessment & penetration test.*
- **Recommend or assist in selection of vulnerability scan software for purchase/license for continued use by the Authority after the assessment is complete** *Included in system selection*

## PROPOSED ENGAGEMENT SERVICES

Every business must ensure that it maximizes its investments in technology and leverages tools that provide competitive advantages. However, this means that cybersecurity exposures are one of the greatest risks facing every organization today. Protection of your business, operations and data is more critical than ever. Our assessments are designed to provide key stakeholders with awareness of the specific risks that the organization faces and provide assurance that appropriate controls and safeguards are in place, are at an adequate level of maturity, and in compliance with regulatory requirements. In addition, we aim to provide practical, cost-effective recommendations for enhancing your cybersecurity posture.

The Freed Maxick Cybersecurity Team will execute scanning and assessment services for the Company with the intention of providing a view into any weaknesses the Company may have that could potentially allow its systems and/or networks to be at risk. Specifically, these services include the following:

## NIST CYBERSECURITY FRAMEWORK ASSESSMENT

The NIST Cybersecurity Framework (NIST CSF) is organized into five key Functions – Identify, Protect, Detect, Respond, Recover. These five Functions provide a comprehensive view of the lifecycle for managing cybersecurity for the Erie County Water Authority. Freed Maxick will use this framework to generally assess cybersecurity related areas in fourteen Information Technology process areas:

- Access Controls
- Asset Management
- Backup and Recovery
- Business Continuity
- Desktop Management
- Governance
- Incident Response
- Network Management
- Risk Management
- System and Network Monitoring
- System Configuration
- System Maintenance
- Third-Party Vendor Management
- Training and Awareness

## PENETRATION TESTING SERVICES

Freed Maxick will execute scanning and assessment services for Erie County Water Authority with the intention of providing a view into any weaknesses Erie County Water Authority may have that could potentially allow the systems and/or networks to be at risk.

- **External Network Vulnerability Assessment** - Perform remote vulnerability scans, from outside of your network as an intruder would, with the goal of identifying and prioritizing weaknesses in the externally facing and accessible network and systems.
- **External Penetration Testing** - Upon completion of the external network vulnerability assessment the RAS team would then attempt to exploit any weaknesses identified in an attempt to gain access to the network in a similar manner as an external intruder would on your organization's publicly visible resources. This activity is typically conducted in a controlled manner to avoid impacts to production and is agreed upon with management prior to the start of any work.
- **Web Application Assessment -** Freed Maxick will review the Erie County Water Authority web applications and mobile application for security vulnerabilities that could leave system and related information susceptible to compromise and unauthorized access.
- **Internal Network Vulnerability Assessment** - Perform internal vulnerability scans which includes the same vulnerability scan as provided with penetration testing, but without the exploitation phase and deeper reporting that a penetration test provides. During the internal vulnerability testing, we will focus on assessing the configuration, maintenance, and usage of internal systems and network devices.
- **Social Engineering - Phishing & Spear Phishing –** Perform a series of 2-4 spoofed emails to selected employees in an effort to assess their understanding and awareness of cybersecurity during their daily activities.

## INFORMATION TECHNOLOGY PROCESS REVIEW

Freed Maxick has deep knowledge in IT operational processes; and our RAS team will interview key personnel, review existing documentation, perform configuration verification exercises, and will provide Erie County Water Authority with a deeper assessment of these processes; an overall process maturity rating for each area; and suggest remediation steps for improvement in each of these areas:

- Policy Review
- Recovery and Resiliency
- System Maintenance and Management
- Access Controls
- Network Management

## ASSESSMENT SERVICES DETAIL

We have included exhibits with information that will help you better understand our approach to the services to be performed.

## ITEM 2 -HARDWARE AND SOFTWARE REQUIREMENTS

**(a) Describe the required hardware and/or software necessary to implement Consultant's plan, if any.**
**(b) Describe the limitations of the service and/or equipment, if any.**
**(c) Identify whether the required hardware and/or software will be provided byConsultant or the Authority.**

We will conduct meetings and interviews virtually or in person, at your discretion and in accordance with current guidance surrounding COVID-19. Additionally, we will ship preconfigured, sanitized laptops to your IT department so that scanning can be performed without the need for your staff to interact with outside visitors. We have included a listing of the security tools that may be used during the course of this engagement as an exhibit.

## ITEM 3 -TIMEFRAME FOR DELIVERABLES

**Provide a timeframe for completing the following deliverables:**

1. **Project Management Deliverables:**
   (a) **Work Breakdown Schedule (WBS) including tasks,**
   (b) **Schedule and dependencies, and**
   (c) **Weekly Status Reports including risks and progress reports.**

Our philosophy is to create and maintain continuous communication with management and keep them well-informed throughout the engagement. We will begin the work described in this proposal on a mutually agreed start date. A detailed schedule will be issued upon appointment and after we have met with key stakeholders.

A sample engagement timeline is included on the following page.

2. **Report: A written report documenting:**
   (a) **Executive summary detailing the Authority's Cybersecurity position, including a comparative scorecard of findings,**
   (b) **Results of vulnerability testing performed,**
   (c) **Identified cybersecurity vulnerabilities, gaps, and mitigation plans,**
   (d) **A prioritized road map of activities, developed in conjunction with Authority's IT staff to enhance the Authority's future cybersecurity position.**

Emphasis will be put on expediency of reporting results without compromising the integrity of the process itself. The availability and support of management and IT personnel during the performance of these services will be a key contingency on the final timeline of report delivery.

3. **Projected solutions and costs:**
   (a) **Provide an estimated range, based upon previous experience, of the total services costs to implement the proposed solutions,**
   (b) **Include a Rate Sheet that specifies and itemizes the cost for each proposed component, including all licensing, support, maintenance, and hosting fees,and**
   (c) **For subscription-based services, provide annual pricing.**

We have included a detailed approach to pricing in **Item 4** of this Proposal.

## SAMPLE ENGAGEMENT TIMELINE

Below is a suggested timeline for all activities contained within this proposal. The mix of services rendered and associated timing is flexible and will be modified to meet your needs.

| | 12-Jul | 19-Jul | 26-Jul | 2-Aug | 9-Aug | 16-Aug | 23-Aug | 30-Aug | 6-Sep | 13-Sep | 20-Sep | 27-Sep | 4-Oct | 11-Oct | 18-Oct | 25-Oct | 1-Nov | 8-Nov | 15-Nov | 22-Nov | 29-Nov | 6-Dec | 13-Dec |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **NIST CYBER-SECURITY FRAMEWORK ASSESSMENT** | | | | | | | | | | | | | | | | | | | | | | | |
| IT Risk Assessment | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | | | | | | | | |
| **PENETRATION TESTING SERVICES** | | | | | | | | | | | | | | | | | | | | | | | |
| External Network Vulnerability Assessment & Penetration Testing | | | | | | | ■ | ■ | ■ | | | | | | | | | | | | | | |
| Web Application & Android Application Assessment | | | | | ■ | ■ | ■ | | | | | | | | | | | | | | | | |
| Internal Network Vulnerability Assessment | | | | | | | | | | ■ | ■ | ■ | ■ | ■ | | | | | | | | | |
| Social Engineering - Phishing & Spear Phishing | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | | | | | | | | | |
| **INFORMATION TECHNOLOGY PROCESS REVIEW** | | | | | | | | | | | | | | | | | | | | | | | |
| Policy Review | | | | ■ | ■ | ■ | ■ | ■ | | | | | | | | | | | | | | | |
| Recovery and Resiliency | | | | | | | | ■ | ■ | ■ | ■ | ■ | ■ | | | | | | | | | | |
| System Maintenance and Management | | | | | | | | | | | ■ | ■ | ■ | ■ | ■ | ■ | ■ | | | | | | |
| Access Controls | | | | | | | | | | | | | | | | ■ | ■ | ■ | ■ | ■ | | | |
| Network Management | | | | | | | | | | | | | | | | | | | ■ | ■ | ■ | ■ | ■ |

## ITEM 4 -PRICE STRUCTURE

1. **Provide a detailed description of the Consultant price structure or pricing option for the services to be provided by the Consultant**

   Please see below.

2. **If the Consultant has a standardize agreement used for such services, include a copy with the Proposal.**

   We have included both our General Business Terms and a Sample Network Authorization Agreement in the Exhibits.

## FEES

We estimate our engagement fees based upon anticipated time and effort, the skill level of personnel needed, and rates set by our Firm, appropriate to the local market. Each engagement is carefully planned, and a time budget is established for each phase of our work. The time of each individual involved is accounted for, and all staff members are well indoctrinated on the need to control and spend time to the best advantage.

Our fee estimates do not reflect the effects of changes in planned scope or level of effort that may be required resulting from the Company’s staff turnover, adoption of new accounting principles or auditing standards, identification of fraudulent activity, significant regulatory changes or other unanticipated operational changes that may bear on matters related to the audit or financial reporting. We recognize that the accounting profession and the regulatory environments continue to evolve, and we pledge to work with your organization closely to mitigate the impact such changes may have on the engagement.

We will keep management informed of all changes in reporting and filing requirements and you will know what impact they will have on your professional fee before any work is started.

## PROPOSED PRICING OPTIONS

Freed Maxick recognizes that a one size fits all approach to assessing security strategies and managing a broader cybersecurity program does not adequately address the day-to-day realities of all organizations  Each organization must take different steps to secure itself, its information, and has different sets of priorities for its business.

**With this in mind, we have provided two approaches to pricing: a bundles service offering allowing you to select only the services you need at this time, and a flex pay option that prioritizes services based on risk**.

## PRICING OPTION A: BUNDLED SERVICE LISTING—SELECT DESIRED OPTIONS

| Service | | | Cost |
|---|---|---|---|
| NIST CYBERSECURITY FRAMEWORK ASSESSMENT | Option #1 | **IT Risk Assessment**<br>*Assessment the ECWA IT environment using NIST CSF* | **$15,000** |
| PENETRATION TESTING SERVICES | Option #2 | **External Vulnerability Assessment & Penetration Testing**<br>*Remote vulnerability scan on externally facing systems and attempt to exploit any weaknesses identified in to gain access from outside of your network, simulating an intruder* | $7,000 |
| | Option #3 | **Web Application & Android Application Assessment**<br>*Review the Erie County Water Authority web applications & Android mobile application for security vulnerabilities* | $14,000 |
| | Option #4 | **Internal Vulnerability Assessment**<br>*Remote vulnerability scans on designated internally facing systems to identify systems that require additional maintenance and remediation protections* | $17,000 |
| | Option #5 | **Social Engineering - Phishing & Spear Phishing**<br>*Perform a series of 2-4 spoofed emails to selected employees* | $7,000 |
| | Option #6 | **Bundled Penetration Testing Services Above**<br>*Includes discounted Option #2 through #5 above* | **$36,000** |
| INFORMATION TECHNOLOGY PROCESS REVIEW | Option #6 | **Policy & Process Review**<br>*Assessment of existing Cybersecurity Policies to identify gaps with the existing policies and enumerate any additional policies required* | $5,000 |
| | Option #7 | **Recovery and Resiliency Review**<br>*Assessment of both Business Continuity/ Disaster Recovery & Backup & Restoration Controls* | $5,000 |
| | Option #8 | **System Maintenance and Management**<br>*Assessment of the existing System Maintenance and Management Processes* | $5,000 |
| | Option #9 | **Access Controls Review**<br>*Assessment of both Access Management & Authentication Controls* | $5,000 |
| | Option #10 | **Network Management Review**<br>*Assessment of General Wired, Wireless, and Remote Network Controls* | $5,000 |
| | Option #11 | **Bundled Policy & Process Review Services Above**<br>*Includes discounted Option #6 through Option #10 above* | **$20,000** |
| BUNDLE ALL | Option #10 | **Bundled ALL Services Above**<br>*Includes discounted Option #1 through Option #9 above* | **$71,000** |
| QUARTERLY VULNERABILITY ASSESSMENTS | Ongoing Monitoring | **Ongoing Quarterly Vulnerability Identification**<br>*Performing vulnerability scanning of the external and internal network environments on a quarterly basis to identify vulnerabilities that should be addressed by Erie County Water Authority* | **$35,000** |

## PRICING OPTION B: FLEX PAY OFFERING

While we recognize the need to assess all of the areas illustrated above as part of a comprehensive cybersecurity program, we understand that a long - term cybersecurity strategy often includes a series of assessments larger in scope than originally anticipated. We recognize that no client has unlimited time and unlimited resources and we pride ourselves on being a firm that is a Trusted partner and flexible with our approach, scheduling, and costing. Many organizations will approach these assessments as parts of a longer project, prioritizing assessments based on risk.

We have provided an example of a prioritized approach to meeting your needs and developing a long-term cybersecurity strategy.

| | PROPOSED FREQUENCY | | |
|---|---|---|---|
| Description of Services | 2021 | 2022 | 2023 |
| NIST CYBERSECURITY FRAMEWORK ASSESSMENT | | | |
| IT Risk Assessment | | X | |
| | | | |
| PENETRATION TESTING SERVICES | | | |
| External Network Vulnerability Assessment & Penetration Testing | X | | |
| Web Application & Android Application Assessment | | X | |
| Internal Network Vulnerability Assessment | X | | |
| Social Engineering - Phishing & Spear Phishing | | | X |
| | | | |
| INFORMATION TECHNOLOGY PROCESS REVIEW | | | |
| Policy Review | | | X |
| Recovery and Resiliency | | X | |
| System Maintenance and Management | X | | |
| Access Controls | | | X |
| Network Management | X | | |
| | $34,000 | $34,000 | $17,000 |

# Exhibit A

## Assessment Services Detail

## ASSESSMENT SERVICES DETAIL

The items listed below are not an exhaustive list of all Freed Maxick Cybersecurity services, and they are intended to explain items specific to this proposal.

**Recovery and Resiliency Process Review:**

1. Reviewing the existing Business Continuity Process and the associated plan.
2. Understanding and documenting the related processes used in BC/DR.
3. Identifying the critical components required for BC/DR including business impact analysis, risk assessment, prioritization of systems and restoration activities, plan and procedural documentation, communication protocols, BC testing/exercises, etc.
4. Identifying any opportunities for improvement related to BC/DR.
5. Reviewing the existing Backup & Restoration Processes.
6. Identifying the critical components required for the Backup & Restoration Process including prioritization of systems and data, restoration activities, backup schedule, backup notification process for failed and successful backups, and remediation procedural documentation, backup testing/exercises, etc.
7. Understanding and documenting the application and technical infrastructure landscape relevant to the Backup & Restoration Process, while prioritizing critical systems where student and employee information, along with Erie County Water Authority critical operating information is kept.
8. Identifying any opportunities for improvement related to the Backup & Restoration Process.

**System Maintenance & Management Process Review:**

1. Reviewing the existing System Maintenance and Management Processes.
2. Identifying the inventory of servers, operating systems, patch and version levels.
3. Identifying the supporting technologies, such as anti-virus/malware and intrusion detection applications.
4. Understanding and documenting the related processes used for building, patching, supporting, monitoring for health and monitoring for events and incidents throughout the environment, including the vulnerability assessment and remediation processes.
5. Identifying any opportunities for improvement related to the configuration and support of systems.

**Access Controls Process Review:**

1. Understanding and documenting the application and technical infrastructure landscape, while prioritizing critical systems where student and employee information, along with Erie County Water Authority critical operating information is kept.
2. Reviewing existing access on a limited amount of systems for obvious inappropriate access, such as terminated employees or accounts with long periods of inactivity.
3. Understanding and documenting the processes used for managing user access (adding and removing user access, along with reviewing access rights).
4. Identifying any opportunities for improvement related to Access Management.
5. Understanding and documenting the process used to authenticate a user to critical systems and networks.
6. Reviewing existing authentication controls
7. Identifying any opportunities for improvement related to Authentication

**Network Management Process Review:**

1. Understanding the network architecture with its control points for both protecting and monitoring.
2. Identifying areas where a single point of failure could potentially occur, or redundancy may be lacking.
3. Identifying areas where additional monitoring may be required.
4. Reviewing existing practices for network and network device management.
5. Reviewing remote access processes for Erie County Water Authority employees, and students, including the controls associated with remote access
6. Reviewing Erie County Water Authority wireless network management practices.
7. Identifying any opportunities for improvement related to Network Management.

**Internal Vulnerability Assessments:**

The vulnerability assessment includes the same vulnerability scan as provided with penetration testing, but without the exploitation phase and deep reporting that a yearly penetration test provides. During the internal vulnerability testing, we will focus on assessing the configuration, maintenance, and usage of systems and network devices. Industry recognized tools are used to scan systems and provide a generic report directly from the assessment tool that provides priority rated findings for quarterly remediation activity by your teams.

Theoretically, a quarterly vulnerability scan provides your organization with a listing of items that require improvement based on industry recognized scoring, Common Vulnerability Scoring System (CVSS), to provide your organization with prioritized tasks to improve each quarter before the next quarterly scan.
It is important to note that a vulnerability scan alone is not the equivalent to a penetration test. Both periodic cycles of vulnerability scans with organizational remediation and the penetration testing, is recommended for a holistic approach to assessments and scanning.

For more information please read our Freed Maxick Blog: "Vulnerability Assessment vs Penetration Testing: What's the Difference?"
http://blog.freedmaxick.com/summing-it-up/vulnerability-assessment-vs-penetration-testing-whats-the-difference

**External Vulnerability Assessments:**

Similarly, to the internal vulnerability assessment the external vulnerability assessment is also ongoing process each quarter includes the same vulnerability scan as provided with penetration testing, but without the exploitation phase and deep reporting that a yearly penetration test provides. The approach for the external vulnerability assessment differs slightly from the internal assessment in that it focuses on the externally facing systems that your organization has. These systems and networks become the first line of defense to an external intruder. Scans are performed from an external source and findings are usually limited to how well your organization secures its perimeter network and systems. The external vulnerability scan also provides your organization with a listing of items that require improvement based on industry recognized CVSS scoring, to provide your organization with prioritized tasks to improve each quarter before the next quarterly scan on all externally facing systems.

**Social Engineering – Phishing & Spear Phishing:**

Our team of security consultants will work with you to configure and test our social engineering platform followed by initiation of various phishing campaigns designed to test end-user susceptibility to related security threats. Our team will design and specifically craft phishing simulations that are designed to teach your users how to identify phishing scams from various sources.

Freed Maxick will conduct various social engineering campaigns entailing the following:

- An initial phishing campaign sending two to three emails to each end user over at undisclosed times over a period of several weeks
- At least one of the campaigns will be specifically designed to be more focused on select individuals as a spear phishing campaign
- Reporting of results and recommendations on improving employee awareness

**Web Application Assessement:**

The Freed Maxick application security review is designed to test for application-level vulnerabilities that may exist due to configuration or coding errors. The objective of an application security review is to demonstrate that exploitable application-level vulnerabilities exist, not to demonstrate that an application is free of all vulnerabilities.

Using provided application and administrative credentials, our application security review will be completed by:

- Exploring the application and creating a list of potential application vulnerabilities,
- Using our web application vulnerability scanning tools, and
- Evaluating and testing these potential vulnerabilities and attempting exploitation.

Based on the outcome of the testing, appropriate recommendations are made to improve the security level of the application. Our web application security review includes tests specifically designed to identify issues based on the Open

Web Application Security Project (OWASP) Top 10 listing of the most common and risky vulnerabilities (https://owasp.org/www-project-top-ten/):

- Injection Attacks
- Broken Authentication and Session
- Management
- Cross-Site Scripting (XSS)
- Broken Access Control
- Security Misconfiguration
- Sensitive Data Exposure
- Insufficient Attack Protection
- Cross-Site Request Forgery (CSRF)
- Using Components with Known
- Vulnerabilities
- Under protected APIs

**Penetration Testing:**

The scope of this phase will focus on the organization's externally assessable systems and internal data networks. During internal network vulnerability assessment, we will focus on assessing the configuration, maintenance, and usage of systems and network devices. Testing also covers the relations between these resources, including insecure communications between systems, weaknesses in access and authentication controls, and inappropriate segregation of critical systems, applications and databases.

The testing approach includes both automated and manual methods in order to take advantage of the benefits of both techniques. Automated testing provides a cost-effective method to analyze large swaths of an environment at once, which can reveal a variety of systemic issues, but this approach is also prone to a high level of false positive results. This style of testing is viewed as being "broad" rather than "deep." Manual methods are utilized to perform complex testing techniques, as well as to validate the findings identified with automated tools.

Based on the results and information gathered from our vulnerability testing, we will work with you to coordinate identifying vulnerabilities to be exploited. We will attempt to exploit identified and agreed-to vulnerabilities to determine the true risk of the vulnerability and establish that a real vulnerability exists.

The External Network Vulnerability Assessment and Penetration Testing consists of assessing and identifying key vulnerabilities your organization's external network and attempting to penetrate those vulnerabilities to gain remote access. Our external testing approach focuses on analyzing those perimeter network devices and systems for weaknesses in configuration, maintenance, usage, access and authentication. Our Freed Maxick Methodology incorporates our experience, knowledge, and techniques to identify both systemic issues as well as complex vulnerabilities.

External testing differs from internal testing primarily in the approach for finding targets, as well as the coordination with both parties to leverage the maintenance windows or system slow time to avoid production impacts. For external testing, we often mimic the activities of real attackers and attempt to use traditional "foot-printing" and enumeration techniques to properly identify the client's Internet-facing systems rather than have the client provide us with lists of Internet Protocol (IP) addresses. This provides the clients insight into what attackers can glean from publicly available information sources, as well as presents the opportunity for our testers to find externally visible systems that were unknown to the client.

The external testing revolves around the approved testing times. It is far more likely that if an operational issue were going to occur because of the security testing, it would occur during the internal section of the assessment. Testing equipment inside the environment can generate far more traffic than expected, and this traffic is traversing the same network segments as the day-to-day user and operational traffic. Testing equipment outside the environment interacts with the target's systems in much the same way as any other type of Internet traffic, and those target systems are built to handle extremely high levels of interaction. In addition, standard security devices, such as firewalls and IPSs, often block much of the testing traffic so that only portions of it actually arrive at the exposed servers. Because of these points, external testing often does not occur during designated testing windows or in windows only meant to exclude specific, high-traffic days. We will gladly perform external testing during desired maintenance windows, but this could greatly extend the duration of the testing. In addition, if security testing does affect the environment, this should be viewed as a finding in and of itself. If approved security testers can degrade service by using common security tools during a scheduled test, malicious attackers can do the same at any time they wish.

For external testing, our initial actions mimic several of the activities performed by an attacker to conduct reconnaissance of their target. Our security consultants begin testing knowing only the name and location of the client. They are unaware of your networks and/or systems and rely only on their skills, experience and abilities to document your external network and identify initial potential weaknesses. By performing these activities, they use their knowledge of technology and exploits to gather information regarding the target systems.

Our penetration testing utilizes skilled professionals that are experienced, and dedicated, to performing vulnerability and penetration testing for our clients. They utilize a testing methodology that involves at a minimum - manual verification of vulnerabilities discovered using tools and other techniques; exploitation of verified and real vulnerabilities using Level 1 attack vectors.
It is possible that there may be some high-risk vulnerabilities that we mutually agree to not penetrate due to the potential risk to system stability.

Activities performed can include:

- “Foot-printing” of external systems - The foot-printing process helps to determine the amount of information available through public sources concerning your organization. Once gathered, we then determine the value of the information obtained through the foot-printing process that could further our efforts to compromise your network. Our foot-printing process can include, but is not limited to, the following activities:

    - Online telephone directory searches
    - Website(s) reviewed for information-gathering potential
    - Mapping of domain names used
    - Mapping of domains linked to your domain names used
    - Web searches performed to discover any private or sensitive information available through public sources
    - American Registry of Internet Number searches
    - Domain Name Service lookups
    - Traceroutes of public systems

- Basic analysis for internal and external systems
    - Common services such as Hypertext Transport Protocol (HTTP), Hypertext Transport Protocol Secure (HTTPS), File Transfer Protocol (FTP), Telnet, Simple Network Management Protocol (SNMP) and finger
    - All active Transmission Control Protocol (TCP) ports
    - All active User Datagram Protocol (UDP) ports
    - Operating systems and software versions
    - Trivial security issues resulting from configurations, default passwords and insecure protocols
    - Obvious information exposure and use of unnecessary services

During vulnerability assessment, we focus on assessing the configuration, maintenance and usage of systems and network devices. The testing approach includes both automated and manual methods in order to take advantage of the benefits of both techniques. Automated testing provides a cost-effective method to analyze large swaths of an environment at once, which can reveal a variety of systemic issues, but this approach is also prone to a high level of false positives results.

This style of testing is viewed as being “broad” rather than “deep.” Manual methods are utilized to perform complex testing techniques, as well as to validate the findings identified with automated tools. Examples of both tool sets are listed in the Security Tools section of this document.

Because our testing can be intrusive in nature and there is a remote possibility of causing system outages, we schedule these tests with all necessary parties involved.

The length of time needed for penetration testing will vary greatly depending on the number and type of vulnerabilities found in the previous step.

# Exhibit B

## Sample Network Security Authorization Agreement

THIS AGREEMENT by and between Client (hereinafter "Client") and Freed Maxick CPAs, P.C. (hereinafter "Freed Maxick"):

**WITNESSETH:**
**WHEREAS, Freed Maxick is engaged in the business of network and information security and vulnerability review and analysis services, and**

**WHEREAS, Client desires that Freed Maxick perform a network and information security and vulnerability review of Client's computer system and network by acceptance of Freed Maxick's engagement letter dated "Date", and**

**WHEREAS, Freed Maxick's conduct of network and information security and vulnerability review services as defined above may cause interruptions or disabling of Client's information processing capabilities, and**

**WHEREAS, Freed Maxick's network and information security and vulnerability review procedures are not legal without Client's explicit permission, and Client desires by this written authorization to provide Freed Maxick with Client's express written consent and instruction to perform said procedures on Client's behalf.**

**NOW, THEREFORE, intending to be legally bound, in consideration of the preceding recitals, the mutual covenants herein and other good and valuable consideration (the receipt and adequacy of which are hereby acknowledged), the parties agree as follows:**

## SECTION 1

### 1. SCOPE OF SERVICES

1.1. Services. **Freed Maxick** agrees to provide, and **Client** wishes **Freed Maxick** to provide, the consulting services for network and information security and intrusion testing as defined in **Freed Maxick's** attached engagement letter dated "Date" (the "Engagement Letter") (collectively, the "Services"). The Services may include but are not limited to:

- Electronic network scanning and testing. These procedures include, but are not limited to, use of software tools and techniques to gain information about **Client's** external and/or internal network connections and devices connected to those networks, and the use of non-destructive tools and techniques to test **Client's** external and/or internal network connections and devices connected to those networks; and
- Electronic network attacks. These procedures include, but are not limited to, the use of software tools and techniques to attack **Client's** networks and devices connected to those networks.

1.2. Method of Performing Services. **Freed Maxick** shall have the right to determine the method, details, and means of performing the work to be performed for **Client**. **Client** shall, however, be entitled to exercise general power of supervision and control over the results of work performed by **Freed Maxick** to assure satisfactory performance, including the right to inspect, the right to stop work, the right to make suggestions or recommendations as to the details of the work, and the right to propose modifications to the work.

1.3. Reporting. **Client** and **Freed Maxick** shall develop appropriate administrative procedures for coordinating with each other. **Freed Maxick** shall periodically provide **Client** with status reports documenting work performed and interim results. **Client** shall periodically provide **Freed Maxick** with evaluations of **Freed Maxick's** performance.

## SECTION 2

### 2. AUTHORIZATION TO CONDUCT PROCEDURES; CLIENT'S RESPONSIBILITIES

2.1. Engagement. **Client** hereby engages **Freed Maxick** to perform the Services. **Client** hereby authorizes and directs **Freed Maxick** to perform the Services on **Client's** behalf and expressly consents to **Freed Maxick's** performance of the Services.

2.2. Security Testing Authorization. **Client** hereby authorizes **Freed Maxick** during its network and information security and vulnerability review procedures to attempt to break into **Client's** computer systems, and consents to **Freed Maxick's** use of penetrating techniques and strategies to attack **Client's** existing security systems.

2.3. Responsibilities. **Client** shall comply with all applicable laws, regulations and statutes relating to **Client's** authorization and instructions to **Freed Maxick** to perform the Services. In the event that one or more IP addresses specified by **Client** identifies computer systems that are not owned by **Client**, including, but not limited to, firewalls, routers, and World Wide Web servers, **Client** agrees to:

- Be solely responsible for communicating any risks, exposures, and vulnerabilities identified on these computer systems by **Freed Maxick's** network and information security and vulnerability review services to system owner(s), and for ensuring that the system owner(s) takes all appropriate actions; and
- Facilitate the exchange of information between the system owner(s) and the **Freed Maxick's** project team, as necessary.

**Client** agrees to inform **Freed Maxick** immediately, during the conduct of network and information security and vulnerability review services, whenever there is a change in ownership of any system identified by the IP addresses communicated to **Freed Maxick**.

## SECTION 3

## 3. ACCEPTANCE OF LIMITATIONS AND RISK

3.1. Limitation Of Liability. **Freed Maxick** shall not be liable for any delays or failures in performance due to circumstances beyond our reasonable control. Freed Maxick's total liability to Client relating to this engagement, including but not limited to any loss of service or data resulting from Freed Maxick's performance of the Services whether arising from tort or contract claim, will in no event exceed an amount equal to the fees we receive from you for the portion of the engagement giving rise to liability, and will not include any special, consequential, incidental, punitive or exemplary damages or loss (nor any loss of profits, savings, data, use of software or hardware or business opportunity, or interruption of business) even if we have been advised of the possibility of such loss, except in cases of **Freed Maxick's** intentional misconduct.

3.2. Acceptance Of Risk. **Freed Maxick** will take reasonable precautions to avoid causing one or more devices to become inoperative and result in loss of **Client's** service or data. However, **Freed Maxick** cannot accurately predict those devices that could be adversely affected by its network and information security and vulnerability review methods. Therefore, **Client** understands and accepts the risk that **Freed Maxick's** performance of the Services may inadvertently cause one or more devices to become inoperative and result in loss of service or data.

# Exhibit C

## Security Tools

**Security Tools**

Our Team uses a number of tools when performing our internal and external scans and penetration testing of enterprise networks. The following is a list of the tools available to our security consultants to assess an organization's data network. We may not use all of these Tools during an assessment. This list is provided to illustrate the variety and breadth of tools that can be used by our security consultants during network security reviews.

| Specialized IT Tools | Description |
|---|---|
| Tenable Nessus 8.0 | One of the most popular network vulnerability scanners in the world. In use with many large organizations across many industries. |
| Netsparker | Web application security scanner that targets high-risk externally facing vulnerabilities including SQL injection and cross-site scripting. |
| Rapid 7 Metasploit Framework | Former open-source penetration testing framework and vulnerability exploitation database. Metasploit is the most common exploitation tool used in both penetration testing and malicious hacking. |
| Armitage | Also developed around the Metasploit framework, Armitage allows a penetration tester to use "Pivoting" to target multiple machines in a network if one externally facing computer is compromised. |
| Microsoft Baseline Security Analyzer (MBSA) | MBSA is used to determine the security state of Microsoft products by assessing missing security updates and weak security settings within a target range of systems. The results of these scans can be used to target specific machines during the penetration test. |
| NMap | As a network mapping and inventory tool, NMap captures all open ports and services running within the scope of an IP range. This information can be imported into one of our commercial tools for a more targeted and less intrusive test. |
| Kali Linux | A Debian Linux distribution that is focused on penetration testing and offensive security. |
| Python | Programming language used in the development of custom exploits and security tests. |

Our team also uses several tools that provide an automated technique for performing information systems (IS) audits and documenting the results. The following is a list of the tools available to Freed Maxick's security consultants to assess an organization's security parameter environment.

| Audit Tools | Description |
|---|---|
| CSVDE Analyzer | Analysis of Windows Domain Controller (Active Directory) extract that defines specific security parameters including group policy parameters, global policy parameters, access control lists and event logging policy. |
| WireShark | A packet analyzing suite used for network troubleshooting, analysis and transmission audits. |
| Nipper | Enables logging and reporting on the security parameters established on network infrastructure devices, most notably firewalls. The reports provided by Nipper offer a detailed security audit trail and configuration report to identify weaknesses in the security configuration of most managed network devices. |

# Exhibit D

## General Business Terms

## GENERAL BUSINESS TERMS

These General Business Terms (the “Terms”) will govern the services provided by Freed Maxick CPAs, P.C. (“Freed Maxick”) as set forth in the attached engagement letter dated mm/dd/yy (the “Engagement Letter”) executed by Client (“Client”) and Freed Maxick to which these Terms are attached. These Terms, together with the Engagement Letter and any of its attachments, constitute the entire understanding and agreement between Client and Freed Maxick with respect to the services described in the Engagement Letter (collectively, the “Agreement”), supersede all prior oral and written communications, and may be amended, modified or changed (including changes in scope or nature of the services or fees) only in writing when signed by both parties. If there is a conflict between these Terms and the terms of the Engagement Letter, these Terms will govern.

**1. Confidentiality** With respect to any information supplied in connection with this Agreement and designated by either party as confidential, or which the recipient should reasonably believe is confidential based on its subject matter or the circumstances of its disclosure, the recipient agrees to protect the confidential information in a reasonable and appropriate manner, and use and reproduce the confidential information only as necessary to perform its obligations under this Agreement and for no other purpose. The obligations in this section will not apply to information which is: (i) publicly known; (ii) already known to the recipient; (iii) lawfully disclosed by a third party; (iv) independently developed; or (v) disclosed pursuant to legal requirement or order. Subject to the foregoing, the recipient may disclose the confidential information on a need-to-know basis to the recipient’s contractors, agents and affiliates who agree to maintain its confidential nature.

**2. Deliverables** (a) Upon full payment of all amounts due Freed Maxick in connection with this Agreement, all right, title and interest in the deliverables set out in the Engagement Letter will become Client’s sole and exclusive property, except as set forth below. Freed Maxick will retain sole and exclusive ownership of all right, title and interest in its work papers, proprietary information, processes, methodologies, techniques, ideas, concepts, trade secrets, knowhow and software, including such information as existed prior to the delivery of the services and, to the extent such information is of general application, anything which Freed Maxick may discover, create or develop during the provision of services for Client. Except for software owned by and/or proprietary to Freed Maxick, to the extent the deliverables contain Freed Maxick’s proprietary information, Freed Maxick grants Client a non-exclusive, non-assignable, royalty-free license to use it in connection with the deliverables and the subject of the Engagement Letter and for no other or further use. To the extent the deliverables contain the proprietary information of a third party; Client agrees to comply with such third party’s terms of license as the same are communicated to Client. All licenses to software (including any enhancements to software) will be licenses to object code only.
(b) Client acknowledges and agrees that any advice, information or work product provided to Client by Freed Maxick in connection with this engagement is for the sole benefit and use of Client and may not be relied upon or used by any third party. Client further agrees that if it makes any such advice, information or work product available to any third party other than as expressly permitted by the Engagement Letter or Section 1(v) above, the provisions of Section 4(c) below will apply unless: (i) Client provides to the third party an acknowledgement and release letter substantially in the form of Exhibit A attached hereto (the “Letter”); and (ii) the third party signs and returns the Letter to Client. Upon request, Client will provide Freed Maxick with a copy of the signed Letter.

**3. Warranty** Freed Maxick warrants that the services will be performed with reasonable care in a diligent and competent manner. Freed Maxick’s sole obligation will be to correct any non-conformance with this warranty or, if Freed Maxick cannot correct the non-conformance, to refund to Client the amount paid to Freed Maxick for the portion of the services or deliverables that does not conform to this warranty; provided that Client gives Freed Maxick written notice within thirty (30) days after the services are performed or, if applicable, deliverables are delivered. The notice will specify and detail the non-conformance and Freed Maxick will have a reasonable amount of time, based on its severity and complexity, to correct the non-conformance. Freed Maxick does not warrant and is not responsible for any third-party products or services. Client’s sole and exclusive rights and remedies with respect to any third-party products or services are against the third-party vendor and not against Freed Maxick. This warranty is Freed Maxick’s only warranty concerning the services and any deliverable, and is made expressly in lieu of all other warranties and representations, express or implied, including any implied warranties of merchantability, fitness for a particular purpose or otherwise, all of which are hereby disclaimed.

**4. Indemnification** (a) Each party agrees to indemnify, hold harmless and defend the other from and against any and all claims, actions, fees, expenses, costs, damages, losses and liabilities (including reasonable attorneys’ fees) (collectively, “Liabilities”) for bodily injury or death of any person or damage to real or tangible personal property which the other party may sustain or incur, to the extent such Liabilities result from the negligence or willful misconduct of the indemnifying party, its employees, agents or representatives.

(b) Freed Maxick agrees to indemnify, hold harmless and defend Client from and against any and all Liabilities to the extent such Liabilities result from the infringement of any third party’s intellectual property by any deliverables provided under this Agreement. The foregoing indemnification will not apply to the extent any infringement results from: (i) the use of the deliverables other than in accordance with the terms of this Agreement and any applicable documentation or instructions supplied by Freed Maxick; (ii) any modification to the deliverables not expressly agreed to in writing by Freed Maxick; or (iii) the combination of the deliverables with any materials not provided or expressly approved by Freed Maxick.

(c) Client agrees to indemnify, defend and hold harmless Freed Maxick from and against any and all Liabilities incurred or suffered by or asserted against Freed Maxick to the extent such Liabilities result from a third party's use, possession of or reliance upon Freed Maxick's advice, information or work product as a result of Client's failure to comply with the Letter requirements of Section 2(b) above.

**5. Liability** Except for each party's indemnification obligations under this Agreement, the total liability of Client and Freed Maxick (and their respective affiliates, officers, directors, employees, contractors, agents and representatives) relating to this Agreement will in no event exceed an amount equal to the fees paid (in the case of Freed Maxick's liability) or owing (in the case of Client's liability) to Freed Maxick under this Agreement. In no event will Client or Freed Maxick (or their respective affiliates, officers, directors, employees, contractors, agents or representatives) be liable for any special, consequential, incidental, punitive or exemplary damages or loss (nor any loss of profits, savings, data, use of software or hardware or business opportunity, or interruption of business) even if advised of the possibility of such loss.

**6. Termination** (a) Either party may terminate this Agreement at any time, with or without cause, upon fifteen (15) days' prior written notice to the other party.
(b) Client will pay Freed Maxick for all services rendered (including deliverables and products delivered), expenses incurred and commitments made by Freed Maxick through the effective date of termination.

**7. General** (a) Except for the payment of money, neither party will be liable for any delays or failures in performance due to circumstances beyond its reasonable control.
(b) No term of this Agreement will be deemed waived, and no breach of this Agreement excused, unless the waiver or consent is in writing signed by the party granting such waiver or consent.
(c) Neither party may assign or transfer this Agreement without the other party's prior written consent.
(d) Any notices given pursuant to this Agreement will be in writing, delivered to the addresses set forth in the Engagement Letter (unless changed by either party by notice to the other party), and will be effective upon receipt.
(e) If any term or provision of this Agreement is determined to be invalid or unenforceable, such term or provision will be deemed stricken and all other terms and provisions will remain in full force and effect.
(f) Each party is an independent contractor and not an employee, agent, joint venture or partner of the other.
(g) Freed Maxick may from time to time use subcontractors to deliver specific products or services to Client. The management of and all financial arrangements with subcontractors will be Freed Maxick's responsibility.
(h) The terms of this Agreement which by their nature are to survive this Agreement will survive its expiration or termination.
(i) The parties acknowledge that they may correspond or convey documentation via Internet e-mail and that neither party has control over the performance, reliability, availability, or security of Internet e-mail. Therefore, neither party will be liable for any loss, damage, expense, harm or inconvenience resulting from the loss, delay, interception, corruption, or alteration of any Internet e-mail due to any reason beyond its reasonable control.
(j) Neither party intends that there be any third-party beneficiaries to this Agreement.
(k) Neither party will use the other party's name, trademarks, service marks, logos, trade names and/or branding without such party's prior written consent. Notwithstanding the foregoing, Freed Maxick may mention Client's name and provide a general description of the engagement in Freed Maxick's client lists and marketing materials.
(l) The parties agree that this Agreement and any dispute or claim arising out of or relating to this Agreement or the services will be governed by and construed in accordance with the laws of the state in which the Freed Maxick office providing the services is located without regard to such state's laws of conflicts. The parties agree that all litigation or other legal proceedings under this Agreement will be brought in the State or Federal courts located therein. The parties agree to this choice of law, jurisdiction and venue, and waive the defense of an inconvenient forum. Additionally, the parties waive trial by jury and agree that any dispute or claim should be resolved by a judge without a jury.
(m) Any action against either party by the other in connection with this Agreement must be brought within eighteen (18) months after the cause of action arises.

# Exhibit E

## Certificate of Insurance

FREEMAX-02 TLANZA

ACORD

# CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)
6/9/2021

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

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

PRODUCER License # 1009544
Lawley, LLC
361 Delaware Avenue
Buffalo, NY 14202

CONTACT NAME:
PHONE (A/C, No, Ext): (716) 849-8618 FAX (A/C, No): (716) 849-8291
E-MAIL ADDRESS:

| INSURER(S) AFFORDING COVERAGE | NAIC # |
|---|---|
| INSURER A : Citizens Insurance Company | 40274 |
| INSURER B : Allmerica Financial Benefits Ins | 41840 |
| INSURER C : | |
| INSURER D : | |
| INSURER E : | |
| INSURER F : | |

INSURED
Freed Maxick CPAs PC
Attn: Joe Volpe
424 Main Street
Buffalo, NY 14202

**COVERAGES** **CERTIFICATE NUMBER:** **REVISION NUMBER:**

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

| INSR LTR | TYPE OF INSURANCE | ADDL INSD | SUBR WVD | POLICY NUMBER | POLICY EFF (MM/DD/YYYY) | POLICY EXP (MM/DD/YYYY) | LIMITS | |
|---|---|---|---|---|---|---|---|---|
| A | ☒ COMMERCIAL GENERAL LIABILITY | | | | | | EACH OCCURRENCE | $ 1,000,000 |
| | ☐ CLAIMS-MADE ☒ OCCUR | | | OBSA187557 | 1/30/2021 | 1/30/2022 | DAMAGE TO RENTED PREMISES (Ea occurrence) | $ 1,000,000 |
| | ☐ | | | | | | MED EXP (Any one person) | $ 10,000 |
| | ☐ | | | | | | PERSONAL & ADV INJURY | $ 1,000,000 |
| | GEN'L AGGREGATE LIMIT APPLIES PER: | | | | | | GENERAL AGGREGATE | $ 2,000,000 |
| | ☐ POLICY ☐ PRO-JECT ☒ LOC | | | | | | PRODUCTS - COMP/OP AGG | $ 2,000,000 |
| | ☐ OTHER: | | | | | | | $ |
| A | AUTOMOBILE LIABILITY | | | | | | COMBINED SINGLE LIMIT (Ea accident) | $ 1,000,000 |
| | ☐ ANY AUTO | | | OBSA187557 | 1/30/2021 | 1/30/2022 | BODILY INJURY (Per person) | $ |
| | ☐ OWNED AUTOS ONLY ☐ SCHEDULED AUTOS | | | | | | BODILY INJURY (Per accident) | $ |
| | ☒ HIRED AUTOS ONLY ☒ NON-OWNED AUTOS ONLY | | | | | | PROPERTY DAMAGE (Per accident) | $ |
| | ☐ ☐ | | | | | | | $ |
| A | ☒ UMBRELLA LIAB ☒ OCCUR | | | | | | EACH OCCURRENCE | $ 5,000,000 |
| | ☐ EXCESS LIAB ☐ CLAIMS-MADE | | | OBSA187557 | 1/30/2021 | 1/30/2022 | AGGREGATE | $ 5,000,000 |
| | ☐ DED ☒ RETENTION $ 0 | | | | | | | $ |
| B | WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y / N | | | | | | ☒ PER STATUTE ☐ OTH-ER | |
| | ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) ☐ | N / A | | W2SA161882 | 1/30/2021 | 1/30/2022 | E.L. EACH ACCIDENT | $ 1,000,000 |
| | If yes, describe under DESCRIPTION OF OPERATIONS below | | | | | | E.L. DISEASE - EA EMPLOYEE | $ 1,000,000 |
| | | | | | | | E.L. DISEASE - POLICY LIMIT | $ 1,000,000 |
| | | | | | | | | |

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

**CERTIFICATE HOLDER**

Erie County Water Authority
295 Main Street, Room 350
Buffalo, NY 14203

**CANCELLATION**

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

# Exhibit F

## Professional Biographies

# David Hansen, CISSP, CISA, PCI QSA, CPA

DIRECTOR

**DAVID.HANSEN@FREEDMAXICK.COM**

David is a Director in Freed Maxick's Risk Advisory Services practice. David has a broad background, specializing in both financial and technical assessments, compliance and risk engagements, and other audit and consulting projects. His primary focus includes third-party risk advisory and assurance, compliance with laws and regulations regarding internal controls over financial reporting and compliance requirements, and cybersecurity. He has been with the Firm since 2007, helping to grow our risk and compliance consulting services.

David is responsible for planning, executing and completing various technology and financial engagements for clients operating in a variety of industries, including technology services, government, manufacturing, health care and financial services. He is responsible for leading our Firm's System and Organization Control Reporting practice, which includes having oversight for quality assurance and in accordance with AICPA and Firm quality standards, and issuance of all reports. David also leads Freed Maxick's Payment Card Industry Compliance (PCI) practice as the Firm's lead Qualified Security Assessor, directing all RAS practice resources to execute Reports on Compliance and other assessments in accordance with the PCI Data Security Standards. He has led numerous SOC engagements, Sarbanes-Oxley consulting projects, PCI compliance assessments and other internal control audits and risk advisory projects for these clients. David's clients include many large, public companies facing complex technical, security, and compliance issues both domestically and abroad.

Prior to his career with the Firm, David was a a member of a global IT audit team with a large, international manufacturing company where he participated in several multinational internal audit engagements, including Sarbanes-Oxley reviews, and commonly served as a facilitator with members of the business community and the organization's external auditors.

## EDUCATION

Bachelor of Business Administration, Finance, State University of New York at Buffalo

Master of Business Administration, Accountancy, State University of New York at Buffalo

## PROFESSIONAL AFFILIATIONS

- Board of Governors, Rochester Chapter of the Institute of Internal Auditors

# Samuel M. DeLucia, CISA

SENIOR MANAGER

**SAMUEL.DELUCIA@FREEDMAXICK.COM**

Sam DeLucia is a Senior Manager in the Risk Advisory Practice at Freed Maxick CPAs, P.C. He has over 20 years of experience in IT, Cybersecurity, Regulatory Compliance and IT Audit. Sam is one of Freed Maxick's practice leader and methodology owner for many of the Firm's Cybersecurity Services such as: Vulnerability Assessment and Penetration Testing, Web Application Security Assessments, Social Engineering (Phishing), NIST CSF Consulting, Cybersecurity Process Assessment, and NIST Privacy Framework Consulting.

Sam applies his experience and leadership to engagements; and is an acting virtual CISO for Firm clients, providing secure strategic and regulatory guidance.

His experience includes leading various advisory and assurance engagements covering Cybersecurity, Governance, Risk and Compliance, and IT Security Audits. Sam has extensive knowledge in various control, security and compliance frameworks, such as COBIT, COSO, SOX, HIPAA, PCI, NYS DFS, ISO27000, NIST, PII.

## EDUCATION

Bachelor of Science, Information Technology, Networking, System Administration, Cybersecurity, Rochester Institute of Technology

## PROFESSIONAL AFFILIATIONS

- Board Member, Past Positions include VP and President, IIA, 2008-2019
- Member, IIA, 2002-Present
- Member, ISACA, 2002-Present

# Justin T. Bonk, CFE, CIA, CISA, CISSP, PCI QSA

SENIOR MANAGER

**JUSTIN.BONK@FREEDMAXICK.COM**

Justin is a Senior Manager in Freed Maxick's Risk Advisory Services practice with over 12 years of experience. Justin's primary responsibilities include the oversight of engagements performed by Freed Maxick's Risk Advisory services, including but not limited to:

- IT Audits;
- Cyber Security Assessments;
- PCI Audits
- Data Privacy Reviews;
- Risk Asessments;
- Internal Audits;
- HIPAA Audits;
- Pre and Post Implementation Reviews;
- Business Process Mapping and Redesign;
- Sarbanes Oxley;
- SOC Audits

Justin has performed these services for companies of all sizes, ranging from small local startups to multinational corporations. Justin's main industries served include Energy, Banking, Software/Platform/Infrastructure-as-a-Service, Payroll, Manufacturing, Health Care (provider and payer), Collections, and Call Centers.

As a Senior Manager with Freed Maxick, Justin has responsibility to deliver cyber security engagements. This includes planning and scoping engagements, overseeing fieldwork performed for the engagement, reviewing the engagement, reporting and client interfacing. Justin is a Certified Information System Auditor (CISA), Qualified Security Assessor (QSA), Certified Information System Security Professional (CISSP),making him a cyber security subject matter expert for the firm. He has performed cyber-security related services for companies of all sizes, from smaller local organizations to organizations listed on the S&P 500.

In 2015, Justin was recognized internationally as one of 15 emerging leaders by Internal Auditor magazine - a distinction given to 15 individuals across the world under 30 recognized for their leadership in the field of internal auditing.

## EDUCATION

Bachelor of Arts, Business Administration, Focus in Internal Audit, State University of New York at Buffalo

## PROFESSIONAL AFFILIATIONS

- Member, Institute of Internal Auditors (IIA), 2008 to Present
- Member, Association of Certified Fraud Examiners (ACFE), 2010 to Present
- Member, International System Security Certification Consortium (ISC2), 2019 to Present
- Member, Information Systems Audit and Control Association (ISACA), 2010 to 2016

## COMMUNITY INVOLVEMENT

- Treasurer of the Board of Directors, Cazenovia Community Resource Center, June 2014 to November 2017
- Volunteer, Compeer of Buffalo, February 2015 to November 2016
- Mentor, Big Brothers Big Sisters of Erie County, March 2015 to July 2017

# Alexander Bliss

SUPERVISOR

**ALEXANDER.BLISS@FREEDMAXICK.COM**

Alex Bliss is a Supervisor in Freed Maxick's Risk Advisory Services Practice. He has over 15 years of software development, system administration and cybersecurity experience. During his consulting career, Alex has participating in a number of Information Technology, Cybersecurity and technical compliance assessments.

Alex Bliss is a Supervisor in Freed Maxick's Risk Advisory Services Practice. He has over 15 years of software development, system administration and cybersecurity experience as well as 3 years of consulting experience. During his consulting career, Alex has participating in a number of Information Technology, Cybersecurity and technical compliance assessments including:

- IT Audits;
- Network Penetration Tests;
- Vulnerability Assessments;
- Web Application Penetration Tests;
- Secure Coding Reviews;
- SOC Audits;
- PCI DSS Engagements;
- Cybersecurity Assessments

Alex has performed these assessments for a number of companies ranging from small businesses to large corporations. As a Supervisor, Alex has lead engagements from planning through fieldwork and reporting. Alex serves as a subject matter expert in many technical matters including practical network and technical security topics as well as system design and software development.

## EDUCATION

Bachelor of Science, Computer Science,
State University of New York at Oswego

## PROFESSIONAL AFFILIATIONS

- Member, IIA, 2017 to Present
- Member, ISACA, 2017 to Present

# Tiffany Williams

SR. ASSOCIATE

**TIFFANY.WILLIAMS@FREEDMAXICK.COM**

Tiffany Williams joined Freed Maxick in January 2020 as a Senior Associate/Consultant in the Risk Advisory Services group. She graduated from RIT in 2016 with a Degree in Computing Security, and has since had experience working as a security researcher and software tester/developer. Notable experience includes mobile and web application security testing, vulnerability analysis and code review for applications, QA and automation testing, development and testing of Windows Red Teaming Product (Patent Pending) to explore security vulnerabilities in enterprise network infrastructure, and development and testing of a custom post exploitation and malware emulation platform.

**EDUCATION**

Bachelor of Science, Computer & Information Sciences, Rochester Institute of Technology

GlobalSecurityIQ™

June 10, 2021

Mr. Terrence D. McCracken
Secretary to the Authority
Erie County Water Authority
295 Main Street, Room 350
Buffalo, NY 14203

Reference: Cybersecurity Risk and Vulnerability Assessment for the Erie County Water Authority

Dear Mr. McCracken:

GlobalSecurityIQ is pleased to submit a bid to provide the Erie County Water Authority with a Cybersecurity Risk and Vulnerability Assessment. Leveraging our many years of experience investigating cyber crimes, currency on the cyber-threat picture and extensive background in offensive hardening relative to cybersecurity risk and vulnerability identification, we are uniquely qualified to conduct your assessment.

As a full-service Cybersecurity Risk Mitigation and Incident Response company, GlobalSecurityIQ specializes in Risk Assessments, Vulnerability Identification, Incident Response services, Digital Forensics, Penetration Testing, Cybersecurity Training, Table Top Exercises, Disaster Recovery/Business Continuity Planning, and Cybersecurity consulting for executive leadership.

We have provided you with the following information as requested:

- Bid Response to Erie County Water Authority Cybersecurity Risk and Vulnerability Assessment
- Federal, state, and county women-owned business certifications

Thank you very much for the opportunity to provide a proposal. If you have any questions, please contact me at 716-550-6145 (cell) or via email at Holly.Hubert@GlobalSecurityIQ.com.

Respectfully,

Holly L. Hubert, FBI ret., CISSP, CISM, CGEIT, CRISC, CMMC-RP
Founder and CEO

GlobalSecurityIQ™

# Reponse to Erie County Water Authority Request for Cybersecurity Risk & Vulnerability Assessment Proposal

June 9, 2021

Presented by:
Holly Hubert, CISSP, CISM, CGEIT, CRISC, FBI ret.

GlobalSecurityIQ, LLC.
1576 Sweet Home Road, Suite 218
Buffalo, NY  14228

(716) 475-9455
Holly.Hubert@GlobalSecurityIQ.com

www.GlobalSecurityIQ.com

Cybersecurity Credentials and Experience Matter

# Contents

Introduction to GlobalSecurityIQ ........ 3

RFP Response Part 1 ........ 3

RFP Response Part 2 ........ 4

Response Part 2, Item 1: Consultant Business Form ........ 4

Response Part 2, Item 2: Consultant Team ........ 6

RFP Response Part 3 ........ 9

Response Part 3, Item 1: Proposed Scope of Service ........ 9

Response Part 3, Item 2: Hardware Requirements ........ 16

Response Part 3, Item 3: Timeline for Deliverables ........ 17

Appendix A – Standardized Agreement........ 22

## Introduction to GlobalSecurityIQ

GlobalSecurityIQ is a full-service cyber risk mitigation company owned and staffed by certified cybersecurity professionals. Detection is no longer enough to ensure protection. Prevention and offensive hardening are the keys to shielding your computing infrastructure from harm. No system can be 100% secure, but most breaches are preventable, and organizations can significantly reduce their risk. GlobalSecurityIQ provides comprehensive solutions that leverage cybersecurity best practices, risk assessment strategies, vulnerability scanning, penetration testing, corporate education, and employee simulated phishing attack testing to detect and mitigate cyber threats. We also assist organizations with digital forensics, incident response, disaster recovery, and business continuity planning.

## RFP Response Part 1

| Response Part 1, Items 1 – 6: Contact Information | |
|---|---|
| Name of Organization | GlobalSecurityIQ, LLC. |
| Name / Title of Contact Person | Holly L. Hubert, CEO |
| Business Address | 1576 Sweet Home Road, Suite 218<br>Buffalo, NY 14228 |
| Telephone No. | 716-475-9455 |
| Email Address | Holly.Hubert@GlobalSecurityIQ.com |
| Fax No. | N/A |

# RFP Response Part 2

## Response Part 2, Item 1:  Consultant Business Form

| Response Part 2, Item 1:  Consultant Business Form | |
|---|---|
| Business / Corporate Structure | Partnership |
| Date and State of Formation | July 3rd 2017, New York State |
| Name of General Partners | Holly Hubert, General Partner |
| Type of Partnership | LLC |
| Principal Place of Business | Amherst, NY |
| EIN | 82-2052574 |
| Identify the number of years your entity has been in business | GlobalSecurityIQ has been in business nearly four (4) years |
| Identify whether your business / corporate structure has changed in the past five years and if yes, describe the change | GlobalSecurityIQ's corporate structure has not changed in the past five (5) years |
| Identify the type and coverage amount of all insurance policies | • Professional liability $2MM / $2MM, Cyber rider<br>• General liability $1MM / $2MM<br>• Workers' compensation – as required by law |

| | |
|---|---|
| Identified the name, address, and contact information for three (3) companies that the Consultant has performed similar services to those being sought by the Authority | **Town of Cheektowaga:**<br>• **Services performed:** NIST-based Cybersecurity Risk Assessment, Full Internal/External Network Vulnerability Scan including a Domain Controller Configuration Audit, on-going Risk Management / Cybersecurity Consulting<br>**Contact:** Lisa Bolognese, Director of Information Technology, Records Management<br>LBolognese@tocny.org<br>**Town of Orchard Park:**<br>• **Services performed:** NIST-based Cybersecurity Risk Assessment, Full Internal/External Network Vulnerability Scan including a Domain Controller Configuration Audit, on-going Risk Management / Cybersecurity Consulting<br>• **Contact:** Paul Pepero, Director of Information Technology<br>PeperoOP@OrchardParkNY.org<br>**Northtown Auto:**<br>• **Services performed:** NIST-based Cybersecurity Risk Assessment, Full Internal/External Network Vulnerability Scan including a Domain Controller Configuration Audit, on-going Risk Management / Cybersecurity Consulting<br>• **Contact:** Kyle Rookey, Chief Financial Officer<br>K.Rookey@NorthtownAuto.com |
| If you are certified, minority and/or women owned business, submit a copy of the certification | GlobalSecurityIQ holds the following certifications:<br>• Federally Certified Woman-Owned Small Business (WOSB)<br>• New York State Certified Women Business Enterprise (WBE)<br>• Erie County / City of Buffalo Certified Women Business Enterprise (WBE)<br>Please find copies of respective certifications attached. |

## Response Part 2, Item 2: Consultant Team

| | **Holly L. Hubert, Founder and CEO**<br>**CISSP, CISM, CGEIT, CRISC, GRCP**<br>**B.S., Information Systems Management, Buffalo State College**<br>**M.A., Communicatoin and Leadership, Canisius College** |
|---|---|
| Relevant qualifications and experience | **Holly Hubert** served as an FBI Agent for 25 years retiring as an Assistant Special Agent in Charge (ASAC) of the FBI Buffalo Division where she had executive oversight of all Cyber, Terrorism, Counterintelligence, Intelligence, and Criminal Programs to include all Crisis Management and SWAT assets. She has extensive experience in assessing and managing risk and has led all aspects of business continuity planning (BCP) to include physical and cyber-related continuity of operations. Hubert has proven capability in establishing order, direction, and collaborative partnerships. As the former FBI Buffalo Division Compliance Officer, she chaired the division's Compliance Council to assess risk and ensure critical adherence to federal law, policy, and best practices.<br>She previously served as the Cyber Squad Supervisory Special Agent and founded the FBI Buffalo Cyber Task Force focusing on Computer Intrusions, Online Crimes against Children, and Internet Frauds. Hubert secured federal funding for and was integral in the development of the Western New York - Regional Computer Forensics Laboratory (WNY-RCFL), one of only 17 FBI Laboratory Division-affiliated facilities dedicated to the science of digital forensics. She received numerous career commendations and was twice the recipient of the "Director's Award," the FBI's highest accolade, to include recognition for "Outstanding Cyber Investigation." She has experience with hundreds of cyber-related incidents and assessments. In 2017, Hubert founded GlobalSecurityIQ and the GlobalSecurityIQ Computer Forensic Laboratory (GCFL). The GCFL, modeled after the WNY-RCFL, is a privatized laboratory specializing in cyber-incident response and digital forensics.<br>Hubert has lectured and provided keynotes in hundreds of forums nationally and internationally on leadership and cyber threats engaging private industry, boards, law enforcement, and academia. |
| State/county of residence | New York, Erie County |
| Scope of responsibility | Project oversight, consulting, risk assessment, vulnerability identification |
| Time working for Consultant | Over 20 years of experience in cybersecurity, assessments, and risk management in the FBI; four (4) years operating the GlobalSecurityIQ consultancy. |

| | **Steven Halter, Executive Director of Risk Management and Audit**<br>**Security+, CHFI, ECIH**<br>**B.S., Business Administration: Management Information Systems, University at Buffalo** |
|---|---|
| Relevant qualifications and experience | **Steven Halter** served as an FBI Agent for 27 years and held the position of Supervisory Special Agent: Program Coordinator White Collar Crime including Internet Fraud, Identity Theft, IPR matters, Public Corruption, and Complex Financial Crimes.<br>Halter's qualifications include work experience across the following areas:<br>• Directed and supervised sensitive internal investigations relating to employee personal and financial misconduct.<br>• Formed the FBI BBCTF consisting of federal, state, and local law enforcement agencies. Directed and fostered the partnership of multiple agency investigators to combat Public Corruption at four international border crossings.<br>• Investigated numerous highly complex financial crime matters including internet frauds, identity theft, and IPR matters, which resulted in the successful seizure of criminal proceeds and prosecution.<br>• Led the investigation of the "Buffalo Billion" public corruption matter, one of the most significant corruption cases investigated in the Western District of New York.<br>• Supervised and maintained responsibility for the periodic audits of 150 parishes within the Catholic Diocese of Buffalo.<br>• Well-versed in managing multiple facets of national and international white collar crime intelligence gathering and investigations including: public corruption, internet fraud, identity theft, IPR matters, domestic intelligence, law enforcement, threat assessment, policy management, evidence collection, and intelligence analysis.<br>• Highly proficient in engendering collaboration and cooperation among federal, state, and local law enforcement partners as demonstrated by the formation of the FBI Buffalo Border Corruption Task Force (BBCTF) and the expansion of the Health Care Fraud and Public Corruption task forces. |
| State and county of residence | New York, Erie County |
| Scope of responsibility | Risk assessment |
| Time working for Consultant | Over 20 years of experience in audits, assessments, and risk management in the FBI; one (1) year working for GlobalSecurityIQ consultancy. |

| | **Andrew Thatcher, Senior Cybersecurity Analyst**<br>**Security+, CHFI, ECIH**<br>**B.S., Business Administration: Management Information Systems, University at Buffalo** |
|---|---|
| Relevant qualifications and experience | An expert in the NIST Cybersecurity Framework and compliance matters, Andrew Thatcher developed a Risk Assessment tool utilized by GlobalSecurityIQ that draws controls from the NIST Cybersecurity Framework and the CIS Critical Security Controls. The assessment instrument maps those controls and best practices to several cybersecurity regulatory requirements, including the HIPAA Security Rule, PCI DSS, and 23 NYCRR 500, enabling efficient and comprehensive assessments. Thatcher has leveraged this instrument to conduct dozens of Risk Assessments and compliance reviews in small, medium, large, and enterprise-level environments.<br>As a certified digital forensics examiner, Thatcher led numerous responses to cyber-related breaches and other incidents. He has conducted digital forensics investigations on profoundly infected networks to identify breach points, data exfiltration, and other exposures. Working collaboratively with business IT partners and executive leadership, he has remediated numerous breaches and hardened organizational cybersecurity postures to prevent further incidents. He has conducted dozens of internal, external, and web application vulnerability scans on a variety of networks including Windows, Cloud, Linux, and Mac environments to ensure all devices are free of malicious code and that vulnerabilities are fully patched.<br>He has developed business continuity and disaster recovery plans, prioritizing critical infrastructure and recommending realistic, actionable approaches, to ensure when a breach occurs, steps for continuity and recovery are clearly defined and immediately actionable. |
| State and county of residence | New York, Erie County |
| Scope of responsibility | Risk assessment, vulnerability identification |
| Time working for Consultant | Nearly four (4) years working for GlobalSecurityIQ consultancy. |

## RFP Response Part 3

### Response Part 3, Item 1: Proposed Scope of Service

Each organization's computing environment is unique and complex. In order to comprehensively assess network vulnerabilities and risk, GlobalSecurityIQ proposes a **Vulnerability Assessment** which is comprised of ***both*** a comprehensive **NIST-based Cybersecurity Risk Assessment** and **a Full Internal/External Network Vulnerability Scan including a Domain Controller Configuration Audit.**

The **NIST-based Cybersecurity Risk Assessment** will identify both technical and non-technical risks. The Risk Assessment drives IT infrastructure and cyber risk-based decision-making serving as the foundational instrument to memorialize your cybersecurity program. GlobalSecurityIQ will document the current-state baseline IT environment as it relates to security, including people, processes, and technologies. The final deliverable will be a report designed for Executive Leadership that documents current cybersecurity practices, identifies/ prioritizes risk, and provides detailed risk mitigation strategies.

In order to comprehensively ascertain cybersecurity risk, GlobalSecurityIQ leverages the NIST Cybersecurity Framework. The framework is structured after the five (5) core NIST functions: Identify, Protect, Detect, Respond, and Recover, which are then broken down into categories and then further broken down into subcategories. Below is a general breakdown of the core NIST functions:

**Identify:**
The Identify Function is foundational for effective use of the framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Categories within this function include: Asset Management; Business Environment; Governance; Risk Assessment; Risk Management Strategy; and Supply Chain Risk Management.

**Protect:**
The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Categories within this function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

**Detect:**
The Detect Function enables timely discovery of cybersecurity events. Categories within this function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

**Respond:**
The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Categories within this function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

**Recover:**
The Recover Function supports timely recovery of normal operation to reduce the business impact of a cybersecurity incident. Categories within this function include: Recovery Planning; Improvements; and Communications.

Following completion of the **NIST-based Cybersecurity Risk Assessment**, GlobalSecurityIQ often provides ongoing **Cybersecurity Consulting** where mitigation strategies identified in the Risk Assessment are collaboratively planned and implemented by GlobalSecurityIQ and the Authority. Services that are available through **Cybersecurity Consulting** include (but are not limited to):

- Incident Response
- Redundant Tool Analysis
- Digital Forensics / e-Discovery
- Compliance / Governance
- Cybersecurity training / Leadership education
- Board consulting
- Configuration review of cloud application and/or hardware / software
- Response / Recovery Planning and testing
- Policy writing
- Physical security of IT assets
- Ad-hoc consulting

The **Full Internal/External Network Vulnerability Scan with a Domain Controller Configuration Audit,** intended for IT personnel, will identify technical vulnerabilities such as security misconfigurations, unpatched software, missing security patches, or non-encrypted communications. The **Vulnerability Scan** report will prioritize and outline remediation actions for each identified vulnerability. The **Domain Controller Configuration Audit** portion applies to the domain controller in Windows environments and benchmarks over 400 domain controller group policy settings against cybersecurity best practices.

## Engagement Implementation Plan

1. Kick-off meeting with the Authority's IT Department leadership and/or appropriate party(ies)

2. Conduct comprehensive **NIST-based Cybersecurity Risk Assessment (Risk Assessment)**

3. Setup and perform **Full Internal/External Network Vulnerability Scan with Domain Controller Configuration Audit (Vulnerabiltiy Scan)**

4. Brief risks and mitigation strategies to leadership within 30 days

| **Response Part 3, Item 1: Proposed Scope of Service** | |
|---|---|
| Services performed on-site or off-site | GlobalSecurityIQ can perform all quoted services at the preference of the Authority either off-site (remotely) / on-site. |
| Review of current state of the Authority's information technology security | The **Risk Assessment** deliverable includes a memorialization of the current state of the Authority's information technology environment mapped against the NIST Cybersecurity Framework (NIST CSF) controls.<br>The **Vulnerability Scan** deliverable includes a memorialization of the current state of the Authority's information technology devices, to include workstations, servers, and networking devices.<br>The **Domain Controller Configuration Audit** deliverable includes a memorialization of the current state of the Authority's domain controller group policy configuration. |
| Development of a vulnerability mitigation plan | The **Risk Assessment** deliverable includes a prioritized listing of all risks identified via the assessment. Each identified risk includes a detailed, actionable mitigation plan.<br>The **Vulnerability Scan** deliverable includes a prioritized listing of all risks idenfied via the scan. Each identified vulnerability includes a detailed, actionable mitigation plan.<br>The **Domain Controller Configuration Audit** deliverable includes a pass/fail score for all domain controller group policy configurations. Pass/fail is determined by comparing the group policy configurations against a best practice baseline developed by the Center for Internet Security. Each "fail" identified includes a detailed, actionable mitigation plan and identifies any potential network impacts that could be a result of the group policy change. |

| | |
|---|---|
| Development of a prioritized road map of activities to enhance the Authority's future Cybersecurity position | The **Risk Assessment** and **Vulnerability Scan** deliverables both include a prioritized listing of identified risk and vulnerabilities. Prioritized by criticality, the deliverables serve as a "road map" to harden the Authority's cybersecurity posture. Risks and vulnerabilities which represent a significant threat to the Authority will be assigned the highest priority. |
| Best practice methodologies to ensure a standardized risk mitigation approach that will offer the highest risk reduction potential, complementing the "Framework for Improving Critical infrastructure Cybersecurity," developed by the National Institute for Standards and Technology (NIST) | As described in the *Proposed Scope of Services* (pages 9 and 10), GlobalSecurityIQ utilizes the NIST Cybersecurity Framework to perform cybersecurity **Risk Assessments,** allowing for a standardized and methodical approach that will, along with the **Vulnerability Scan** and **Domain Controller Configuration Audit**, equip the Authority with a highly effective and actionable risk reduction program. |
| Test for susceptibility to Advanced Persistent Threats (APTs) such as viruses, malware, Trojan horses, botnets, and other targeted attack exploits. | GlobalSecurityIQ's **Full Network Vulnerability Scan** includes credentialed internal and external vulnerability scanning.<br>The credentialed internal scanning will check internal information technology devices, such as workstations, servers, and networking devices, for exploitable vulnerabilities. Exploitable vulnerabilities include "openings" which allow viruses, malware, trojan horses, botnets, etc. to enter environments.<br>The external vulnerability scan will test your network perimeter to determine exploitable weaknesses. Identified weakness/vulnerabilities will include actionable mitigation recommendations. |

| | |
|---|---|
| Evaluate the Authority's current threat posture including antivirus and Intrusion Detection and Prevention (IDP) capabilities | Antivirus and Intrustion Detection/Prevention capabilities will be evaluated through both the **Risk Assessment** and the **Vulnerability Scan.**<br>Through the **Risk Assessment**, GlobalSecurityIQ will review the configuration and implementation of the in-place network firewall, endpoint protection, and processes related to receiving and responding to security alerts.<br>Through the **Vulnerability Scan**, GlobalSecurityIQ will (depending on the antivirus solution) identify when antivirus definitions for each applicable device were last updated. Devices with antivirus definitions more than 24 hours out-of-date will be highlighted for remediation. |
| Evaluate the Authorities planned changes and improvements to the threat surface and assist identifying and addressing security concerns | The **Risk Assessment** deliverable includes a memorialization of the current state of the Authority's information technology environment mapped against the NIST Cybersecurity Framework (NIST CSF) controls. Additionally, the deliverable includes a prioritized listing of all risks identified via the assessment. Each identified risk includes a detailed, actionable mitigation plan.<br>Following completion of the **Risk Assessment**, GlobalSecurityIQ can provide ongoing **Cybersecurity Consulting** where changes / mitigation strategies identified in the Risk Assessment are collaboratively planned and implemented by GlobalSeucrityIQ and the Authority. |
| Review the Authority's current Supervisory Control and Data Acquisition (SCADA) water systems for security vulnerabilities | Through the **Risk Assessment** all Authority information technology systems, including the SCADA water system, are in-scope and will be evaluated for security risks/vulnerabilities. |

| | |
|---|---|
| Review wireless network system components for security vulnerabilities, validating system-specific operating systems and firmware versions for known exploits and recommend upgrades, updates, and mitigations. | Wireless network system components are evaluated for security vulnerabilities via the **Vulnerability Scan**. For all applicable devices, the operating system, firmware version, and other system-specific vulnerabilities will be identified with remediation guidance provided as necessary.<br>IT practices as they relate to system updates, to include operating system and firmware updates, will be evaluated through the **Risk Assessment**. |
| Review current system-specific operating systems and firmware versions for known exploits and recommend upgrades, updates, and mitigations. This includes firewalls, switches and routers, Microsoft Active Directory, email and file servers, web servers, wireless routers, WAN, VPN, VoIP, and CCTV systems. | Operating system and firmware versions are evaluated by the **Vulnerability Scan** for all applicable devices. Out-of-date operating systems / firmware versions are typically highlighted as critical / high vulnerabilities in the **Vulnerability Scan** deliverable.<br>IT practices as they relate to system updates, to include operating system and firmware updates, will be evaluated through the **Risk Assessment**. |
| Assess VoIP network system components for security vulnerabilities, validating system-specific operating system and firmware versions and reviewing for known exploits | System-specific operating system and firmware exploits for applicable VoIP devices will be identified via the **Vulnerability Scan** where device version/configuration allows (some VoIP devices are unable to be fully scanned due to age and/or model).<br>IT practices as they relate to system updates, to include operating system and firmware updates, will be evaluated through the **Risk Assessment**. |
| Review existing IT policies and procedures and make recommendations for changes and/or additional policy and procedure development. | All IT policies and procedures will be comprehensively evaluated for completeness and security. Where gaps exist in documentation, GlobalSecurityIQ will make recommendations for changes and/or additional policy and procedure development. |

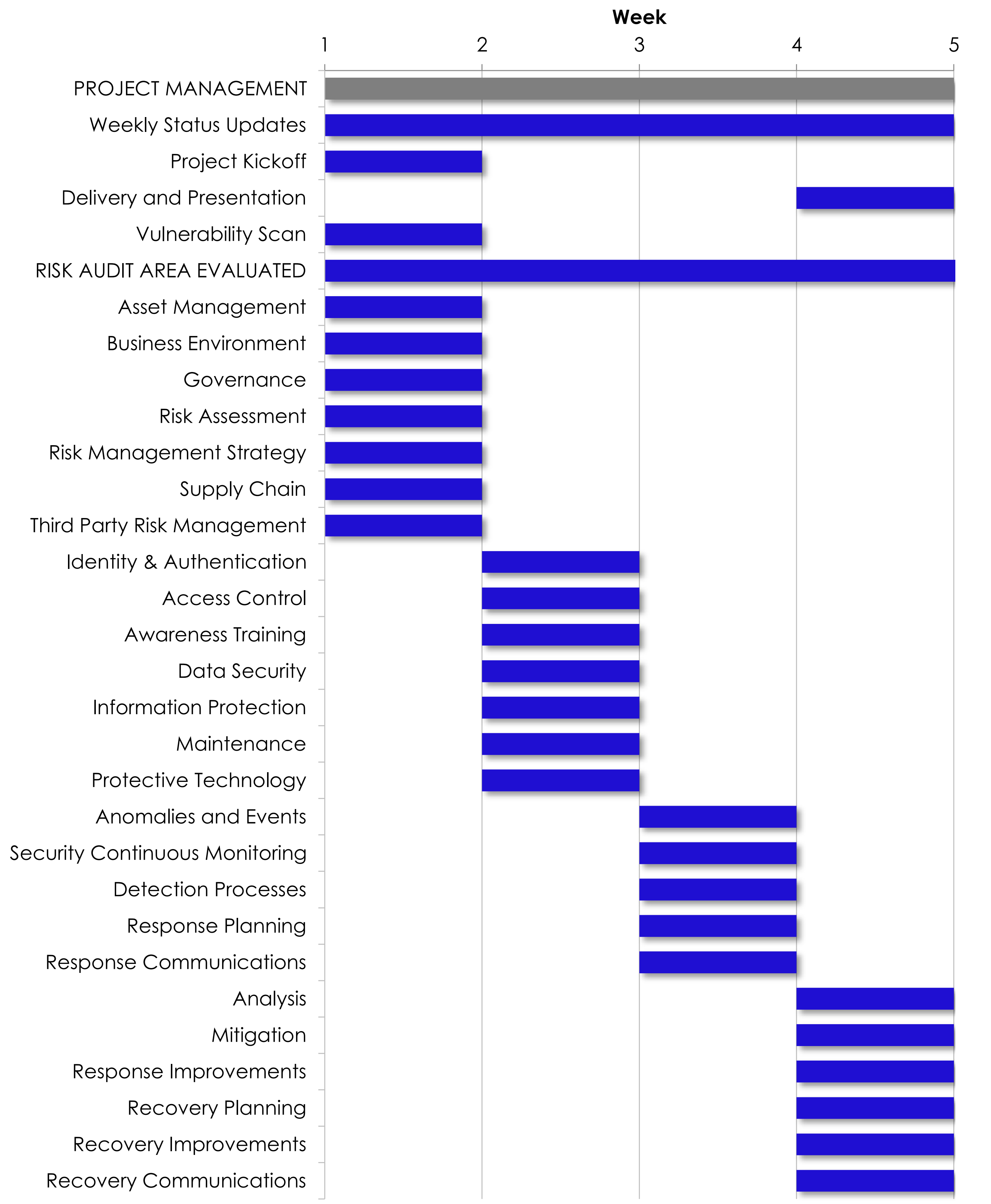
| | |
|---|---|
| Execute and review internal network vulnerability scans and external vulnerability and penetration scans and make recommendations to reduce the threat attack surface | The **Vulnerability Scan** deliverable includes a memorialization of the current state of the Authority's information technology devices, to include workstations, servers, and networking devices. Additionally, the **Vulnerability Scan** deliverable includes a prioritized listing of all risks idenfied via the scan. Each identified vulnerability includes a detailed, actionable mitigation plan. |
| Recommend or assist in selection of vulnerability scan software for purchase/license for continued use by the Authority after the assessment is complete | GlobalSecurityIQ provides ongoing **Cybersecurity Consulting** following a Vulnerability Assessment to collaboratively plan and implement mitigation strategies identified in the **Vulnerability Scan** and **Risk Assessment**.<br>GlobalSecurityIQ is highly familiar and experienced with various cybersecurity products, including commercial vulnerability scanning software, and can make product recommendations as needed. |

## Response Part 3, Item 2:  Hardware Requirements

| Response Part 3, Item 2:  Hardware Requirements | |
|---|---|
| Describe the required hardware and/or software necessary to implement Consultant's plan, if any | The **Vulnerability Scan** will require a dedicated Authority workstation GlobalSecurityIQ can remotely access for the duration of the scan (1 – 2 business days).  The workstation must be domain-joined and capable of communicating with all network locations to be scanned.<br>Commercial vulnerability scanning software will be utilized to complete the scan.  Commercial remote access software will be used to access the workstation.<br>No other hardware/software is required to complete the engagement. |
| Describe the limitations of the service and/or equipment, if any | N/A |
| Identify whether the required hardware and/or software will be provided by Consultant or the Authority | Dedicated domain-joined workstation will be provided by the Authority.<br>Vulnerability scanning and remote access software will be provided by GlobalSecuriytIQ. |

## Response Part 3, Item 3: Timeline for Deliverables

**Response Part 3, Item 3: Timeline for Deliverables**



CONFIDENTIALITY NOTICE: The information in this quote is strictly confidential and is supplied on the understanding that it will be held confidentially and not disclosed to third parties without the prior written consent of GlobalSecurityIQ, LLC. Pricing herein is non-published and therefore governed by trade secret law.

| Response Part 3, Item 3: Timeline for Deliverables | |
|---|---|
| Project Management Deliverables:<br>A) Work Breakdown Schedule (WBS) including tasks<br>B) Schedule and dependencies<br>C) Weekly Status Reports including risks and progress reports | Please refer to the aforementioned table, the **Vulnerability Scanning** and **Risk Assessment** will begin the first week of the engagement. "Risk Audit Area Evaluated" refers to the NIST Cybersecurity Framework functions that will be evaluated.<br>Weekly Status Reports will be provided (either via email, telephonically, or in-person). Notification to the Authority will be made prior to report delivery should a time-sensitive critical risk/vulnerability be identified.<br>It should be noted that the Security Officer/IT Manager (and others) is/are required to be available on an as needed basis during this engagement period to provide critical input to both assessments. |

| | |
|---|---|
| Report: A written report documenting:<br>A) Executive summary detailing the Authority's Cybersecurity position, including a comparative scorecard of findings<br>B) Results of vulnerability testing performed<br>C) Identified cybersecurity vulnerabilities, gaps, and mitigation plans<br>D) A prioritized road map of activities, developed in conjunction with Authority's IT staff to enhance the Authority's future cybersecurity position. | The **Risk Assessment** deliverable includes:<br>• Memorialization of the current state of the Authority's information technology environment mapped against the NIST Cybersecurity Framework (NIST CSF) controls.<br>• Prioritized listing of all risks identified via the assessment.  Each identified risk includes a detailed, actionable mitigation plan.<br>The **Vulnerability Scan** deliverable includes:<br>• Memorialization of the current state of the Authority's information technology devices, to include workstations, servers, and networking devices.<br>• Prioritized listing of all risks idenfied via the scan.  Each identified vulnerability includes a detailed, actionable mitigation plan.<br>The **Domain Controller Configuration Audit** deliverable includes:<br>• Memorialization of the current state of the Authority's domain controller group policy configuration.<br>• A pass/fail score for all domain controller group policy configurations.  Pass/fail is determined by comparing the group policy configurations against a best practice baseline developed by the Center for Internet Security.  Each fail identified includes a detailed, actionable mitigation plan and identifies any potential network impacts that could be a result of the group policy change. |

| | |
|---|---|
| Project solutions and costs:<br>A) Provide an estimated range, based upon previous experience, of the total services costs to implement the proposed solutions<br>B) Include a Rate Sheet that specifies and itemizes the cost for each proposed component, including all licensing, support, maintenance, and hosting fees<br>C) For subscription-based services, provide annual pricing | A) **Total service cost** for the Vulnerability Assessment which includes the **NIST-based Cybersecurity Risk Assessment** and **Full Internal/External Network Vulnerability Scan including a Domain Controller Configuration Audit**: $33,875<br>**Risk Management / Cybersecurity Consulting:**<br>Hourly rate: $389<br>Hours purchased in block of 20: $369/hour<br>B) $33,875 + desired Cybersecurity Consulting hours (variable)<br>C) Service costs (firm-fixed):<br>**NIST-based Cybersecurity Risk Assessment (firm-fixed):**<br>$24,975<br>**Full Internal/External Network Vulnerability Scan including a Domain Controller Configuration Audit (firm-fixed):**<br>$8,900<br>**Risk Management / Cybersecurity Consulting:**<br>Hourly rate: $389<br>Hours purchased in block of 20: $369/hour |

| **Response Part 3, Item 4: Price Structure** | |
|---|---|
| Provided a detailed description of the Consultant price structure or pricing option for the services to be provided by the Consultant. | Service costs:<br>**NIST-based cybersecurity Risk Assessment (firm-fixed):**<br>$24,975<br>**Full internal/external network Vulnerability Scan including a Domain Controller Configuration Audit (firm-fixed):**<br>$8,900<br>**Risk Management / Cybersecurity Consulting:**<br>Hourly rate: $389<br>Hours purchased in block of 20: $369/hour |
| If the Consultant has a standardize agreement used for such services, include a copy with the Proposal. | See Appendix A – Standardized Agreement |

## Appendix A – Standardized Agreement

**Cybersecurity Risk and Vulnerability Assessment:**

- **NIST-based cybersecurity Risk Assessment (firm-fixed):** $24,975
- **Full internal/external network Vulnerability Scan including a Domain Controller Configuration Audit (firm-fixed):** $8,900
- **Risk Management / Cybersecurity Consulting:**
  Hourly rate: $389
  Hours purchased in block of 20: $369/hour

## Accurate Information

To complete the Services, some information may only be derived from Client or Client external IT service provider. Any information needed from any external or internal entity shall be coordinated through Client Security Officer/IT Manager/Coordinator. Client is responsible for potential fees generated by any external agency/IT provider.

## Privacy Statement

Client and GlobalSecurityIQ both agree that neither party shall disclose, in whole or in part, by any means whatsoever, any Proprietary Information provided by the disclosing Party to any third party without the express prior written consent of the disclosing Party. The receiving Party shall not alter, modify, decompile, disassemble, reverse engineer, or create derivative works from the disclosing Party’s Proprietary Information. The receiving Party shall use Proprietary Information of the disclosing Party only for the limited purpose described above and not for any other purpose. Proprietary Information shall include, but is not limited to, specifications, frameworks, outlines, designs, process information, technical data, marketing and business plans, customers’/client names/data, product road maps, pricing, toolkits, software, and/or intellectual property that the disclosing Party considers to be protected by applicable laws.

## Billing

Risk Assessments require ½ down. Time charges/service charges are billed monthly and/or at the conclusion of each Service quoted herein and are payable within 15 days of Client receipt of GlobalSecurityIQ’s invoice. Should Client account remain unpaid after 30 days, a late-payment fee of 0.95% per month will be added to the amount due.

**For Cybersecurity Consulting (outside of firm-fixed Services):**

Telephonic and remote hours will be billed at 1/4 hour increments and 1/2 hour increments on holidays, nights, and weekends. Onsite work will be billed at a one (1) hour minimum, in 1/4 hour increments, in addition to travel.

All work will be performed on Monday-Friday during traditional business hours (8:30 AM – 5:00 PM). Any work performed on a Saturday will be billed at 1.5 times the regular rates detailed above. Any work performed on a Sunday or Holiday will be billed at two (2) times the regular rates detailed above. GlobalSecurityIQ's holiday schedule follows "federal holidays" as set by U.S. Office of Personnel Management (OPM) (www.OPM.gov).

Hourly rates are subject to a 3% increase each year from the date of this Agreement. GlobalSecurityIQ's normal incident response hourly rate is $450.00 flat and will be lowered to the quoted rate as long as the Client's bill remains current. This discounted rate will be guaranteed for one (1) year after the date of this quote and increased 3% each year thereafter.

In addition to GlobalSecurityIQ's fees for rendering the Services, Client shall be responsible for, and GlobalSecurityIQ's invoices will include, separate charges for performing services such as computer database searches, photocopying, delivery/messenger charges, travel/mileage/tolls, hard drives/equipment, and other expenses and services incurred incidentally to the performance of the Services. Travel outside a 50-mile radius of Buffalo, New York will result in additional travel expenses.

## Disclaimer

The Parties understand and agree that while the performance of these Services may improve the Client's security posture, the Services can neither identify nor eliminate all risks by unauthorized or authorized parties to affect the Client's environment, business, electronic and other systems.

Limitation of Liability: In no event will GlobalSecurityIQ be liable for any consequential, indirect, exemplary, special, or incidental damages arising from or relating to this Agreement. GlobalSecurityIQ total cumulative liability in connection with this Agreement, whether in contract or tort or otherwise, will not exceed the aggregate amount of fees owed by Client to GlobalSecurityIQ for Services performed under this Agreement.

## Indemnity

Client agrees to indemnify, defend and hold harmless GlobalSecurityIQ against any liability (including attorney's fees and court costs) arising from Services described above.

## Governing Law

This Agreement shall be governed by the laws of the State of New York, without regard to its principles on conflicts of law, and any disputes hereunder shall be heard by a court of competent jurisdiction in Erie County, New York.

This Agreement (the "Agreement") is entered into February 16, 2021, by and between Client and GlobalSecurityIQ, LLC.

By:

_______________________________________

Name:

_______________________________________

Title:

_______________________________________

GlobalSecurityIQ, LLC.

By:

_______________________________________

Holly L. Hubert
Chief Executive Officer

County of Erie
**Mark Poloncarz**
County Executive
Division of Equal Employment Opportunity
**Certification Letter**

Jesse L. Burnette
Director

July 19, 2018

GlobalSecurityIQ, LLC
1576 Sweet Home Rd Suite 102C
Amherst, New York 14228

Dear Ms. Hubert:

The County of Erie & City of Buffalo Joint Certification Committee has completed its review and evaluation of your application for certification as a bona-fide Women Business Enterprise. Your application is approved for the original trade only.

Based upon the information provided by your firm, the Joint Certification Committee has determined that your company is owned, controlled and operated by Women in accordance with the definition set forth by the County of Erie Local Law No. 1-1987. Consequently, certification of GlobalSecurityIQ, LLC is hereby granted to provide the following services:

- Cybersecurity related services to include Risk/Vulnerability Assessments; Penetration testing; Digital Forensics; Education for boards, Leadership/Management and Employees

This certification is recognized by the following agencies and authorities: The County of Erie, City of Buffalo, Buffalo Sewer Authority, Buffalo Board of Education and Buffalo Municipal Housing Authority.

The Joint Certification Committee must be notified in writing of any changes which may affect the ownership, control and operation of the business and of any restructuring, which includes the issuance of stock, changes in the bylaws or any other changes affecting the proprietorship of the business.

Your certification expires on July 21, 2021 however, certification may be revoked or suspended by the Joint Certification Committee for reasonable cause.

Please **be advised that the Joint Certification Committee has been revised its current Rules and Regulations. The new Rules and Regulations have been published on the EEO website, http://www2.erie.gov/eeo/.**

**Respectfully,**

Jesse L Burnette

**Jesse L. Burnette**
**Erie County & City of Buffalo**
**Joint Certification Committee**

**CC: Joint Certification Committee Members**

EXCELSIOR

# NEW YORK STATE

## MINORITY- AND WOMEN-OWNED BUSINESS ENTERPRISE ("MWBE")

## CERTIFICATION

Empire State Development's Division of Minority and Women's Business Development grants a

## Women Business Enterprise (WBE)

pursuant to New York State Executive Law, Article 15-A to:

## GlobalSecurityIQ, LLC

**Certification Awarded on:** July 29, 2019
**Expiration Date:** July 29, 2022
**File ID#:** 64632

NEW YORK
STATE OF
OPPORTUNITY.

Division of Minority
and Women's
Business Development

A Division of Empire State Development

# Women-Owned Small Business Program Self-Certification Summary

## GLOBALSECURITYIQ, LLC

**DUNS:** 080933400

**CAGE:** 84Q21

Summary

### 8(a)

Is the qualifying individual(s) currently certified by the U.S. Small Business Administration as an 8(a) Business Development (BD) Program Participant and does this woman own at least 51% of the business?
**Response:** No

### Third Party

Is the qualifying individual(s) certified as a WOSB or EDWOSB by an SBA-approved Third-Party Certifier?
**Response:** No

---

## Non-qualification

Has an SBA-approved Third-Party Certifier declined WOSB or EDWOSB certification for the qualifying individual(s)?
**Response:** No

---

## LLC

Do the Articles of Organization, Operating Agreements and any amendments show that at least 51% of each class of member interest is unconditionally and directly owned by the qualifying individual(s)?
**Response:** Yes

**Attachments:**

| File Name | Document Type | Upload Date |
|---|---|---|
| Certificate of GlobalSecurityIQ Articles of Organization.pdf | Articles of incorporation | 07/15/2018 |
| Operating Agreement GlobalSecurityIQ single member LLC.pdf | Unknown | 07/15/2018 |

Do the Articles of Organization and any amendments or Operating Agreement and any amendments show that the qualifying individual(s) serve as management members, with control over all decisions of the limited liability company?

**Response:** Yes

**Attachments:**

| File Name | Document Type | Upload Date |
|---|---|---|
| Certificate of GlobalSecurityIQ Articles of Organization.pdf | Articles of incorporation | 07/15/2018 |
| Operating Agreement GlobalSecurityIQ single member LLC.pdf | Unknown | 07/15/2018 |

## Citizenship

Do the birth certificates, naturalization papers, or passports show the qualifying individual(s) are U.S. citizens?
**Response:** Yes

**Attachments:**

| File Name | Document Type | Upload Date |
|---|---|---|
| birth cert.pdf | Birth certificates | 07/15/2018 |

## Ownership

Is the following statement true? The qualifying individual(s) is not subject to any conditions, executory agreements, voting trusts, or other arrangements that cause or potentially cause ownership benefits to go to another person.
**Response:** Yes

Is the qualifying individual's ownership direct; that is the ownership is not held through another business entity (including employee stock ownership plan) that is, in turn, owned and controlled by the qualifying individual(s)?
**Response:** Yes

If the 51% ownership is held through a trust, is the trust revocable, and does it designate the qualifying individual(s) as the grantor, the trustee, and the sole current beneficiary?
**Response:** Na

## Management

Are the management and daily operations of the business controlled by the qualifying individual(s)?
**Response:** Yes

Does the qualifying individual(s) hold the highest officer position in the business and does she have the managerial experience needed to run the business?
**Response:** Yes

**Attachments:**

| File Name | Document Type | Upload Date |
|---|---|---|
| H Hubert Resume July 2018.pdf | Resume | 07/15/2018 |

Does the qualifying individual(s) have ultimate managerial and supervisory control over those who possess the required licenses or technical expertise for the business? The qualifying individual(s) herself may have the technical expertise or possess the required license for the business.

**Response:** Yes

Does the qualifying individual(s) who holds the highest officer position manage the business on a full-time basis and devote full-time attention to the business during the normal working hours of similar businesses?
**Response:** Yes

Does the qualifying individual(s) fully control the business, that is, no one else has actual control or has the power to control the business?
**Response:** Yes

Is the qualifying individual(s) in control of long-term decision making and day-to-day operations?
**Response:** Yes

---

## SBA Exam

Is the following statement true? The qualifying individual(s) has not received a decision from the SBA – in connection to an examination or protest – finding that the business does not qualify as a WOSB or an EDWOSB.
**Response:** Yes

---

Certificate Letter

Print Back

Return to top

Your experience is important to us! Please visit the **Certify Knowledge Base** for assistance.

**SBA.gov/contracting**

**WhiteHouse.gov**

**Regulations.gov**

**BusinessUSA.gov**

**USA.gov**

U.S. Small Business Administration

## Contact SBA

(800) 827-5722

Version: 4.6.2.ga57b81509b0e99fcc3b2a3e5958dbbd83e74e32f

# Cybersecurity Development Program

# Cybersecurity Risk & Vulnerability Assessment

## Proposal

For:

Date: 6/10/2021

**Prepared by:**

Felix DiCamillo
VP of Sales | Sedara
716-261-9940 ext. 103
Felix.dicamillo@sedarasecurity.com

**Prepared for:**

Terrence D. McCracken
Secretary to the Authority | Erie County Water Authority
295 Main Street, Room 350 Buffalo, New York 14203
tmccracken@ecwa.org

# Contents

PART 1 ........ 3

PART 2 ........ 3

Item 1 – Consultant Business Form ........ 3

Item 2 – Consultant Team ........ 4

Order of Escalation ........ 7

Roles and Responsibilities ........ 8

PART 3 ........ 9

Item 1 – Proposed Scope of Services ........ 9

Pre-Engagement ........ 10

Intelligence Gathering ........ 11

Vulnerability Analysis ........ 12

Exploitation ........ 12

Post-Exploitation ........ 13

Initial Findings ........ 13

Next Steps and Follow up ........ 14

Scope ........ 14

Item 2 – Hardware and Software Requirements ........ 16

Hardware ........ 16

Software ........ 16

Item 3 – Timeframe for Deliverables ........ 17

Project Management Deliverables ........ 17

Report ........ 17

Projected solutions and costs ........ 18

Item 4 – Price Structure ........ 19

Definitions ........ 19

# PART 1

| Sedara | |
|---|---|
| 77 Goodell St. Suite 420<br>Buffalo, NY 14203<br>Telephone: 844-4-SEDARA | |
| **Contact Person:** | Felix DiCamillo |
| **Title:** | VP of Sales |
| **Phone:** | 585-944-1006 |
| **Email:** | Felix.dicamillo@sedarasecurity.com |
| Program Contact: | Dilip Singh |
| Phone: | 716-261-9940 ext. 108 |
| Email: | Dilip.Singh@sedarasecurity.com |

# PART 2

## Item 1 – Consultant Business Form

1. Identify the Consultant's business or corporate structure:
    a. If a corporation, including the following:
        i. Date and State of Incorporation
            1. November 7, 2013 New York
        ii. List Name and Title of Executive Officers
            1. Darrick Kristich, CEO
        iii. Principal Place of Business
            1. Buffalo, New York
        iv. List all Related Principal or Subsidiaries Corporations
            1. None
        v. Closed or Publicly Traded
            1. Closed
        vi. EIN
            1. 46-4123250
    b. If a Partnership…
        i. N/A
    c. If a Joint Venture…
        i. N/A
    d. If a Sole Proprietorship…
        i. N/A

2. Identity the number of years your entity has been in business.
    a. 8 years

3. Identity whether your business/corporate structure has changed in the past five years and if yes, describe the change.
    a. No

4. Identity the type and coverage amount of all insurance policies.
    a. General Liability: $1 million per occurrence / $2 million aggregate
    b. Umbrella: $10 million per occurrence / $10 million aggregate
    c. E&O/Cyber: $20 million per occurrence
    d. Workers' Compensation: $1 million per occurrence

5. Identified the name, address, and contract information for three (3) companies that the Consultant has performed similar services to those being sought by the Authority.
    a. Corning Museum of Glass
        i. Contact name: Damon Smith
        ii. Title: IT Security and Network Operations Supervisor
        iii. Email: smithdv@cmog.org
    b. Mercantile Solutions
        i. Contact name: Tom Vaughn
        ii. Title: VP of IT/CISO
        iii. Email: TVaughan@mercantilesolutions.com
    c. West Herr Automotive Group
        i. Contact name: Nate Wintringer
        ii. Title: Director of IT
        iii. Email: nwintringer@westherr.com
6. If you are a certified, minority and/or women owned business, submit a copy of the certification.
    a. N/A

## Item 2 – Consultant Team

<table>
<tr><th colspan="2">Dilip Singh | VP of Cyber Operations</th></tr>
<tr><td>Relevant Qualifications and Experience:</td><td>Over 24 years of business and technical IT and Cybersecurity experience.</td></tr>
<tr><td>State and County of Residence:</td><td>Erie County, New York</td></tr>
<tr><td>Scope of responsibility:</td><td>> Act as Erie County Water Authority's Chief Information Security Officer<br>> Create, Outline and implement Vulnerability Mitigation Plan<br>> Align with Erie County Water Authority's governance, risk and compliance<br>> Map initiatives to NIST Cybersecurity Framework 1.1<br>> Help align and prioritize Erie County Water Authority's cybersecurity activities with its business/mission requirements, risk tolerances, and resources.</td></tr>
</table>

| | |
|---|---|
| | > Cybersecurity activities, outcomes, and informative references that are common across Erie County Water Authority and critical infrastructure.<br>> Using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of Erie County Water Authority's risk management processes.<br>> Communicate among internal and external stakeholders about the assessment.<br>> Advise, Document Report and Present<br>> Deliver a Plan of Action and Milestones (POAM) document to Erie County Water Authority. |
| Length of time working for Sedara: | 3 years |

### Nick Aures | Offensive Security Consultant

| | |
|---|---|
| Relevant Qualifications and Experience: | Over 10 years of IS and IT experience. Certified Ethical Hacker (CEH). |
| State and County of Residence: | Erie County, New York |
| Scope of responsibility: | > CEH imparts offensive tactics supplemented with defensive countermeasures.<br>> CEH professional can have a holistic security perspective of the organization.<br>> Leads a team of highly technical red teamers.<br>> Utilizing various frameworks and methodologies including, but not limited to:<br>○ National Institute of Standards and Technology (NIST) guidelines<br>○ Framework for Improving Critical Infrastructure Cybersecurity - NIST Cybersecurity Framework (CSF) 1.1<br>○ Penetration testing Execution Standard (PTES)<br>○ NIST 800-115<br>○ The Open Web Application Security Project (OWASP)<br>○ Payment Card Industry Data Security Standards (PCI-DSS)<br>○ MITRE ATT&CK<br>> Understands advanced Red Team concepts such as performing covert operations against complex networks while remaining entirely undetected, advanced application manipulation, and programming concepts.<br>> Manage internal and external interactions and communications with stakeholders in a professional manner, referring problems to and communicating with the appropriate department manager or director.<br>> Lead teams supporting operating system testing, database testing, network fabric asset testing, and wireless communication testing. |

| | |
|---|---|
| | ➢ Lead team members to conduct web application security testing activities for web applications and web-services<br>➢ Develop comprehensive and accurate reports and presentations for both technical and executive audiences<br>➢ Lead the scoping, planning, and execution of prospective engagements<br>➢ Typically manages complex projects, involving delegation of work and review of work products |
| Length of time working for Sedara: | 3 years |

## Christopher Bruns | Cybersecurity Program Analyst

| | |
|---|---|
| Relevant Qualifications and Experience: | Security+ certification. |
| State and County of Residence: | Broome County, New York |
| Scope of responsibility: | ➢ Experience with firewalls, vulnerability management, and intrusion detection systems.<br>➢ Responsible for managing customer security systems, including Endpoint Security, IDS and others.<br>➢ Responsible for monitoring and analyzing information security tools, events and collected data, across many customer environments.<br>➢ Provide prescriptive guidance on discovered security issues, current data collection practices, incident response activities and corrective actions.<br>➢ Ensures compliance with and provide input to security policies, standards and procedures.<br>➢ Conducts all tasks in accordance with the requirement to comply with security controls.<br>➢ Researches and provides input to customer and internal security strategy<br>➢ Follows trends and technologies related to IT Security and Compliance.<br>➢ Knowledge in:<br>o Vulnerability Management<br>o Managed Detection and Response (MDR)<br>o Firewalls<br>o Endpoint Security<br>o Intrusion Detection System (IDS)<br>o Intrusion Prevention System (IPS)<br>o Virtual Private Network (VPN) and Remote Access<br>o Security Incident Response (IR)<br>o Desktop Encryption<br>o Device Management<br>o Patch Management |
| Length of time working for Sedara: | 1 year |

| Darrick Kristich \| Executive Sponsor | |
|---|---|
| Relevant Qualifications and Experience: | Over 10 years of business and technical IT and Cybersecurity experience. |
| State and County of Residence: | Erie County, New York |
| Scope of responsibility: | Executive level leadership in cybersecurity, risk, program management, enterprise systems or related information technology advisory engagements.<br>Key sponsor of initiatives, internal and external. |
| Length of time working for Sedara: | 8 years |

## Order of Escalation

There will be consultants working with the Authority through the engagement however Sedara will be available 24x7 for support throughout the engagement.

Escalation begins with the following contact information:

- By Phone:
  - Technical - 716-261-9940 or 844-4SEDARA option 1
    - This will ensure the current technical resource is reached via phone 24x7x365
    - This will also log when calls are received for reporting purposes
    - Technical resource will open a ticket to track activity and time for reporting purposes
    - Appropriate technical resource will call back following ticket escalation
  - Non-technical – Sales contact phone number from table in Section 1
- By Email:
  - Technical: help@sedarasecurity.com
    - This will ensure a ticket is generated in our system and the current technical resources will be notified to begin the appropriate escalation immediately.
  - Non-technical – Sales contact phone number from table in Section 1

The more Sedara understands the actual services required, the more detail can be added to the escalation process.

### Normal Business Hours Escalation

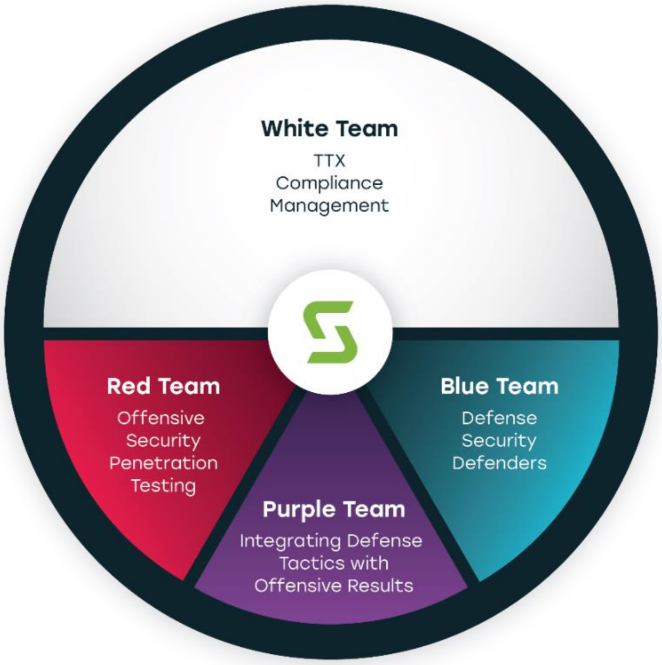
- If urgent technical request, contact the Sedara Technical Contact via information in Section 1.
- If urgent account engagement request, contact the Sedara Sales Contact via information in Section 1.
- If general service request, contact the Sedara Program Contact via information in Section 1.

### After Business Hours Escalation

1. All after-hours requests
   - 716-261-9940 or 844-4SEDARA option 1

## Roles and Responsibilities

Sedara will provide Red Team and White Team resources for this engagement. The Red Team offers many real-world attack vectors and simulations. They attempt real world attack to gain access to what is important to you as a company. The White Team manages the engagement and includes project management.



### Red Team

- External, internal, web, app, wireless, physical penetration testing and scanning
- Social Engineering

### White Team

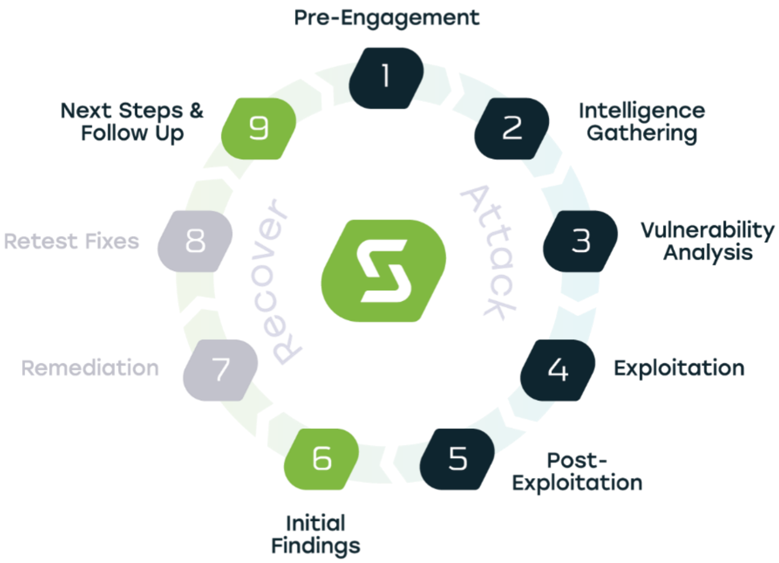
- Management
- Internal and External Governance, Risk and Compliance (GRC)

# PART 3

## Item 1 – Proposed Scope of Services

Sedara will work in consultation with the Erie County Water Authority ("the Authority") IT staff to develop a comprehensive IT Cybersecurity Risk and Vulnerability Assessment.

The proposed scope of work outlines a Cybersecurity Risk & Vulnerability Assessment ("the assessment") for Erie County Water Authority's network. This follows 7 of the steps in Sedara's 9-step approach shown below.



The engagement will involve conducting a cybersecurity risk and vulnerability assessment, then after the assessment is complete, Sedara will provide a Plan of Action and Milestones (POAM) document. The POAM will report findings and make recommendations to mitigate any risks or vulnerabilities in conformity with the standards developed by the National Institute for Standards and Technology (NIST) for federally designated critical infrastructures (NIST CSF 1.1).

Sedara will provide the assessment with the following objectives:

- Analyzing the Authority's vulnerabilities, threats, and possible consequences from potential internal or external cyberattacks,
- Ranking of the priority and timeframe to address vulnerability and security issues,
- Advising the Authority on matters relating to employee training and education, and preventative measures to be taken to secure Authority assets,
- Recommending additional staffing for the Authority's IT Department, and
- Such other work as may be directed by the Authority's Executive Management Team,

- Testing should be appropriate for complexity, size and risk of organization
- Should include all critical data locations, critical network connections, application storing, processing or transmitting sensitive data
- Attempt to penetrate at network level and application level
- Safely and effectively execute a technical information security assessment using the presented methods and techniques
- Appropriately handle technical data (collection, storage, transmission, and destruction) throughout the assessment process
- Use Assume Breach testing in to identify and exploit system and network service vulnerabilities to assess whether a motivated insider or visitor could elevate access to cause harm to Erie County Water Authority
- Solution adopted to realize risk-based vulnerability management practices with the confidence to report risk at an organizational level

Sedara uses industry-accepted assessment approach derived from industry best practices such as but not limited to **NIST CSF 1.1, PTES**, **NIST SP 800-115**, **OWASP** and **OSSTMM** methodologies. The best practice methodologies will ensure a standardized risk mitigation approach that will offer the highest risk reduction potential, complementing the "Framework for Improving Critical Infrastructure Cybersecurity", developed by the National Institute for Standard and Technology, as requested in the RFP Part 3 Item 1 d.

### Pre-Engagement

- Defining targets based on scope
- Defining teams
- Terms and Conditions of Erie County Water Authority's internal sponsors
- Identify Rules of Engagement
    - Debriefing frequency and contact method
    - Start and end-dates of the testing
    - Times at which testing may occur
    - What personnel are notified about testing
    - Approval process to commence the attack upon an IP being shunned
    - Approval process to commence the attack upon encountering a Security Barrier
    - Determine point of contact for bypassing common security controls (i.e. – firewall, antivirus, 2FA, etc.)
    - Determine Time-to-Detect and Time-to-Mitigation reporting
    - List of IP's we will be testing from
    - Type of testing will be grey-box
    - What is the policy in regards to viewing data on compromised hosts?

- Scoping Process
    - Determine and define Assume Breach for customer
    - Determine if there are specific concerns/focuses
    - Determine contacts from both parties
    - Determine length of test
    - Determine debrief frequency and method
    - Determine if any testing restrictions exist (times, machines, methods, etc.)
    - Determine methods for internal tests (i.e. - VPN connection to segments needing tests, SMA provided by Sedara, etc.)
    - Determine customer policy on viewing sensitive data

## Intelligence Gathering

- (RFP Part 3 Item 1 a) Review of current state of the Authority's information technology security
- Discovery Scans
    - External
        - Determine status of all ports on public facing devices/applications
        - Determine services running on public facing devices/applications
        - Determine if there are known vulnerabilities with the devices, applications, and services that have been discovered
        - Determine if there are any common configuration vulnerabilities
        - Publicly available information disclosure search
        - Additional information discovery as it relates to attack and exploitation planning
    - Internal
        - Determine status of all ports on internal devices/applications
        - Determine services running on internal devices/applications
        - Determine if there are known vulnerabilities with the devices, applications, and services that have been found
        - Determine if there are any common configuration vulnerabilities
        - Determine internal access controls to be further assessed during attack phase
    - Web Application scans
    - Operation Technology scans
        - Including SCADA systems, PLCs, DCS, IED, HMIs and more

### Vulnerability Analysis

Begin analysis based on scan results.

- Researching Common Vulnerabilities and Exposures (CVE)
- Looking for public exploits related to vulnerabilities
- Identifying attack methods related to Common Weakness Enumerations (CWE) that we find
- (RFP Part 3 Item 1 e) Review the Authority's current Supervisory Control and Data Acquisition (SCADA) water systems for security vulnerabilities.
    - Our solution actively queries SCADA assets on your network. Active querying gives us deep insights and unparalleled situational awareness into your infrastructure without impacting operations. This patented approach gathers far more information than passive monitoring alone, including identification of devices that do not communicate on your network.
- (RFP Part 3 Item 1 e) Review current system-specific operating systems and firmware versions for known exploits and recommend upgrades, updates, and mitigations. This includes firewalls, switches and routers, Microsoft Active Directory, email and file servers, web servers, wireless routers, WAN, VPN, VoIP, and CCTV systems.
- (RFP Part 3 Item 1 e) Assess VoIP network system components for security vulnerabilities, validating system-specific operating system and firmware versions and reviewing for known exploits.
- (RFP Part 3 Item 1 e) Evaluate the Authority current threat posture including antivirus and Intrusion Detection and Prevention (IDP) capabilities.
- (RFP Part 3 Item 1 e) Evaluate the Authorities planned changes and improvements to the threat surface and assist identifying and addressing security concerns.

### Exploitation

- Attack/Additional Discovery
    - (RFP Part 3 Item 1 e) Test for susceptibility to Advanced Persistent Threats (APTs) such as viruses, malware, Trojan horses, botnets, and other targeted attack exploits.
    - (RFP Part 3 Item 1 e) Execute and review internal network vulnerability scans and external vulnerability and penetration scans and make recommendations to reduce the threat attack surface.
    - Exploit vulnerabilities found externally and/or internally to determine repercussions of each.
        - Document additional discovery or effects of exploitation
        - Document recommended mitigations for each
        - Dangerous exploits will not be used (Blue Screen, DDOS, anything that deletes or modifies data, etc.)

- Wireless Testing for 4 SSID's. (RFP Part 3 Item 1 e) Review wireless network system components for security vulnerabilities, validating system-specific operating systems and firmware versions for known exploits and recommend upgrades, updates, and mitigations.
    - Password attacks
    - WEP/WPA cracking
    - Guest wireless segmentation checks
    - Traffic sniffing attacks
    - SSID spoofing
    - Rogue access point discovery

## Post-Exploitation

- Typically, exploitation leads to either data leaking or access being improperly gained. In either event, during post exploitation an attacker will review either the data, or their new set of permission as if they were back to phase 2 (Intelligence Gathering).
- The actions that follow vary based on many things but they can include actions such as:
    - Strengthening the "foothold" or essentially creating some form of persistence so the attack can continue to further the attack without worrying their only connection being discovered and dropped
    - Digging for sensitive data that can be viewed or exfiltrated as per customers data exfiltration policy
    - Attempting to improve the level or privilege the attacker has
    - Proving business impact from exploitation as relevant to the customer, to the best of our ability given the limited knowledge of the network
    - Providing feedback and validation as to best practices controls

## Initial Findings

- Report from assessment results tied to business impact
    - Technical narrative
    - Attack narrative
    - Identified targets and focus
    - Vulnerability Priority Rating (VPR) scoring to generate vulnerability and risk levels using intelligence gained for each asset in your OT network. Reports include detailed insights, along with mitigation suggestions. This will enable Sedara and the Authority to quickly identify the highest risk for priority remediation before attackers can exploit vulnerabilities.

## Next Steps and Follow up

- Plan of Action and Milestones
    - (RFP Part 3 Item 1 b) Development of a vulnerability mitigation plan
    - (RFP Part 3 Item 1 c) Development of a prioritized road map of activities to enhance the Authority's future Cybersecurity position
- (RFP Part 3 Item 1 e) Recommend or assist in selection of vulnerability scan software for purchase/license for continued use by the Authority after the assessment is complete.

## Scope

Sedara will be carrying out external and web application penetration testing, and internal and wireless Risk and Vulnerability scans for Erie County Water Authority. The scope of what will be assessed is shown below.

### Web App

Multiple web applications with varying degrees of authentication will be tested. The Authority will provide credentials for the authenticated testing.

- 4 web applications
    - 3x unauthenticated web application tests
    - 1x both unauthenticated and authenticated web application test
        - Authenticated roles:
            - Customer
            - Employee

### External

All external IPs in the following range are considered in scope and will be tested.

- Two 26-bit subnets
- Passive scan estimation table (Used for proposed pricing)

| Domain | IP Addresses |
|---|---|
| alerts.ecwa.org | 72.43.206.133; |
| autodiscover.ecwa.org | 52.96.69.8;52.96.88.8;52.96.182.104;52.96.9.184;2603:1036:302:415d::8;2603:1036:302:481e::8;2603:1036:302:415b::8;2603:1036:302:4833::8; |
| cw.ecwa.org | 40.117.238.82; |
| cw2.ecwa.org | 40.76.53.11; |
| ecwa.org | 107.180.92.100; |
| email.ecwa.org | 65.207.39.132;72.43.206.137; |
| ftp.ecwa.org | 72.43.206.133; |
| mail.ecwa.org | 72.43.206.137; |
| my.ecwa.org | 72.43.206.133; |
| portal.ecwa.org | 40.121.54.34; |
| portal2.ecwa.org | 40.87.125.181; |

| | |
|---|---|
| sip.ecwa.org | 52.112.65.27;2603:1037:0:c::f;2603:1037:0:a::b;2603:1037:0:15::c;2603:1037:0:7::b;2603:1037:0:2::b;2603:1037:0:e::f;2603:1037:0:5::b;2603:1037::b; |
| testweb.ecwa.org | 72.43.206.138; |
| w3.ecwa.org | 72.43.206.133; |
| www.ecwa.org | 107.180.92.100; |

### Internal (RFC 1918)

Any internal networking (routing/switching) infrastructure that can or needs to be leveraged for the assessment and can also be considered in-scope. In the past, siloed IT and OT security practices resulted in significant blind spots, thus limiting the ability to detect vulnerabilities and prevent attacks. Our approach eliminates blind spots with a holistic view of cyber exposure with both IT and OT domain expertise in a single solution to comprehensively identify potential risks and address security threats sooner.

- 2000 IP's
  - 300-400 workstations
  - 100 servers
  - Various other systems and infrastructure
- 100 PLC's

### Wireless

- 4 SSID's

### Out of Scope

- Social Engineering including the following campaigns
  - Live payloads sent to users via email. Payloads give Sedara remote access, and do not damage the "infected" machine
  - Credential harvesting attempts to users via email.  The goal is to collect credentials from users which can then be used during the test
  - Payloads sent to users via mailed USB/flash drives. Payloads give Sedara remote access, and do not damage the "infected" machine.
  - Retest fixes
    - Test the initial findings to check the success of remediation efforts. Another report is provided to validate that the recommended fixes were made and verified.
- Phishing risk assessment
- Physical cybersecurity testing

## Item 2 – Hardware and Software Requirements

### Hardware

Sedara will provide a preconfigured Security Management Appliance (SMA) for the assessment. The SMA is a hardware appliance that will act as an assumed breach on the Authority's network as if an internal endpoint or server has already been compromised. By assuming that an attacker has obtained access to the internal network, we can then operate from the standpoint of a real-world attack.

The SMA will also be used for Penetration testing tools and assume breach testing. This reduces the need for Erie County Water Authority to provide additional infrastructure such as RDP, VDI, etc. for the assessment.

#### Model

SMA3000v3

#### Specifications

- Operating System: Linux
- Dell Model: PE R240
- RAM: 48GB
- OS Storage: 2x 1TB SATA 6Gps (SW RAID 1) and 16GB SD
- HD: 2x 4TB Single SATA 6Gbps (SW RAID 1)
- CPU: Xeon E-2246 6C/12T
- PSU: Single 450W
- Chassis: 1U
- Networking: Onboard Dual Port and Dual Port 1Gbe

#### Connectivity Requirements

- Internal network DHCP lease
- Customer will provide any special cabling needed

### Software

Sedara will provide all required software for the assessment. Some of the more common tools we use are as follows:

- **TenableIO** – A vulnerability scanning and management tool
- **TenableOT** – A vulnerability management tool for SCADA systems
- **Rapid7 Metasploit** - A vulnerability scanning and penetration testing framework tool.
- **Cobalt Strike** - A command-and-control infrastructure suite.
- **Burpsuite Pro** - The golden standard tool for web application testing.
- **Nmap** - Network mapping and service identification tool.
- **Masscan** - Network mapping and service identification tool.

- **Responder** - LLMNR/NBT-NS/mDNS Poisoner for spoofing.
- **Bettercap** – A man-in-the-middle framework.
- **PowerSploit** – A powershell-based offensive security toolkit.
- **CME (CrackMapExec)** - A powershell-based offensive security toolkit.
- **BloodHound/SharpHound** – Active directory domain security mapping.
- **ADRecon** – Active directory data dumping tool.
- **Nikto** – Web application vulnerability scanning.
- **OpenVas** – Network vulnerability scanning.

Sedara may use other various tools.

These will reside independently from Erie County Water Authority's network or on the SMA, and will be pre-approved by Erie County Water Authority.

## Item 3 – Timeframe for Deliverables

The timeframe for deliverables outlined below are based on Sedara's current understanding of the scope from the RFP, RFP Q&A, and availability of Erie County Water Authority personnel. The timeframe and deliverables are subject to change.

### Project Management Deliverables

- Work Breakdown Structure (WBS) will be delivered within 1 week after scope acceptance.
- The schedule and dependencies will be delivered 1 week after scope acceptance.
- Weekly status reports including risks and progress reports will be delivered once per week.
  - If a severe risk is discovered during the assessment, the Authority will be notified immediately.

### Report

Delivery of Final Report, Documentation and POAM shall not exceed 15 business days after assessment completion. This will include the following.

- Executive summary detailing the Authority's Cybersecurity position, including a comparative scorecard of findings.
- Results of vulnerability testing.
- Identified cybersecurity vulnerabilities, gaps, and mitigation plans.
- A POAM
  - Prioritized road map of activities, developed in conjunction with Authority's IT staff to enhance the Authority's future cybersecurity position

### Projected solutions and costs

Projected solutions and costs will be provided after review and discussion of the report and POAM with the Authority at the end of the initial assessment.

- (a) Provide an estimated range, based upon previous experience, of the total services costs to implement the proposed solutions,
- (b) Include a Rate Sheet that specifies and itemizes the cost for each proposed component, including all licensing, support, maintenance, and hosting fees, and
- (c) For subscription-based services, provide annual pricing.

The table below shows current estimates for potentially recommended licensing, implementation services, and training for vulnerability management technology on an annual basis. These estimates are based on Sedara's current limited understanding. The pricing will vary depending on exact count of assets and type of assets in scope.

Pricing may also vary depending on additional services or monitoring the Authority may want to include, or line items that the Authority may not want to include.

Please note that the pricing directly below is a rough estimate and is subject to change based on proper scoping and potential discounts.

| Vulnerability Management | Quantity | Unit Cost | Total |
|---|---|---|---|
| Tenable.io vulnerability management for 750 Assets – 1 Year, includes Standard Tenable VM Container | 1 | $26,250 | $26,250 |
| Tenable.io Quick Start Deploy Remote Implementation | 1 | $6,000 | $6,000 |
| 2-Day Seat for Tenable.io Specialist Course training | 1 | $2,000 | $2,000 |
| Tenable.ot for 500 Assets – 1 Year, includes 2 OT configurable sensors | 1 | $35,000 | $35,000 |
| Tenable.ot Core Platform | 1 | $5,000 | $5,000 |
| Tenable.ot Quick Start Deploy Remote Implementation | 1 | $15,600 | $15,600 |
| Staff Augmentation Weekly | 1 | $13,500 | $13,500 |

Annual rough estimates for licensing, implementation and training.

| Year | Total |
|---|---|
| Year 1 estimate | $103,350 |
| Annual estimate for Years 2 and beyond | $66,250 |

Sedara can provide a risk and vulnerability management service that includes licensing and services in a single subscription. This would include managed vulnerability scanning, analysis, reporting and actionable risk and vulnerability guidance on a 24x7x365 basis from Sedara's Security Operations Center. This pricing will be delivered after review and discussion of the report and POAM with the Authority at the end of the initial assessment.

## Item 4 – Price Structure

1. Provided a detailed description of the Consultant price structure or pricing option for the services to be provided by the Consultant.

Sedara estimates that the risk and vulnerability assessment and penetration testing requested by the original RFP will take about 16.5 days of effort. Days of effort will often exceed the minimum of 8 hours per day including after normal business hours. Billing will be mutually agreed upon between Erie County Water Authority and Sedara.

| Cybersecurity Development Program | Teams | Days of Effort | Unit Cost | Total |
|---|---|---|---|---|
| Pre-Engagement Planning | Red | 1 | $2,000 | $2,000 |
| External Penetration Test | Red | 4 | $2,000 | $8,000 |
| Assume Breach - RFC 1918 | Red | 7.5 | $2,000 | $15,000 |
| Web Application Testing | Red | 4 | $2,000 | $8,000 |
| Social Engineering Campaign | - | 0 | - | $0 |
| Wireless Testing | Red | 0 | included | included |
| Physical Penetration Testing | - | 0 | - | $0 |
| Remediation Guidance | White | included | included | included |
| Final Report and Documentation | Red, White | included | included | included |
| Project Manager | White | Full Engagement | included | included |
| Hardware (SMA3000) | Red | hardware | included | included |
| Tenable Vulnerability Scanning licensing | Red | licensing | $4,000 | $4,000 |
| **Total** | | **16.5** | | **$37,000** |

Sedara reserves the right to re-estimate the risk and vulnerability assessment cost if the scope is altered to be different than what is shown in this proposal. If Erie County Water Authority requires an increased scope for the penetration test beyond what has already been proposed, Sedara and Erie County Water Authority will generate an amendment to the agreement.

2. If the Consultant has a standardize agreement used for such services, include a copy with the Proposal.
   - See Appendix A. This is standard language that will be discussed and mutually agreed upon between Sedara and Erie County Water Authority prior to execution.

# Definitions

- **PTES** Penetration Testing Execution Standard is a new standard designed to provide both businesses and security service providers with a common language and scope for performing penetration testing. http://www.pentest-standard.org/index.php/Main_Page
- **NIST SP 800-115** Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
- **NIST CYBERSECURITY FRAMEWORK 1.1** Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective

approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security. https://www.nist.gov/cyberframework/framework

- **OSSTMM** Open-Source Security Testing Methodology Manual (OSSTMM) provides a methodology for a thorough security test, herein referred to as an OSSTMM audit. An OSSTMM audit is an accurate measurement of security at an operational level that is void of assumptions and anecdotal evidence. As a methodology it is designed to be consistent and repeatable. http://www.isecom.org/mirror/OSSTMM.3.pdf
- **OWASP** Open Web Application Security Project™ unbiased source of information on best practices as well as an active body advocating open standards. OWASP focuses on improving the security of software making software security visible to organizations to make informed decisions. https://www.owasp.org/index.php/Main_Page
- **Work Breakdown Structure** organizes the project's total scope while reflecting the work specified. https://www.pmi.org/pmbok-guide-standards/framework/practice-standard-work-breakdown-structures-3rd-edition
- **Assume Breach** is assuming that a breach has already occurred into the network. This supports the concept that there will always be 0-day exploits and allows quicker identification of secondary and tertiary step of an attack.
- **Security Barrier** may be personnel or technical security control that interferes with the red team progressing through the assessment.
- **Grey-box** is a penetration test where some information is available beforehand such as provided log in credentials, but not all information such as a full list of IP ranges or a network map.
- **RFC 1918** is address allocation for private internets. https://tools.ietf.org/html/rfc1918
- **Class A, Class B, or Class C Summary** - Summarizes host information. The vulnerability score for an address is computed by adding up the number of vulnerabilities at each severity level and multiplying it with the organization's severity score. Starting out with a Class A or Class B summary can identify more active network ranges for networks with a large number of active IP addresses. https://docs.tenable.com/tenablesc/Content/VulnerabilityAnalysisTools.htm
- **Interviewing** is the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or identify the location of evidence. Assessment results are used to support the determination of security control effectiveness over time.
- **Days of Effort** is equal to a minimum of 8 hours of work. A typical Red Team day often exceeds 8 hours.
- **GRC is Governance, Risk, and Compliance** for example CMMC, HIPAA, NIST SP 800-171, DFARS, CCPA, GDPR, ITAR.

# Cybersecurity Development Program

# Risk and Vulnerability Assessment

## Standard Agreement Language

For:

**Prepared by:**

Felix DiCamillo
VP of Sales
716-261-9940 ext. 103
Felix.dicamillo@sedarasecurity.com

**Date: 6/10/2021**

# Contents

6. General Terms: .... 3

6.1 Amendments .... 3

6.2 Severability .... 3

7. Confidentiality and Proprietary Rights: .... 3

7.1 Confidentiality .... 3

7.2 Customer Reports .... 4

8. Limitation of Liability & High Risk Disclaimer: .... 4

8.1 Limitation of Liability .... 4

9. Indemnification: .... 5

# 6. General Terms:

### 6.1 Amendments

Except as expressly stated herein, the terms of this Agreement may not be modified except by a written agreement signed by both parties.

### 6.2 Severability

If any provision of this Agreement is held illegal or unenforceable by any court of competent jurisdiction, such provision shall be deemed severed from the remaining provisions of this Agreement and shall not affect or impair the validity or enforceability of the remaining provisions of this Agreement.

# 7. Confidentiality and Proprietary Rights:

### 7.1 Confidentiality

Sedara acknowledges and agrees that it may acquire confidential and proprietary information of Customer including, but not limited to, technical and non-technical data, security information, and other business information of Customer and its clients during the delivery of the penetration test. Customer will own all right, title and interest to data provided to or discovered by Sedara.

Customer acknowledges and agrees that in the delivery of the penetration test by Sedara, Customer may gain access to proprietary and confidential information, developed or acquired by Sedara, including, but not limited to technical and non-technical data, formulas, patterns, compilations, devices, methods, techniques, drawings, contracts, pricing and processes related to Products, their usage or Sedara internal operations. Sedara will own all right, title and interest to data provided to or discovered by Customer.

The parties may use confidential information solely in accordance with this Agreement and will take all reasonable precautions necessary to safeguard the confidentiality of such information. The parties will hold in confidence and not disclose, reproduce, distribute or transmit the confidential information, directly or indirectly, in any form, by any means, or for any purpose, except to those of its employees, agents, consultants or subcontractors who require access for Customer's authorized use of the Software in accordance with the terms of this Agreement. Each party will implement reasonable security measures to protect such confidential information at a level no less restrictive than used to protect its own confidential information.

The parties shall not be restricted under this Section 7 with respect to confidential information that the receiving party affirmatively establishes that (i) has or becomes generally available to the public other than as a result of an act or omission of the receiving party or any of its employees, agents, subcontractors or consultants, (ii) was in the possession of the receiving party before receiving the information, (iii) is independently developed by the receiving party without use of the confidential information, or (iv) is required to be disclosed by law, court order or other legal process, provided that the receiving party shall first provide the disclosing party with prompt written notice thereof.

Customer acknowledges that (i) any use or threatened use of the Software in a manner inconsistent with this Agreement, or (ii) any other misuse of the confidential information of Sedara will cause immediate irreparable harm to Sedara for which there may be no adequate remedy at law. Accordingly, Customer agrees that Sedara shall be entitled to seek injunctive relief in the event of any such breach or threatened breach by Customer, without the need of posting a bond. Nothing contained herein shall limit Sedara's right to any remedies at law.

### 7.2 Customer Reports

Customer shall own all right, title and interest to any reports, summaries, documents, analyses, findings or any other information identified or discovered exclusively for customer.

## 8. Limitation of Liability & High Risk Disclaimer:

### 8.1 Limitation of Liability

8.1.1 IN NO EVENT, WHETHER IN TORT, CONTRACT, OR OTHERWISE, SHALL SEDARA, PARTNERS, OR SUPPLIERS BE LIABLE TO CUSTOMER OR ANY THIRD PARTIES UNDER THIS AGREEMENT FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, COSTS, LOSSES OR EXPENSE, (INCLUDING BUT NOT LIMITED TO LOST PROFITS, LOSS OR INTERRUPTION OF USE, LOSS OF DATA, DAMAGE TO NETWORKS, EQUIPMENT, OR HARDWARE, OR THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR TECHNOLOGY), OR ANY AMOUNTS IN EXCESS OF THE ORIGINAL PURCHASE PRICE OF THE SOFTWARE OR SERVICE. THE FOREGOING LIMITATIONS SHALL APPLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND DO NOT APPLY TO BODILY INJURY TO A PERSON.

8.1.2 SEDARA'S AGGREGATE LIABILITY (WHETHER IN CONTRACT, TORT OR OTHERWISE) FOR ALL CLAIMS OF LIABILITY ARISING OUT OF, OR IN CONNECTION WITH ANY SERVICE PROVIDED PURSUANT TO THIS AGREEMENT SHALL NOT EXCEED: (A) THE AMOUTS PAID BY CUSTOMER FOR THE SPECIFIC SERVICE(S) GIVING RISE TO SUCH CLAIM DURING THE PRIOR TWELVE (12) MONTH PERIOD WITH RESPECT TO THE SERVICES; AND (B) THE AMOUNT OF THE STATEMENT OF WORK THAT IS THE SOURCE OF SUCH LIABILITY, WITH RESPECT TO THE CONSULTING OR PENETRATION TESTING SERVICES.

EACH PARTY ACKNOWLEDGES THAT THESE LIMITATIONS APPLY EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR THE REMEDIES FAIL OF THEIR ESSENTIAL PURPOSE AND THAT, WITHOUT THESE LIMITATIONS, THE FEE FOR THE SERVICES PROVIDED HEREUNDER WOULD BE HIGHER.

8.1.3 The foregoing limitations, exclusions and disclaimers shall apply, regardless of whether the claim for such damages is based in contract, warranty, strict liability, negligence, and tort or otherwise. Insofar as applicable law prohibits any limitations herein, the parties agree that such limitations will be automatically modified, but only to the extent so as to make the limitation permitted to the fullest extent possible under such law. The parties agree that the limitations on liabilities set forth herein are agreed allocations of risk constituting in part the consideration for Sedara's sale of services and/or Products to Customer, and such limitations will apply notwithstanding the failure of essential purpose of any limited remedy and even if a party has been advised of the possibility of such liabilities.

8.1.4 Certain Consulting Services that Sedara performs for its customers follow a defined methodology, rather than being driven by a specific end result or deliverable. Due to this inherent property of these certain Consulting Services, Sedara cannot guarantee the outcome of its testing, assessment, forensics, or remediation methods as all such methods have reliability limitations including, but not limited to, (i) results produced differing from initial customer expectations, (ii) missing certain compliance gaps and (iii) missing certain security gaps. Sedara cannot guarantee that a weakness, noncompliance issue or vulnerability will be discovered if evidence of such is not encountered during the performance of the contracted engagement. Sedara uses a sampling methodology which attempts to reduce the cost to its customers while minimizing the impact to the accuracy and reliability of the results. Customer acknowledges and accepts that limitations and inherent risks exist from approaches used by Sedara to deliver the Consulting Services.

This section shall survive any expiration or termination of the Agreement.

# 9. Indemnification:

Sedara shall indemnify and hold harmless Customer and its officers, employees, agents and representatives and defend any action brought against same with respect to any third-party claim, demand or cause of action, including reasonable attorney's fees, to the extent that it is based upon a claim that the Software infringes or violates any United States patents, copyrights, trade secrets, or other proprietary rights of a third-party. Customer may, at its own expense, assist in such defense if it so chooses, provided that Sedara shall control such defense and all negotiations relating to the settlement of any such claim. Customer shall promptly provide Sedara with written notice of any claim which Customer believes falls within the scope of this Section 9. In the event that the Software or any portion thereof is held to constitute an infringement and its use is enjoined, Sedara may, at its sole option and expense, (i) modify the infringing Software so that it is non-infringing, (ii) procure for Customer the right to continue to use the infringing Software, or (iii) replace said Software with suitable, non-infringing software. Notwithstanding the foregoing, Sedara will have no obligation for any claims to the extent such claims result from (i) modifications or alterations of the Software made by or for Customer or any other party that were not provided by Sedara or authorized by Sedara in writing; (ii) use outside the scope of the license granted hereunder, (iii) use of a superseded or previous version of the Software if infringement would have been avoided by the use of a newer version which Sedara made available to Customer, or (iv) use of the Software in combination with any other software, hardware or products not supplied by Sedara. This indemnity obligation is subject to the limitation of liability and does not apply to any open-source components of the Software.

# ERIE COUNTY WATER AUTHORITY

## Cybersecurity Risk & Vulnerability Assessment

Erie County
Water Authority

RFP#
202100116

Date Due
June 11, 2021

Submitted by
Edvard Lauman
EdvardL@aesi-inc.com

AESI

1990 Lakeside Parkway
Suite 250
Tucker, Georgia
USA 30084
P · 770.870.1630
F · 770.870.1629

775 Main Street E
Suite 1B
Milton, Ontario
Canada L9T 3Z3
P · 905.875.2075
F · 905.875.2062

www.aesi-inc.com

aesi@aesi-inc.com

PRIVATE AND CONFIDENTIAL

AESI

Cybersecurity Risk & Vulnerability Assessment

# ERIE COUNTY WATER AUTHORITY

## Cybersecurity Risk & Vulnerability Assessment

RFP # 202100116

Author: ______________________ Date: June 11, 2021
Edvard Lauman, P. Eng., GCIA
Vice President, Cyber Security & Operational Technology

Authorized By: J Charlebois Date: June 11, 2021
Joel Charlebois, P.Eng.
Vice President, Regulatory Compliance

Third Party Disclaimer
The content of this document is not intended for the use of, nor is it intended to be relied upon by any person, firm or corporation, other than the client and AESI. AESI denies any liability whatsoever to other parties for damages or injury suffered by such third party arising from use of this document by them, without the express prior written authority of AESI and our client. This document is subject to further restrictions imposed by the contract between the client and AESI and these parties' permission must be sought regarding this document in all other circumstances.

Liability
The total aggregate liability of AESI resulting from any culpability with respect to the performance of the contracted consulting services and compliance activities associated with this project shall be limited to the total fee paid to AESI for project work resulting from the acceptance of this proposal. Should the Client be subject to any findings or claims of regulatory non-compliance, including associated sanctions or penalties, it is the Client's sole responsibility to address any such findings or claims.

Confidential
This document is for the confidential use of the addressee only. Any retention, reproduction, distribution or disclosure to parties other than the addressee is prohibited without the express written authorization of AESI.

Force Majeure
Neither party shall be in default of the Agreement where the failure to perform an obligation is due wholly to a cause beyond its reasonable control. The party experiencing such a difficulty shall promptly notify the other of its inability to perform its obligation. The parties agree to negotiate in good faith an extension of time for performing the obligation, avenues to resolve the situation and resolution of any financial impacts. Both parties shall mitigate their losses.

# TABLE OF CONTENTS

1. Company Introduction ........ 1
2. Company Experience ........ 2
3. Key Project Personnel ........ 7
3.1. Project Team ........ 7
3.2. Organizational Structure ........ 9
3.3. Cross Reference Table ........ 10
4. Project Understanding ........ 10
4.1. Vulnerability Assessment and Penetration Testing ........ 10
4.2. Document Review ........ 11
4.3. Reporting ........ 11
4.4. Optional Services ........ 11
5. Management Approach ........ 11
5.1. Stage 1 – Pre-On-Site Activities ........ 11
5.1.1. Rules of Engagement (ROE) ........ 12
5.2. Stage 2 – Remote & On-Site Discovery (Assessment Phase) ........ 12
5.3. Stage 3 – Risk Assessment & GAP Analysis ........ 13
5.4. Stage 4 – Report and Recommendations ........ 14
6. Methodology ........ 14
6.1. Vulnerability Assessment (VA) Testing Methodology ........ 14
6.1.1. Overview ........ 14
6.1.2. Planning ........ 15
6.1.3. Discovery ........ 15
6.1.4. Vulnerability Analysis ........ 16
6.1.5. Exploit Vulnerabilities ........ 17
6.2. Cyber Vulnerability Assessment (CVA) Methodology ........ 18
6.3. Our Vulnerability Assessment and Infrastructure Evaluation Process ........ 19
6.4. Wireless Network Testing Approach and Methodology ........ 20
7. Deliverables ........ 21
8. Schedule and Milestones ........ 21
9. Project Contingency ........ 22
9.1. COVID-19 Business Continuity ........ 22

9.1.1. Travel Restrictions ..... 22
9.1.2. Remote Work ..... 23
10. Assumptions ..... 23
11. Cost for Services ..... 24
11.1. Total Fixed Fee ..... 24
11.2. Milestone Payment Schedule ..... 24
11.3. Hourly Rates ..... 24
11.1. Out of Scope ..... 25
1. PART 1 ..... 26
2. PART 2 ..... 26
3. PART 3 ..... 30

## Appendix Listing

Appendix A Response Requirement Answers
Appendix B Insurance Coverage
Appendix C Standard Contract and Non-Disclosure Agreement

**Please see Appendix A for responses only based on the "Response Requirement" section of the RFP.**

# 1. Company Introduction

**Established in 1997**, AESI-US, Inc. (AESI) is a privately owned, consulting and engineering firm **supporting the critical infrastructure community, including the government sector, electricity, water, gas, public safety, and other essential services**. We provide critical infrastructure management and engineering, compliance management services, production automation, cyber security, smart grid, and risk management services to government sector, public power utilities, co-ops, IOUs and IPPs. AESI's clients benefit from access to industry leading expertise, reliability improvements and lower costs.

Building on the bench strength of direct experience and a practical consulting background, we have established a solid reputation with our non-traditional blend of both engineers, and technical staff. Our **in-house, highly knowledgeable professionals** have extensive, real-life IT and Operational Technology (OT) experience that feeds a healthy understanding of true operations, so the fundamentals of what is being protected are thought of—from the individual cyber asset to the system as a whole. The nature and importance of the information that must be protected is well understood by the team selected for this engagement.

We have a solid history of helping electric power and water utilities develop and implement a **synergistic cyber security program -** from the fundamentals of assessing hardware and systems, to foundations of training/educating the people that use those systems daily, and up through to reporting as an element of risk management.

AESI is best known for providing regulatory and Cyber Security Services to electrical power and water facilities across North America. Clients include water utilities of all sizes from small municipals to California Water, small, medium, and large public power utilities, Joint Action Agencies, and co-ops, as well as investor-owned utilities and independent power producers.

AESI's foundation for the requested services are based in providing cyber security to water/wastewater and power utilities—whose operating systems support critical infrastructure in a live 24/7 environment—for best practices and compliance. AESI's approach for Vulnerability Assessments (VAs) and Penetration Testing incorporates multiple individual assessments that contribute to the overall assessment and analysis for a holistic assessment. AESI uses the **NIST standards** such as SP800-53r4 Cybersecurity Framework, **AWWA Security Guidance for the Water Sector**, and other industry standards, such as the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards and the DHS Sector-Specific Plans to perform its analysis and assessments.

Our methodology is proven and incorporates rigor for diligence and intelligence for insight. Our reports are designed to be easy to read and easy to understand, and more importantly, with recommendations that are practical, implementable, and sustainable. This comes from the experience of having **completed more than 200 security assessments** for utilities in North America.

Best practices and recommendations for the improvements sought by the Eric County Water Authority (ECWA) will be measured through qualitative and quantitative analysis of peer organizations and experience-based input of AESI professionals.

Some companies are project based - at AESI, we like to think we are client based. There is a fundamental difference that drives this perspective, and it shows in our client relationships, the diligence in project management, and more specifically in our deliverables—where we provide long term roadmaps that **go beyond remediation for enhancements and future endeavors**.

Our detailed report will not stop at the findings that result from these tasks—we provide our clients **the full value of all our knowledge** with a detailed analysis of the findings to develop a prioritized and justifiable roadmap to attain an appropriate level of security, while balancing security with optimal operations.

To ensure projects are delivered to schedule and budget, we employ regimented project management practices. Risk is inherent; having completed multiple similar projects, we know where the pitfalls can lie and are prepared with mitigation strategies to address any issues that could arise. To ensure quality is received; we are  diligent with our quality control/quality assurance processes.

This proposal will demonstrate that AESI has the right combination of engineering resources to meet the various and demanding project requirements. Our proposal is based on three main strengths:

- A strong team of professionals with extensive direct knowledge of all aspects of critical and non-critical applications and telecommunications systems in addition to asset and cybersecurity protocols
- Proven experience on projects with many critical infrastructure clients
- Cost effectiveness, plus a track record of delivering high quality services and excellent value to electric utilities

Within our scope of work, we refer to the work associated with penetration testing as a Vulnerability Assessment (VA), of which involves both testing and infrastructure evaluations.

Any technical questions for this proposal should be directed to Edvard Lauman at 770-870-1630 ext. 235; commercial questions should be directed to Joel Charlebois at JoelC@aesi-inc.com or 770-870-1630 ext. 236.

## 2. Company Experience

Vulnerability Assessments (VAs) are an extension of AESI's portfolio of services for NERC CIP Compliance and cyber security risk assessments. AESI has performed many VAs for water/waste water utilities, electrical transmission, generation, operations, and distribution utilities, and mass transit. AESI has served water/wastewater and electrical utilities for more than 20 years, and is very aware of the cyber security requirements, capabilities and constraints of utilities of various sizes from small cooperatives and municipals to large vertically integrated utilities spanning multiple US state or entire Canadian provinces. This knowledge ensures that AESI's recommendations are actionable, effective, and sized/priced appropriately for each client.

We have selected the following projects to demonstrate our experience in conducting VAs and other Cyber Security Vulnerability Assessments (CVAs) for clients similar to ECWA.

| | |
|---|---|
| **Lakeland Electric (City of Lakeland)** | |
| Industry | Municipal Electric Utility |
| Project Title | Cyber Vulnerability Assessments (CVAs) |
| Project Duration/Date | 2014 to 2019 |
| Client Objective(s) | Ensure effective security measures are implemented throughout the organization to properly protect assets from security threats, vulnerabilities, and exposures. |
| Scope of Work | Conduct CVAs to evaluate effectiveness of security controls that protect in-scope BES assets in accordance with current applicable NERC CIP guidance. Involved network vulnerability and penetration testing to identify and evaluate weaknesses of targeted systems using automated and manual testing tools and methodologies. |
| AESI's Role | AESI carried out all assessment tasks (information gathering, discovery, analysis, reporting). Upon completion of the assessment, AESI delivered a report detailing discovered exploits, information on likelihood of the exploit being triggered, and risks of potential downtime. All exploits were documented and verified throughout the assessment. All reports (e.g., interim reports) included a description of the exploits, documentation of testing activities, and remediation recommendations. |
| AESI's Project Team | Ivan Wong – Project Manager & Cyber Security SME |
| Client Reference | Larry Watt, Larry.Watt@lakelandelectric.com |
| **EPCOR Utilities** | |
| Industry | Electric Distribution; Water & Wastewater |
| Project Title | Active Vulnerability Assessment (VA) & Penetration Test |
| Project Duration/Date | 2018 |
| Client Objective(s) | Assess the cyber security posture of a subset of EPCOR's SCADA systems located in Canada and U.S. |
| Scope of Work | Perform a VA of the SCADA system at EPCOR's control center for their electricity transmission and distribution network in Edmonton, Alberta, and a VA of SCADA systems for its water and wastewater facilities in Phoenix, Arizona, U.S. |
| AESI's Role | AESI was tasked with completing the following:<br>Vulnerability Scanning:<br>• Identification of active devices<br>• Network Discovery, Ports and Services Identification, and Vulnerability Scanning<br>• Identification of vulnerabilities of SCADA systems including components such as historians, engineering and operations workstations. |

| | |
|---|---|
| | • Identification of outdated software versions, missing patches, and misconfigurations<br>• Identification of vulnerabilities associated with the services running on enabled logical network accessible ports.<br>• Review of configuration vulnerabilities related to firewalls, routers and switches protecting SCADA systems.<br>• Identification and review of wireless networks connected to the SCADA system, where applicable<br>Wireless Review:<br>• Identification and review of existing wireless networks within the specific locations where SCADA systems were located.<br>• Confirmation that the wireless networks were not used for SCADA / OT communications.<br>• Detect wireless signals and networks in the physical perimeter.<br>• Capture wireless traffic that specifically identifies the wireless local area networks (WLANs), wireless access points (WAPs), and wireless client devices within range of the wireless scanning tool.<br>• Analysis of wireless traffic to identify the attributes of the detected WLANs, WAPs, and wireless client devices, and of the wired networks to which they are connected.<br>Residual Risk Analysis:<br>• Review of network and security architecture of SCADA environments including, the implementation of IDS/IPS, Firewalls, etc.<br>• Review of processes and security tools related to logical and network access, patch management etc. applied to the SCADA environment.<br>• Review of related security policies, standards, and procedures |
| AESI's Project Team | Edvard Lauman – SCADA & OT SME & QA<br>Ivan Wong – VA Tester, Cyber Security SME & Support<br>James Chacko - VA Tester, Cyber Security SME & Support |
| Client Reference | Jean Masbang, IT Auditor; 780-412-4492; jmasbang@epcor.com |
| **Clay County Utility Authority (CCUA)** | |
| Industry | Water Utility |
| Project Title | SCADA System Security Assessment |
| Project Duration/Date | 2016 to 2017 |
| Client Objective(s) | Conduct a comprehensive SCADA System Security Assessment using a "blind scan" methodology for evaluation that would imitate an unknown attacker with limited or no knowledge of the existing SCADA system. |

| | |
|---|---|
| Scope of Work | External Network Penetration and Assessment and an Internal Network Penetration and Assessment. |
| AESI's Role | AESI was tasked with completing the following:<br>External Network Penetration and Assessment<br>• Public/External IP addresses of all endpoints<br>• Performance of reconnaissance operations to collect information that may be used in formulating an attack against the CCUA reclaimed water SCADA system.<br>• Evaluation of all public IP address endpoints for exposed security vulnerabilities<br>Internal Network Penetration and Assessment<br>• Internal IP address subnets<br>• Evaluation of all SCADA internal subnets for potential security vulnerabilities that may allow the SCADA network to be compromised.<br>AESI's final report captured the process and methodology, results of the assessments and tests conducted, our assessment of the findings, identification of any cyber security issues and their risk profile, and a prioritized list of recommendations. |
| AESI's Project Team | Ivan Wong – Project Manager & Cyber Security SME |
| Client Reference | Allen Boatright, Chief Information Officer; 904-272-5999; aboatright@clayutility.org |
| **New Brunswick Power (NB Power)** | |
| Industry | Electric Utility |
| Project Title | Cyber Vulnerability Assessment (CVA) |
| Project Duration/Date | 2014 to Present |
| Client Objective(s) | Evaluate the security posture of NB Power's Electronic Security Perimeters (ESP) and the cyber assets within them, both at the control centers and the medium impact transmission sites. |
| Scope of Work | Annual CVA for NB Power's Primary and Backup Control Centres and six transmission sites. |
| AESI's Role | As part of NB Power's NERC CIP program support, AESI conducts annual Cyber Vulnerability Assessments on their Control Centres (primary and back-up) and substations.<br>AESI conducted CVAs per the NERC CIP standards in 2014 and 2015. With CIP v5, CVAs have changed from one calendar year to one every 15 months, as such; a CVA was not conducted in 2016 but was instead completed in 2017.<br>The difference between the two CVAs (2014 and 2015) was in the substation configuration. In 2014, the substation CVAs were based on scanning of networking equipment as most of the IEDs were serial |

| | |
|---|---|
| | based. In 2015, the second year the substations were upgraded to use the IEC 61850 protocol and many of the devices were now connected via IP. AESI adjusted our scanning methodology to be able to scan IEDs that were in production at the substations. |
| AESI's Project Team | Edvard Lauman – Project Manager<br>Ivan Wong – VA Tester, Cyber Security SME & Support |
| Client Reference | Luther Eroh, IT Professional Digital Technology; 506-458-4622; Luther.Eroh@nbpower.com |
| **City of Tallahassee** | |
| Industry | Municipal Electric Utility |
| Project Title | Paper Cyber Vulnerability Assessment (CVA) |
| Project Duration/Date | 2018 |
| Client Objective(s) | To ensure that all electronic Cyber Assets (CAs) were secure via user account management, equipment configuration, password management, and secure networking policies to ensure compliance with NERC CIP standards. |
| Scope of Work | Conduct a NERC CIP Paper-based CVA of the City of Tallahassee's NERC CIP information network and control systems. |
| AESI's Role | AESI's CVA was conducted in accordance with NIST SP 800-115, and within the criteria established in ISO 27001:2005, Sandia National Labs Center for Control System Security (C2S2) Guide to CIP Cyber Vulnerability Assessment, and other applicable standards.<br>AESI prepared a concise report that captured the Cyber Vulnerability Assessment (process and methodology), vulnerability analysis and prioritized list of recommendations (proposed remediation or mitigation activities).<br>Tasks included:<br>• Analysis that maintained data integrity<br>• Physical inspection that verified that the network map accurately portrayed the network configuration.<br>• Network and system configuration analysis<br>• Review of network perimeter and access points<br>• Review of user account auditing and recommendation of strategies<br>• Verification of vulnerabilities and documenting the discovery of new potential vulnerabilities.<br>• Executive briefing with high-level findings of the CVA and recommended mitigations |
| AESI's Project Team | Edvard Lauman – Project Manager<br>Ivan Wong – VA Tester, Cyber Security SME & Support |

| | |
|---|---|
| Client Reference | Karen Webb, AGM - Electric System Compliance; 850-891-3125; Karen.Webb@talgov.com |

# 3. Key Project Personnel

Our dedication to client satisfaction is more than just deliverables and adhering to a project schedule; it is about quality and relationships. It is based on our commitment to a high standard of customer service, professionalism, and mutual trust that our clients reward AESI with repeat engagements for new and recurring services.

- 30+ years providing consulting services to over 500 utilities.
- Credible professional staff with extensive cyber security experience
- Selected by Hometown Connections (subsidiary of the American Public Power Association) as the public power partner for cyber security and IT / OT services
- Our value proposition is knowledge transfer.
- Staff have relevant experience including:
  - Former SCADA and Security Operations Managers, Operators, Linesmen, Compliance Managers, Planners
  - In-house capabilities for Critical Infrastructure Protection standards
  - Staff with Auditor Training and/or former Auditors
  - Regional Standards Committee Participation
  - Staff & Associates located across North America
  - Multi-Disciplined Staff Knowledgeable in Multiple Practice Areas

We confirm that the proposed personnel named in this document are available, and fully committed to this engagement, whenever and wherever required. Although not expected, any changes to our key personnel members will be approved by ECWA, and another equally experienced team member will be put forward.

## 3.1. Project Team

### Project Director: Edvard Lauman, P. Eng., GCIA

Edvard (Ed) has more than 17 years of experience working as a Cyber Security Specialist, including hands-on operation and management of SCADA systems, security and network operations for a large electric transmission and distribution utility. He is a system integration expert, specializing in SCADA, Data Historians, Distributed Control Systems, related network, and security infrastructure, as well as custom software development. His experience incorporates requirements and technology assessments with the design and development of IT/Control solutions, as well as identifying and resolving network, telecommunications, and application-level issues.

Ed will act as the Project Director and will have the overall responsibility for the quality and timeliness of our services. He will monitor the overall progress and communicate with our project team to ensure satisfaction with our process and deliverables.

Ed will provide support as the SCADA/OT SME for system administration, networks, physical and cyber security, system configuration and operational technology. Ed is located in Edmonton, Canada.

*Relevant Experience*

- Conducted multiple Cyber Vulnerability Testing for distribution, transmission and generation power utilities
- Developed cyber security policies and procedures for several distribution utilities, including a utility implementing a 16-million-dollar smart grid project encompassing all aspects of their operation
- Designed and implemented cyber security architectures for the SCADA portion for many utilities' networks

## Project Manager, Cyber Security SME & Tester: Ivan Wong, CCNA

Ivan is a goal-oriented and collaborative IT professional with proven experience analysing and troubleshooting large corporate networks with more than 10 years of experience. He has conducted multiple cyber security vulnerability assessments, including paper assessments, for power generation utilities, distribution utilities, water treatment plants, and corporate environments through preliminary document review, on-site vulnerability scan, analysis, and reporting while meeting NERC CIP v3 and v5 requirements. His strong technical knowledge, coupled with the ability to quickly learn new systems, allows him to provide practical solutions. He is comfortable supporting both technical and non-technical audiences.

Ivan will be the Project Manager and will assist Edvard Lauman, the Project Director, with the overall responsibility for the quality and timeliness of our services. He will monitor the overall progress and communicate with our project team to ensure satisfaction with our process and deliverables. In addition, Ivan will be the Cyber Security SME and Tester. Ivan will be engaged in all phases of the project through completion with active participation in the assessment and testing phases. He will assist with analysis and documentation development. Ivan is located in Toronto, Canada.

*Relevant Experience*

- Conducted multiple cyber security vulnerability assessments for power generation utilities, distribution utilities, water treatment plants, and corporate environments through preliminary document review, on-site vulnerability scans, and analysis
- Implemented cybersecurity tools, such as firewalls, access controls, SIEM, and network monitoring tools at client sites to meet CIP requirements
- Designed and implemented firewalls that met NERC CIP v3 and v5 requirements for power generation and distribution utilities
- Provided network services to power generation and distribution utilities including configuration review, network troubleshooting, network design, network implementation, access rules review, and network diagrams creation
- Designed and implemented firewalls that met NERC CIP v3 and v5 requirements for power generation and distribution utilities
- Provided network services to power generation and distribution utilities including configuration review, network troubleshooting, network design, network implementation, access rules review, and network diagrams creation

## Cyber Security SME & QA/QC: James Chacko, CISSP, CISA, ITIL, CEH, CHFI

James Chacko is a Senior Security Specialist with over 11 years of progressive experience with emphasis on projects related to infrastructure, systems, and application deployment. He has proven experience in operations and technical support, systems/network administration, business technical analysis and project management. His experience comprises of security policy and procedures for networking (LAN/WAN), software evaluations, network security assessments and recommendations for improvements.

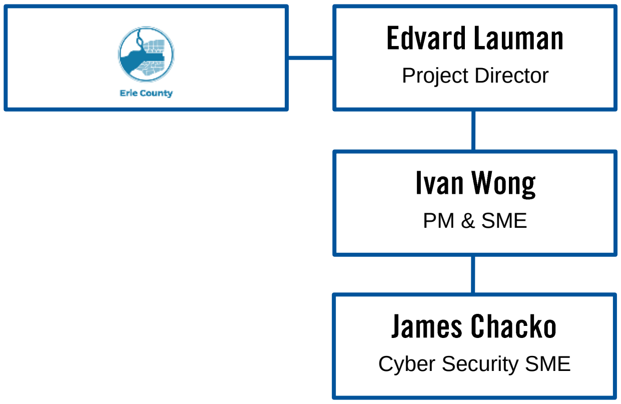
James will provide support as an SME for cyber security standards, baselines, policies, procedures, and guidelines. James will perform most of the CVA and penetration testing related work on external/internet facing nodes. James is located in Edmonton, Canada.

*Relevant Experience*

- Content development and technical presenter for USF OEB Cyber Security Framework training
- Developing IT/OT cyber security training for American Public Power Association (APPA)
- Part of a team developing an American Public Power Association (APPA) survey to collect data and evaluate "data-in-motion"
- Developed and delivered training for a complete backbone network structure for the building, the data center, security and access control systems, in suite technology, and back office systems
- Served as the SME for the PCI data security standards compliance requirements for a hospitality reservation, POS and back office system. Scheduled internal audits for the payment systems to ensure that regulatory controls were in place and applied.
- Maintained audit reports and served as the point of contact during the external audits
- Provided comprehensive cyber security risk assessment of the data warehouse and supervised migration of Back-Office application – Sage ERP 300 v2012 to Sage ERP 300 v2017, from an on-site server to a hosted solution

## 3.2. Organizational Structure

As Project Director, Edvard Lauman will have the overall responsibility for implementing and facilitating all aspects of the project. Ed will be the single point of contact with ECWA. All resources engaged will report to Ed.



## 3.3. Cross Reference Table

| Project Resource | Reference Project | Role of Resource |
|---|---|---|
| Edvard Lauman | EPCOR Utilities | Project Manager |
| | NB Power | Project Manager |
| | City of Tallahassee | SCADA/OT SME and QA |
| Ivan Wong | City of Lakeland | Cyber Security SME |
| | EPCOR Utilities | VA Tester and Cyber Security SME & Support |
| | Clay County Utility Authority | Project Manager |
| | NB Power | VA Tester and Cyber Security SME & Support |
| | City of Tallahassee | VA Tester and Cyber Security SME & Support |
| James Chacko | EPCOR Utilities | VA Tester and Cyber Security SME & Support |

# 4. Project Understanding

The scope of this engagement involves the following:

## 4.1. Vulnerability Assessment and Penetration Testing

AESI will perform a vulnerability assessment on EWCA's infrastructure and penetration testing on EWCA's internet facing infrastructure, which will include the following:

- Test for susceptibility to Advanced Persistent Threats (APTs) such as viruses, malware, Trojan horses, botnets, and other targeted attack exploits.
- Evaluate the ECWA's current threat posture including antivirus and Intrusion Detection and Prevention (IDP) capabilities.
- Evaluate ECWA's planned changes and improvements to the threat surface and assist identifying and addressing security concerns.
- Review the ECWA's current Supervisory Control and Data Acquisition (SCADA) water systems for security vulnerabilities.
- Review wireless network system components for security vulnerabilities, validating system-specific operating systems and firmware versions for known exploits and recommend upgrades, updates, and mitigations.
- Review current system-specific operating systems and firmware versions for known exploits and recommend upgrades, updates, and mitigations. This includes firewalls, switches and routers, Microsoft Active Directory, email and file servers, web servers, wireless routers, WAN, VPN, VoIP, and CCTV systems.
- Assess VoIP network system components for security vulnerabilities, validating system-specific operating system and firmware versions and reviewing for known exploits.

- Execute and review internal network vulnerability scans and external vulnerability and penetration scans and make recommendations to reduce the threat attack surface.

### 4.2. Document Review

- Review of current state of the ECWA's information technology security by reviewing existing IT policies and procedures and make recommendations for changes and/or additional policy and procedure development.

### 4.3. Reporting

Based on the assessment and review, AESI will:

- Provide findings and recommendations based on methodologies from National Institute for Standards and Technology (NIST), including NIST Cybersecurity Framework, and NIST SP 800-115, and related documents, such as "Framework for Improving Critical Infrastructure Cybersecurity".
- Development mitigation plans based on the identified cybersecurity vulnerabilities and gaps from the vulnerability assessment and penetration tests.
- Development of a prioritized road map of activities to enhance the EWCA's future Cybersecurity position.

### 4.4. Optional Services

EWCA may wish to include the following optional services:

- Physical Security Review – Review the current physical security process and technology in place for a sample number of sites. Identify gaps and provide recommendations to mitigate the vulnerabilities.
- Social Engineering – AESI will perform a phishing campaign on ECWA's 300 users and provide recommendations based on the results.

## 5. Management Approach

AESI performs VAs based on the methods detailed in NIST SP 800-115, Technical Guide to Information Security Testing and Assessment. AESI will determine the means and processes that an attacker would use to breach critical infrastructure systems and compromise assets.

Vulnerability testing will involve experienced security professionals who will examine the weaknesses of targeted systems. AESI will report all possible exploits and provide information such as risk of downtime to help the client determine if a test or exploit should be attempted. AESI will ensure that all exploits are documented and verified throughout the assessment. All reports (i.e., interim reports) will include a description of the exploit attempts and the successes or failures, documentation of testing activities, and remediation recommendations.

Our four-staged approach is detailed below.

### 5.1. Stage 1 – Pre-On-Site Activities

This stage is focused on the planning and schedule logistics prior to the start of the on-site IT/cyber security assessment and vulnerability test activities. This will include the following activities in collaboration with staff.

1. **Kickoff Meeting** – Schedule coordination and planning meeting with identified project participants. Obtain agreement on time and execution plans, monitoring requirements and exit plans for scheduled or forced terminations of the testing and vulnerability scanning process.
2. **Documentation Review** – Obtain and review documentation outlining security management practices, network diagrams, device configurations, IT security related processes and procedures.
3. **Personnel Interviews** – Obtain a list of key individuals from including 3rd parties who can provide the insight into the organization's security processes, technical aspects of network structure and configurations.

### 5.1.1. Rules of Engagement (ROE)

The planning stage of the VA will include regular communication with key points of contact. The testing plan will include:

- Contact information and procedures for all phases
- Type and number of systems to be tested (e.g., servers, workstations, mobile devices)
- Rules of engagement

For penetration testing, AESI develops a rules of engagement document that governs how the testing will be conducted and any exception management that may be required.

The rules of engagement contain critical information about the scope of the project, key contacts, and incident response procedures:

- Introduction
  - Purpose
  - Scope of Testing
  - Assumptions and Limitations
  - Potential Risks
- Logistics
  - Personnel assigned to the project
  - Testing schedule
  - Test site or location
  - Test equipment, if any
- Communication Strategy
  - General Communication Procedures
- Target System(s)/Network(s)
- Reporting Procedures
- Acknowledgment Page

## 5.2. Stage 2 – Remote & On-Site Discovery (Assessment Phase)

Stage 2 focuses on evaluating the internal cyber security practices and processes pertaining to cyber security and conducting the Vulnerability Assessment and Infrastructure Evaluation.

Key activities for Stage 2 include the following activities:

1. Conduct interviews and discussions with key staff to assess the governance pertaining to the practices/processes for the management of the cyber security services.

2. Perform Vulnerability Assessment and Infrastructure Evaluation – We use non-intrusive tools and methods in conducting the vulnerability scans on operating IT environments. We will also explore options on first conducting vulnerability scanning on some assets in a test environment or during a scheduled outage or maintenance window prior to scanning live/operating environments.
3. AESI will explore these options with technical and operations staff and agree on the approach and methodology.

A QA/Development System may be used as a target of penetration testing and vulnerability scan instead of the live production systems if requested by ECWA to minimize operational risk. This type of review is effective if the QA/Development systems is representative of the production systems and has identical configuration, connectivity, access controls, patch levels, etc. For more details on each of the following activities, refer to the Methodology section.

- **Vulnerability Assessment** – Vulnerability test and vulnerability scan activities will be conducted to gather information regarding external hosts owned by ECWA. Vulnerability scans will be performed to determine if any vulnerabilities are present and whether it can be exploited. Attempts will be made to gain access to external internal facing devices and internal LAN.
- **Infrastructure Evaluation** – Identify and evaluation security controls used for the following items: Applications, Web Applications, Client-side data, email spam filter, Firewall, VPN, VoIP.
- **Wireless Scanning Evaluation** – Wireless scanning tools will be used to determine if any wireless signals or networks exist within the physical perimeter of the building. The results of the scans will be analyzed to determine if any of the discovered wireless signals, devices, and/or networks belong to unauthorized systems. AESI will also capture the wireless security settings and identify any known vulnerabilities.
- **Physical Security Evaluation (Optional)** – A physical inspection of the physical security perimeter to ensure that critical systems are securely protected.
- **Social Engineering Evaluation (Optional)** – Social engineering using various channels attempting to collect data such as usernames, passwords, SNMP strings, IP addresses, etc. Data collected during the social engineering assessments may be used during the exploitation stage of the penetration tests, validating that the information obtained was accurate and would cause a security risk.

## 5.3. Stage 3 – Risk Assessment & GAP Analysis

Stage 3 will focus on AESI performing the analysis on the results from the vulnerability scanning, and the governance aspects of the cyber security management and practices. The risk assessment will utilize the raw results of the scans, combined with the technical, administrative, and procedural safeguards that are in place, to determine the residual risks posed by the discovered vulnerabilities. AESI will also propose additional controls, which should further reduce cyber risks to acceptable levels.

AESI will identify the Cyber Assets, associated protection, and risks. This step will lead to the current state assessment and will include identification of gaps associated with people, process and technology as outlined in **the NIST Cybersecurity Framework**. The NIST Cybersecurity Framework is, in effect, the worldwide standard for cyber security for critical infrastructure. At a high level, the focus will be on the following:

- Cyber Asset Identification of IT systems and determining the risks associated with the assets
- Review of services provided by third parties
- Identification of protection technologies such firewalls, IDS/IPS, Access Management Solutions, encryption technologies
- Identification of cyber protection on network and communications infrastructure
- Identification of current vulnerability and patch management processes
- Identification of Security Event Monitoring and associated processes
- Identification of sensitive / confidential information
- Identification of organizational structure and governance supporting IT systems and Cyber security

## 5.4. Stage 4 – Report and Recommendations

Stage 4 will focus on AESI preparing the draft and final report with recommended solutions that cover what is required to address technical issues, establishment of required policies, and employee training opportunities. The report includes the data collected, the results of evaluations including deficiencies, and recommendations and associated best practices.

The reports also include the following specific items:

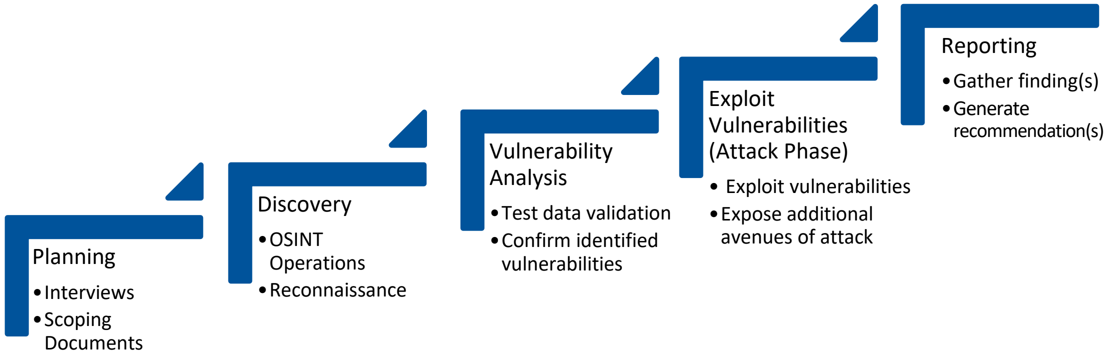
- Comprehensive Risk Assessment
- Gap Analysis
- Roadmap to Compliance

# 6. Methodology

## 6.1. Vulnerability Assessment (VA) Testing Methodology

### 6.1.1. Overview

Using honed defense and commercial hacking skills, the latest industry tools and unique, manually operated techniques, our technicians follow a disciplined process to ensure a complete understanding of your organization's requirements, that discovery is properly planned, attacks are done within the scope and expectation of the organization and a comprehensive report is delivered. The diagram below illustrates our five-stage process for penetration testing:



Planning
- Interviews
- Scoping Documents

Discovery
- OSINT Operations
- Reconnaissance

Vulnerability Analysis
- Test data validation
- Confirm identified vulnerabilities

Exploit Vulnerabilities (Attack Phase)
- Exploit vulnerabilities
- Expose additional avenues of attack

Reporting
- Gather finding(s)
- Generate recommendation(s)

Our testing approach is based on industry accepted ethical hacking best practices and standards and follows the penetration testing methods is based on NIST SP800-115, “Technical Guide to Information Security Testing and Assessment”, as well as the standards outlined by Open Web Application Security Project (OWASP) and the Penetration Test Execution Standards (PTES).

AESI performs penetration test assessments in a manner that is as non-intrusive as possible, while providing a thorough and accurate cyber security posture assessment, i.e., cyber security risk profile.

### 6.1.2. Planning

Our tests begin with a critical planning process that outlines the parameters of the test, allowing AESI to build rapport with stakeholders, and establish mutual expectations. Planning starts upon award of the contract and includes telephone interviews designed to determine the exact intent of your penetration testing needs. The goal is to properly scope out the requirements, as well as determine the Rules of Engagement (ROE). We will help you define each of the items listed above by forwarding a technical scoping questionnaire that serves as an invaluable part of planning and scoping process, which lists the details for the penetration test phases. The following items will be developed during this phase:

- Rules of engagement
- Type of test (white, grey, or black box penetration test)
- Client and AESI team contact information and procedures
- Types of systems to be tested (e.g., servers, workstations, mobile devices)

As part of our methodology, the planning process does not end at the start of the penetration test. Our personnel, including the project manager, will be in continuous contact with your security and management stakeholders to ensure transparency, answer questions and provide a continuous update on penetration test findings.

### 6.1.3. Discovery

AESI searches for and collects various type of information from public sources using Open-Source Intelligence (OSINT) collection methodologies honed from years of expertise in conducting cyber security assessments and intelligence collection against the nation’s threats. During this portion of the discovery process, information is collected using public web searches and passive collection. The intent is to collect information that outlines potential entry points into an organization by identifying publicly available information relating to your organization, your employees, vendors, and other key corporate attributes. This information will be used to perform reconnaissance against the vulnerability and exploitation stages. Information collected during this phase includes such critical information about the organization such as:

- Locations
- Relationships: landlords, vendors, clients, employees
- Products
- Documents, publications, public speaking events
- Organization
- Marketing/Public Relations/Communications
- Infrastructure and Assets
- Social Media and Internet Presence

Our team will perform extensive network host discovery, service discovery and enumeration. This will help identify both authorized and unauthorized (rogue) devices on any network. The following steps are typically performed during this phase:

- A thorough assessment of public routing policy, ISP announcements, and net block assignments for each public IP range
- Analysis of publicly registered information related to network address blocks, DNS service Start of Authority (SOA) records, and associated infrastructure for potential logical or physical weaknesses
- Analysis of email and internet domains, with the expressed intent of identifying email exchanges, web servers, and related domains, with the further intent of discovering related IP addresses
- Analysis of external systems using active scanning techniques – team members will use network mapping tools and network discovery techniques to verify organization-owned devices
- Segmentation checks – during the VA testing and in accordance with applicable standards, network segmentation controls will be scanned and tested for effectiveness in isolating sensitive and controlled data
- Evaluation of hosts identified in previous steps with the explicit intent of detecting services and protocols with associated vulnerabilities, if any
- Use tools to examine networks connected to the internet to report which hosts are visible, what operating systems are running, and the server's uptime
- Foot printing, i.e., interacting with the organization to determine weaknesses or obtain information that can be used during the attack phase
- Conduct a network survey that will also report on the type of packet filters/firewalls that are in use
- Perform port scanning to obtain information about closed and open ports that are running on the system or network. This provides information on:
    - Operating System Identification – staff will use active and passive Operation System identification automated tools to classify each network asset's operating system or platform. This process will also attempt to re-enumerate each asset, the hardware vendor, physical network address and hostname given to the device.
    - Open Port Identification – Port scanning and port knocking techniques will be used to determine enabled ports and services on all identified network hosts. Wherever possible, firewalls, routers and other network appliances will be scanned from each connected subnet to identify the services enabled on each network.
    - Device Identification – staff will use active and passive scans to determine what applications and hardware are used to host the various websites.
    - Back End Services Identification – staff will use various testing methods and scanning to determine back-end services that are in use with the websites such as SQL Servers, Proxy Servers, Load Balancers, etc.

The information collected will be analyzed to identify key vulnerabilities or potential points of access into your system such as DNS entries, IP ranges, email addresses, operating system (OS), email, ERP, and any 3rd party partnerships.

### 6.1.4. Vulnerability Analysis

During this stage, our team will conduct a vulnerability analysis of the flaws that were identified in the vulnerability assessment and discovery stages. This will determine which of those flaws in the tested systems and applications can be leveraged by a hacker or attacker. The vulnerabilities identified can range from insecure application design, weak passwords or service, and host misconfigurations. The process for vulnerability analysis will include efforts by the penetration tester to conduct **"active"** testing for vulnerabilities, **"passive"** collection efforts, and **"validation"** to ensure that identified vulnerabilities are exploitable.

During the **active** phase, the tester will interact with the devices and the IT stack directly. For this effort, those activities will be limited to the components utilized to segment external IP address spaces, such as firewalls and those components identified by the organization to be tested during the internal test. The tester will utilize both automated vulnerability assessment tools, such as port-based or service-based scanners, as well as web application scanners and brute force tools, when applicable. To ensure a comprehensive scan is conducted, the tester will also apply manual interaction with the vulnerabilities identified and use automated tools to validate them for the exploit stage.

The **passive** phase will include extending some of the passive collection accomplished in the discovery phase to identify vulnerabilities. During this phase, we will conduct actions such as metadata analysis of published documents and marketing collateral, as well as traffic monitoring to capture data to conduct off-line analysis.

During this **validation** phase, the tester will validate identified vulnerabilities to determine which are legitimate and can be used during the attack phase. The tester will manually validate the most critical vulnerabilities identified by automated tools—an important step when multiple tools are used. The tester will also categorize the vulnerabilities by group such as DNS, VPN, web, email, etc. This will allow the penetration tester to determine the attack avenues that will be utilized during the attack phase. Additional research on the identified vulnerability to be used in the attack phase will also be conducted. Using public research on vulnerability databases and archives, the use of exploit databases and databases of common misconfigurations will be used to build the attack plan based on the organization's requirements.

### 6.1.5. Exploit Vulnerabilities

With the agreement of the EWCA, AESI will attempt to exploit the vulnerabilities detected in the previous stage to determine if they expose an avenue that can be used to gain access to the application/device/site or to other systems. As mentioned in Stage Three, our penetration testers will take the findings of any previous vulnerability scans and attempt to exploit them, all the way up to the application layer. Using the identified vulnerabilities, AESI will determine the means and processes that an attacker would use to steal data, damage systems, deface websites, etc. VA testing will involve appropriate experienced security professionals who will examine the weaknesses of the targeted systems, with oversight provided by CISSP- and CEH- certified team leaders.

Prior to conducting this phase, AESI will present an *attack* plan to the organization to confirm the scope of the test, rules of engagement and the testing schedule and both the on- and off-limit IP addresses. The dates and times of the penetration testing will be at your discretion, but at a mutually agreeable time with AESI. If mission-critical networks are being tested, AESI recommends that all testing occur within a defined maintenance window to prevent disruption of business operations, and in a development versus a production environment, if available.

To conduct the test, the tester will use scripts and available exploitation frameworks to minimize the time of creating specific exploitation harnesses.

During the test, it is possible that the tester will exploit a vulnerability that could expose other avenues of attack or lead to administrative or “root” access or privilege escalation. Additionally, the new attack avenues created may allow AESI to “pivot” and exploit other systems which would increase their knowledge of the impact of that vulnerability and the security of your technology architecture. Prior to pursuing these additional vulnerabilities and/or their impact on the organization’s architecture, our testers will confirm with the assigned Point of Contact (POC) the vulnerability and the proposed plan to pursue that vulnerability—including the tools or software to be utilized and confirm authorization to continue to exploit that vulnerability.

Throughout the vulnerability scanning and testing, AESI will provide daily updates unless otherwise agreed to by the organization and AESI. Should any critical issues be encountered during the penetration test, AESI will alert the ECWA POC and technical staff immediately and provide mitigation recommendations as appropriate.

## 6.2. Cyber Vulnerability Assessment (CVA) Methodology

Our approach to conducting infrastructure evaluations includes a combination of vulnerability assessment and technology reviews while being non-intrusive to ECWA operations and providing a thorough and accurate cyber security posture assessment, i.e., cyber security risk profile. Our comprehensive reports and deliverables present a detailed description of the methodology and findings effectively illustrated with appropriate scorecards and dashboards to highlight key measures and findings. And we will recommend any required actions to remedy discovered cyber security issues, risks and vulnerabilities identified during the assessment.

AESI’s CVA methodology incorporates guidance published by leading standards organizations for the planning, operation, and protection of critical infrastructure. These policies seek to reduce vulnerabilities, minimize consequences, identify, and disrupt threats, and hasten response and recovery efforts related to critical infrastructure.

Our vulnerability assessment framework combines methods described in NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, and methods from the Sandia National Laboratory (SNL) Information Design Assurance Red Team (IDART™) methodology, which was initially developed to assess and protect the United States’ nuclear arsenal and is now adapted for cyber security. Members of our team are certified in the IDART method.

1. **Network and Service Scanning**: Identify networking and related services running on target systems.
2. **System Identification**: Identify the name and location of each system on the network, including the operating system and any services running on those assets.
3. **Port Mapping**: Identify ports open on each device.
4. **Operating System/Service Map**: Test operating system and services running on target systems.
5. **Default Configurations**: Check for default configurations on web servers, applications, and other systems, including default credentials and other services that appear to have not been reconfigured for the operating environment.
6. **Internet Mapping**: Enumerate network and asset relationships and exposure to the Internet, including DNS and host name (domain name) registration information.
7. **Open Shares**: Locate and identify shares open on systems, including administrative, hidden, and unauthorized shares.

8. **Server Probing**: Analyze the details of any relevant servers (e.g., domain controller, SQL) and attempt to gain privileged access.
9. **Banner Grabbing**: Acquire banners from any exposed services.
10. **Remote Administration Enumeration and Testing**: Examine remote administration services, such as, RDP, telnet and SSH.
11. **Known Vulnerability Analysis and Verification**: Check for well-known vulnerabilities (i.e., CVE) and misconfigurations (i.e., weak passwords).
12. **Pivot to Internal and Neighboring Systems**: Determine if a vulnerability or exploit allows a pivot to an internal network from an external system or neighboring systems in the internal network.
13. **Wireless Scanning**: Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System.

Report sections to be included and excluded will be identified in the Rules of Engagement (RoE), discussed later in this statement of work.

## 6.3. Our Vulnerability Assessment and Infrastructure Evaluation Process

| Assessment Phase | Step | Process |
|---|---|---|
| **Environment Assessment and Planning** | Information Gathering | Collect information about the environment and the Cyber Assets in scope. (Network Diagram, ESP/PSP Diagrams, Access Control and Management procedures, system configurations (i.e. appliances, email spam filters, VoIP servers, firewalls, switches, VPN concentrators, etc.), authorized ports/services list, password management procedures. |
| | Tools and Environments | Prepare assessment hardware, software, commands, and configurations |
| **Execution and Analysis (On-site)** | Reconnaissance | Review the provided network diagrams, configurations, and inventories |
| | | Identification of network ranges and access points |
| | | Identification of Active Hosts using<br>• a host discovery scanner<br>• manual inspections where it was not safe to scan |
| | Wireless Scanning | Use automated scanners to identify any wireless signals and networks |
| | Ports and Services | Use automated scanners or OS commands to collect the open and in use ports and their associated services |
| | Community Strings Enumeration | Use network scanners and automated configuration analyzers to collect and analyze the community strings |
| | Account Enumeration | Use credentialed scans to enumerate accounts or manual audit where it is not safe to perform automated scans |
| | Vulnerabilities Discovery | Use vulnerability scanner to discovery any vulnerabilities on assets |
| | Evaluating Account Parameters | Use automated network scanners to determine account histories |
| | Physical walk down | Review physical access controls and verify equipment on hand |

| Assessment Phase | Step | Process |
|---|---|---|
| **Analytics** | Firewall, VPN, VoIP, email spam filter, Configuration Review | Use parsing tools and manual review to discover vulnerabilities based on configurations Categorize vulnerabilities based on high, medium, low |
| | Account Validation | Compare discovered results to approved accounts list and report on any unauthorized accounts |
| | Ports and Services Validation | Compare discovered ports and services to approved ports and services list and report on any unauthorized ports and services |
| **Vulnerability Assessment Result Documentation** | Findings | Used the results of the VA to produce a final report and produce a remediation plan to fix found vulnerabilities |
| | Recommendations | |
| | Mitigation plan | |

## 6.4. Wireless Network Testing Approach and Methodology

AESI uses automated and comprehensive manual testing to identify all wireless network and business-logic related vulnerabilities. Performed from the perspective of an attacker who is within wireless range, AESI will evaluate the wireless network's security posture in the context of generally accepted network security best practices. During the wireless assessment, AESI will take a wireless footprint of the target environments to identify and verify all the access points identified in the Rules of Engagement (ROE). AESI will also determine the encryption types used across the wireless environment. Key targets will then be selected for verification and approval. Observed unencrypted network clear-text transmissions will be captured and re-assembled to identify user credentials and other sensitive information.

AESI may initiate several discoveries depending on the wireless environment. Weak protocols will be identified and documented for any affected networks. Tests may include man-in-the-middle mock attacks, brute force mock attacks, session hijacking, and mass de-authentication. If enterprise authentication is used, AESI will perform tests against the wireless clients to determine if the devices are properly configured.

If AESI successfully penetrates the wireless environment, an assessment will be performed on the network’s endpoints. Security checks via vulnerability scanning will be made to check for proper segmentation between corporate and guest wireless networks (if any) and the hard-wired network. If approved, AESI will progress into the network as vulnerabilities are identified and will identify exploitable critical exposures to determine the extent of the access that could be achieved by a legitimate attacker.

Testing will include:

- Wi-Fi Misconfiguration
- Legal Encryption
- Weak Encryption Keys
- Evil Twin Attacks
- Insecure EAP Types
- Wi-Fi Protected Setup (WPS) Vulnerabilities
- Man-In-the-Middle Attacks
- Access Point Impersonation

# 7. Deliverables

AESI's reports are custom created and tailored to your requirements. AESI analyzes the vulnerabilities to determine why they exist and what should be done to mitigate these vulnerabilities. We provide a prioritized action plan with estimated time to correct and mitigate the discovered issues.

What makes AESI different from many other vendors that perform vulnerability assessments is that we have worked across multiple critical infrastructure sectors for nearly four decades. We put that knowledge to work when we make our recommendations.

AESI will prepare a concise and easy to understand report that will capture the Infrastructure Vulnerability Testing (process and methodology), vulnerability analysis and prioritized list of recommendations (proposed remediation or mitigation activities).

Our deliverables will include:

- An Executive Summary
- A comprehensive Infrastructure Vulnerability Testing Report on the results of the penetration tests for each site
- A documented process of the penetration testing methodology performed
- A comprehensive/sound assessment of the findings and results of the penetration testing
- Details on the review of system configurations
- Findings on the review of policies and procedures such as (patching, password management, anti-virus/anti-malware, etc.)
- Identify the cyber security strengths
- Identify any cyber security vulnerabilities and their risk profile
- Mitigation plans which include prioritized list of recommendations, action plans and budgetary estimates, along with an assessment of resources and timelines required for the proposed remediation or mitigation activities
- A comprehensive report detailing the methodology, analysis and recommended remediation of vulnerabilities and exploitations found as a result of the penetration and vulnerability tests. The report will include recommended solutions that cover technical issues, establishment of policies, and employee training opportunities based on the collected data, identified deficiencies, AESI's recommendations and associated best practices.
- A report summarizing the findings and recommendations from reviewing ECWA's IT process and procedure documents.
- Estimated hours and/or cost to implement the recommendations

# 8. Schedule and Milestones

AESI anticipates the project will take approximately six weeks. Most of the work will be completed off-site. AESI will work with ECWA to develop a schedule that will meet ECWA's requirements and AESI's resources. The schedule will be determined based on the number of facilities to assess, location of the facilities, travel time between sites, facility size, number of elements to included, assets/devices to be assessed, and number of networks within any given facility.

Based on a typical schedule for a similar sized project, the anticipated schedule is outlined in the below table:

| Duration | Activity | Description |
|---|---|---|
| Three weeks prior to on-site visit | Pre-on-site activities, Kick-off Meeting | • Firm up logistics for client resources, site activities |
| Five Days | Publish WBS and schedule for onsite task | • Based on kickoff meeting, AESI will develop a work breakdown schedule to provide to EWCA |
| Five Days | On-site Penetration Testing and Vulnerability Assessment | • Conduct Internal Vulnerability Testing<br>• On-site Infrastructure and Risk Assessment evaluations |
| Two Days | Remote Penetration Testing | • Conduct external penetration testing |
| One Day | (Optional) Physical Security Review | • Onsite physical security review of sample set of location |
| Two Days | (Optional) Social Engineering Testing | • Perform phishing campaign for approximately 300 ECWA users. |
| Approximately four weeks after on-site work has been completed | Draft Report | • Prepare and issue draft report |
| Two weeks | Report uploaded to ShareFile for commenting | • ECWA provide comments on the report |
| Two days | Final report issued after review of comments provided | • Finalize and issue |

# 9. Project Contingency

## 9.1. COVID-19 Business Continuity

The health and safety of our employees and our clients continues to be our highest priority.

With reports of the Novel Coronavirus (COVID-19), we recognize the importance of pandemic preparedness. While pandemics are unpredictable in their timing and severity, there are a number of preventative measures we can and have taken to help protect the safety of our staff, clients, and stakeholders.

### 9.1.1. Travel Restrictions

AESI continues to closely monitor the impact of COVID-19 and the risk to the public by staying up to date with official information published by the Centers for Disease Control & Prevention (CDC). We have implemented temporary travel restrictions for our employees travelling internationally, which is currently identified as a travel health risk by the CDC.

Non-essential business travel has been suspended in order to protect the health and safety of our employees, clients, and the public. Reasonable exceptions to the project schedule and in-person engagements shall be made in accordance with the current COVID-19 pandemic and government regulations/restrictions that may impact our ability to perform meetings and presentations in-person. AESI will utilize alternative methods such as web and/or mobile conferencing, where possible, in substitution of on-site field work (i.e., data gathering, interviews, and in-person meetings and presentations). Where an alternative method to business travel is not available, employees are required to follow AESI's health and safety protocols, such as practicing hand hygiene and physical distancing, and wearing a mask or face covering when physical distancing cannot be maintained.

Additionally, any employee who has recently travelled internationally, or resides with someone who has recently travelled internationally, is not permitted to work at AESI's offices, or at our client workplaces, for a period of 14 days from the date of their return. These employees must be symptom-free before returning to AESI's offices or client workspaces. These employees will work remotely from their home, within the confines of confidentiality agreements, and provided their job function permits.

### 9.1.2. Remote Work

To prevent the spread of COVID-19, we have implemented remote work from home for all staff. AESI has a strong business continuity plan and infrastructure setup that has allowed us to seamlessly transition to a remote work environment early on with minimal to no impact to our ongoing projects and client expectations. It is our hope that project work will continue as planned. We will work with our clients to accommodate any disruptions as they arise.

Additionally, staff are prohibited from entering AESI's offices or client workplaces if they are experiencing symptoms of COVID-19 or have come into contact with someone with a probable or confirmed case of COVID-19.

AESI is committed to the safety and well-being of our clients and staff and is continuously monitoring government-official notices and will update these restrictions as appropriate.

It is AESI's expectation that our clients implement similar preventative measures. AESI will continue to take appropriate action as directed by government officials.

## 10. Assumptions

AESI will make every effort to conduct the engagement within the time frame and cost allotted, with the following assumptions:

1. ECWA will assign a point of contact (POC) to work with AESI throughout the engagement.
2. ECWA will make available all relevant materials to AESI, including, but not limited to, network and systems documentation, applicable prior assessment artifacts, and relevant information necessary to carry out the assessment.
3. ECWA will ensure that AESI has appropriate physical and electronic access to target systems and networks in scope.
4. AESI will notify ECWA of any possible risks to ECWA networks and systems that may result from any testing scheduled to be performed. AESI will require ECWA to approve of any testing of this nature in writing before testing will commence or resume.

# 11. Cost for Services

## 11.1. Total Fixed Fee

The cost for the Erie County Water Authority Cyber Security Risk and Vulnerability Assessment is **$47,000**, Fixed Fee inclusive of labor and expenses. Our quote does not include any applicable taxes. The optional social engineering service is an additional **$5,100** while the optional physical security review is an additional **$3,700**.

*Options for Project*

| Options | Total Fixed Price |
|---|---|
| **Option 1**: CVA + Pen Test + Document Review | $47,000 |
| **Option 2**: CVA + Pen Test + Document Review + Social Engineering | $52,100 |
| **Option 3**: CVA + Pen Test + Document Review + Physical Security Review | $50,700 |
| **Option 4**: CVA + Pen Test + Document Review + Social Engineering + Physical Security Review | $55,800 |

## 11.2. Milestone Payment Schedule

| | | Option 1 | Option 2 | Option 3 | Option 4 |
|---|---|---|---|---|---|
| Due Upon Project Award | 30% | $14,100 | $15,630 | $15,210 | $16,740 |
| Due Upon Completion of Onsite and Remote Work | 40% | $18,800 | $20,840 | $20,280 | $22,320 |
| Due Upon Delivery of Final Report | 30% | $14,100 | $15,630 | $15,210 | $16,740 |

## 11.3. Hourly Rates

The following table lists AESI standard hourly rates:

*Hourly Rates for 2020 & 2021*

| Staff | Hourly Rate * |
|---|---|
| Edvard Lauman | $280 |
| Ivan Wong | $220 |
| James Chacko | $205 |

* AESI adjusts its rates annually effective January 1

### 11.1. Out of Scope

Additional services, beyond the identified scope of work will be based on our hourly rates, and expenses incurred at cost.

# APPENDIX A – RESPONSE REQUIREMENT

## 1. PART 1

Item 1 - Name of Individual or Organization: **AESI-US, Inc.**
Item 2 - Name and Title of Contact Person: **Joel Charlebois, VP, Regulatory Compliance**
Item 3 - Business Address: **1990 Lakeside Parkway, Suite 250 · Tucker, Georgia · USA · 30084**
Item 4 - Telephone #: **770-870-1630 ext. 236**
Item 5 - Email Address: **JoelC@aesi-inc.com**
Item 6 - Fax #: **770-870-1629**

## 2. PART 2

**Item 1 - Consultant Business Form**

1. Identify the Consultant's business or corporate structure:

   **Type of Business: Corporation**

   **Date and State of Incorporation: July 15, 1997, in Atlanta, Georgia.**

   **List Name and Title of Executive Officers: Donald J.A. Robinson, Loreto D. Sarracini, Joseph G. Raso**

   **Principal Place of Business: 1990 Lakeside Parkway, Suite 250, Tucker, GA. 30084**

   **List all Related Principal or Subsidiaries Corporations: AESI Acumen Engineered Solutions International Inc.**

   **Closed or Publicly Traded: Closed**

   **EIN: 58 2340591**

2. Identity the number of years your entity has been in business.
   **24 years (Found in 1997)**

3. Identity whether your business/corporate structure has changed in the past five years and if yes, describe the change:
   **No**

4. Identity the type and coverage amount of all insurance policies.
   **Please see Appendix B – Insurance Coverage**

5. Identified the name, address, and contract information for three (3) companies that the Consultant has performed similar services to those being sought by the Authority.

   Name: **Lakeland Electric**
   Address: **501 E Lemon St, Lakeland, FL 33801**
   Contact: **Larry Watt, Larry.Watt@lakelandelectric.com**

   Name: **EPCOR Utilities**
   Address: **10432 101 Street NW Suite 2000 Edmonton, AB T5H 0E8 Canada**
   Contact: **Jean Masbang, IT Auditor; 780-412-4492; jmasbang@epcor.com**

   Name: **New Brunswick Power (NB Power)**
   Address: **NB Power 515 King Street, Fredericton, NB E3B 4X1**
   Contact: **Luther Eroh, 506-458-4622; Luther.Eroh@nbpower.com**

6. If you are a certified, minority and/or women owned business, submit a copy of the certification.

   **N/A**

**Item 2 - Consultant Team**
**Item Description:**
This section identifies all the AESI staff who will be working on this project. Identify the individuals whose professional services will be utilized to undertake a comprehensive IT Cybersecurity Risk and Vulnerability Assessment, including thoroughly reviewing the current state of the Authority's information technology security, developing a vulnerability mitigation plan, and developing a prioritized road map of activities to enhance the Authority's future Cybersecurity position.

The following information for each identified individual:

A) Relevant qualifications and experience, including educational degrees and any applicable licenses or certifications (e.g., CISSP, CISM, CGEIT, CRISC), and

B) State and county of residence, and

C) Scope of responsibility, and

D) Length of time working for Consultant.

AESI RESPONSE:

## Project Director: Edvard Lauman, P. Eng., GCIA

A) Edvard (Ed) has more than 17 years of experience working as a Cyber Security Specialist, including hands-on operation and management of SCADA systems, security and network operations for a large transmission and distribution utility. He is a system integration expert, specializing in SCADA, Data Historians, Distributed Control Systems, related network, and security infrastructure, as well as custom software development. His experience incorporates requirements and technology assessments with the design and development of IT/Control solutions, as well as identifying and resolving network, telecommunications, and application level issues.

*Relevant Experience*

- Conducted multiple Cyber Vulnerability Testing for distribution, transmission and generation power utilities
- Developed cyber security policies and procedures for several distribution utilities, including a utility implementing a 16-million-dollar smart grid project encompassing all aspects of their operation
- Designed and implemented cyber security architectures for the SCADA portion for many utilities' networks
- Relevant qualification: P. Eng., GCIA

B) Ed is located in Edmonton, Canada.

C) Ed will act as the Project Director. Ed will have the overall responsibility for the quality and timeliness of our services. He will monitor the overall progress and communicate with our project team to ensure satisfaction with our process and deliverables.

In addition, Ed will provide support as the SCADA/OT SME for system administration, networks, physical and cyber security, system configuration and operational technology.

D) Ed has been at AESI for 14+ years

## Project Manager, Cyber Security SME & Tester: Ivan Wong, CCNA

A) Ivan is a goal-oriented and collaborative IT professional with proven experience analysing and troubleshooting large corporation networks with more than 10 years of experience. He has conducted multiple cyber security vulnerability assessments, including paper assessments, for power generation utilities, distribution utilities, water treatment plants, and corporate environments through preliminary document review, on-site vulnerability scan, analysis, and reporting while meeting NERC CIP v3 and v5 requirements. His strong technical knowledge, coupled with the ability to quickly learn new systems, allows him to provide practical solutions. He is comfortable supporting both technical and non-technical audiences.

*Relevant Experience*

- Conducted multiple cyber security vulnerability assessments for power generation utilities, distribution utilities, water treatment plants, and corporate environments through preliminary document review, on-site vulnerability scans, and analysis
- Reviewed process and procedure documents for cybersecurity gap assessment projects.
- Relevant Certification: CCNA

B) Ivan is located in Toronto, Canada.

C) Ivan will be the Project Manager and will assist Edvard Lauman, the Project Director, with the overall responsibility for the quality and timeliness of our services. He will monitor the overall progress and communicate with our project team to ensure satisfaction with our process and deliverables. In addition, Ivan will be the Cyber Security SME and Tester. Ivan will be engaged in all phases of the project through completion with active participation in the assessment and testing phases. He will assist with analysis and documentation development, including mitigation plans and road map for ECWA's future cybersecurity posture.

D) Ivan has been at AESI for 8+ years.

## Cyber Security SME & QA/QC: James Chacko, CISSP, CISA, ITIL, CEH, CHFI

A) James Chacko is a Senior Security Specialist with over 11 years of progressive experience with emphasis on projects related to infrastructure, systems and application deployment. He has proven experience in operations and technical support, systems/network administration, business technical analysis and project management. His experience comprises of security policy and procedures for networking (LAN/WAN), software evaluations, network security assessments and recommendations for improvements.

*Relevant Experience*

- Content development and technical presenter for USF OEB Cyber Security Framework training
- Developing IT/OT cyber security training for American Public Power Association (APPA)
- Part of a team developing an American Public Power Association (APPA) survey to collect data and evaluate "data-in-motion"
- Developed and delivered training for a complete backbone network structure for the building, the data center, security and access control systems, in suite technology, and back office systems
- Served as the SME for the PCI data security standards compliance requirements for a hospitality reservation, POS and back office system. Scheduled internal audits for the payment systems to ensure that regulatory controls were in place and applied.
- Maintained audit reports and served as the point of contact during the external audits
- Provided comprehensive cyber security risk assessment of the data warehouse and supervised migration of Back-Office application – Sage ERP 300 v2012 to Sage ERP 300 v2017, from an on-site server to a hosted solution
- Relevant Certifications: CISSP, CISA, ITIL, CEH, CHFI

B) James is located in Edmonton, Canada.

C) James will provide support as an SME for cyber security standards, baselines, policies, procedures, and guidelines. James will perform most of the CVA and penetration testing related work on external/internet facing nodes.

D) James has been at AESI for 5+ years

# 3. PART 3

**Item 1 - Proposed Scope of Service**

**Item Description**

Working in consultation with the Authority's IT staff, the Consultant will be required to develop comprehensive IT Cybersecurity Risk and Vulnerability Assessment.

Describe the scope of service, which the Consultant would recommend to the Authority, to undertake a comprehensive IT Cybersecurity Risk and Vulnerability Assessment. The scope should include the following elements, along with such elements will be performed on-site or off-site:

A. Review of current state of the Authority's information technology security,

B. Development of a vulnerability mitigation plan,

C. Development of a prioritized road map of activities to enhance the Authority's future Cybersecurity position,

D. Best practice methodologies to ensure a standardized risk mitigation approach that will offer the highest risk reduction potential, complementing the "Framework for Improving Critical Infrastructure Cybersecurity", developed by the National Institute for Standards and Technology (NIST),

E. Assessment that includes but not limited to:

- Test for susceptibility to Advanced Persistent Threats (APTs) such as viruses, malware, Trojan horses, botnets, and other targeted attack exploits.
- Evaluate the Authority's current threat posture including antivirus and Intrusion Detection and Prevention (IDP) capabilities.
- Evaluate the Authorities planned changes and improvements to the threat surface and assist identifying and addressing security concerns.
- Review the Authority's current Supervisory Control and Data Acquisition (SCADA) water systems for security vulnerabilities.
- Review wireless network system components for security vulnerabilities, validating system-specific operating systems and firmware versions for known exploits and recommend upgrades, updates, and mitigations.
- Review current system-specific operating systems and firmware versions for known exploits and recommend upgrades, updates, and mitigations. This includes firewalls,

switches and routers, Microsoft Active Directory, email and file servers, web servers, wireless routers, WAN, VPN, VoIP, and CCTV systems.
- Assess VoIP network system components for security vulnerabilities, validating system-specific operating system and firmware versions and reviewing for known exploits.
- Review existing IT policies and procedures and make recommendations for changes and/or additional policy and procedure development.
- Execute and review internal network vulnerability scans and external vulnerability and penetration scans and make recommendations to reduce the threat attack surface.
- Recommend or assist in selection of vulnerability scan software for purchase/license for continued use by the Authority after the assessment is complete.

AESI Response:

**AESI will be able to deliver all the in-scope items mentioned above. For more details of the items in scope, refer to Section 4, title *Project Understanding*, in the main sections of the proposal.**

**Item 2 - Hardware and Software Requirements**

A. Describe the required hardware and/or software necessary to implement Consultant's plan, if any.

**AESI will be using two laptops dedicated for vulnerability assessments and penetration testing. One laptop will be used onsite to perform the assessment while the other one will be used remotely to perform the assessment on the external IP addresses. AESI will be using a variety of tools to perform the assessment, the main tools will be Nessus and Metasploit. Other tools within the Kali Linux OS may also be used as well depending on the scenario.**

B. Describe the limitations of the service and/or equipment, if any.
**None**

C. Identify whether the required hardware and/or software will be provided by Consultant or the Authority.

**AESI will provide the hardware and software to perform the assessment.**

**Item 3 - Timeframe for Deliverables**

Provide a timeframe for completing the following deliverables:

1. Project Management Deliverables:
   a. Work Breakdown Schedule (WBS) including tasks,
   b. Schedule and dependencies, and
   c. Weekly Status Reports including risks and progress reports.

**AESI will deliver the draft WBS and schedules during the first kickoff meeting and will finalized the WBS and schedule within 5 business days after the kickoff meeting. Weekly Status Reports will be provided once the onsite or remote work has begun.**

2. Report: A written report documenting:
   a. Executive summary detailing the Authority's Cybersecurity position, including a comparative scorecard of findings,
   b. Results of vulnerability testing performed,
   c. Identified cybersecurity vulnerabilities, gaps, and mitigation plans,
   d. A prioritized road map of activities, developed in conjunction with Authority's IT staff to enhance the Authority's future cybersecurity position.

**AESI will present a draft report based on the items above four weeks after the onsite and remote work is completed. EWCA will have two weeks to review the report and AESI will finalize the report once all questions and comments regarding the draft report has been addressed.**

3. Projected solutions and costs:
   a. Provide an estimated range, based upon previous experience, of the total services costs to implement the proposed solutions,
   b. Include a Rate Sheet that specifies and itemizes the cost for each proposed component, including all licensing, support, maintenance, and hosting fees, and
   c. For subscription-based services, provide annual pricing.

**The cost of this project to provide professional services will not require EWCA to purchase any additional components, such as licensing, support, maintenance, hosting fees, or subscription-based fees.**

**The cost for the Erie County Water Authority Cyber Security Risk and Vulnerability Assessment is $47,000, Fixed Fee inclusive of labor and expenses. Our quote does not include any applicable taxes. The optional social engineering service is an additional $5,100 while the optional physical security review is an additional $3,700.**

*Options for Project*

| Options | Total Fixed Price |
|---|---|
| **Option 1**: CVA + Pen Test + Document Review | $47,000 |
| **Option 2**: CVA + Pen Test + Document Review + Social Engineering | $52,100 |
| **Option 3**: CVA + Pen Test + Document Review + Physical Security Review | $50,700 |
| **Option 4**: CVA + Pen Test + Document Review + Social Engineering + Physical Security Review | $55,800 |

## Item 4 - Price Structure

1. Provide a detailed description of the Consultant price structure or pricing option for the services to be provided by the Consultant.

**The project is a fixed price project identified in Item 3.3. Additional services, beyond the identified scope of work will be based on our hourly rates, and expenses incurred at cost.**

*Hourly Rates for 2020 & 2021*

| Staff | Hourly Rate * |
|---|---|
| Edvard Lauman | $280 |
| Ivan Wong | $220 |
| James Chacko | $205 |

* AESI adjusts its rates annually effective January 1

2. If the Consultant has a standardize agreement used for such services, include a copy with the Proposal.

**Please see Appendix C.**

# APPENDIX B – INSURANCE COVERAGE

# CERTIFICATE OF LIABILITY INSURANCE

**ISSUE DATE** YYYY/MM/DD
2021/04/15

BROKER

**HUB International Ontario Limited**
**2265 Upper Middle Road East, Suite 700**
**Oakville, ON L6H 0G5**

**This certificate is issued as a matter of information only and confers no rights upon the certificate holder and imposes no liability on the insurer. This certificate does not amend, extend or alter the coverage afforded by the policies below.**

| | |
|---|---|
| Company A | Continental Casualty Company (CNA) |
| Company B | AIG Commercial Insurance Company of Canada |
| Company C | |
| Company D | |
| Company E | |

**INSURED'S FULL NAME AND MAILING ADDRESS**
AESI Acumen Engineered Solutions International Inc.
a/o AESI US Inc.
775 Main Street E. Suite #1B
Milton, ON L9T 3Z3
Canada

## COVERAGES

This is to certify that the policies of insurance listed below have been issued to the insured named above for the policy period indicated notwithstanding any requirements, terms or conditions of any contract or other document with respect to which this certificate may be issued or may pertain. The insurance afforded by the policies described herein is subject to all terms, exclusions and conditions of such policies.

**LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS**

| TYPE OF INSURANCE | CO LTR | POLICY NUMBER | EFFECTIVE DATE YYYY/MM/DD | EXPIRY DATE YYYY/MM/DD | LIMITS OF LIABILITY (Canadian dollars unless indicated otherwise) | |
|---|---|---|---|---|---|---|
| **COMMERCIAL GENERAL LIABILITY**<br>□ CLAIMS MADE<br>☒ OCCURRENCE<br>☒ PRODUCTS AND/OR COMPLETED OPERATIONS<br>☒ PERSONAL INJURY<br>☒ EMPLOYER'S LIABILITY<br>☒ TENANT'S LEGAL LIABILITY<br>☒ NON-OWNED AUTOMOBILE<br>☒ HIRED AUTOMOBILE | A | MPR2718929 | 2021/01/31 | 2022/01/31 | EACH OCCURRENCE | $ 2,000,000 |
| | | | | | GENERAL AGGREGATE | $ 5,000,000 |
| | | | | | PRODUCTS - COMP/OP AGGREGATE | $ 2,000,000 |
| | | | | | PERSONAL INJURY | $ 2,000,000 |
| | | | | | EMPLOYER'S LIABILITY | $ 2,000,000 |
| | | | | | TENANT'S LEGAL LIABILITY | $ 1,000,000 |
| | | | | | NON-OWNED AUTOMOBILE | $ 2,000,000 |
| | | | | | HIRED AUTOMOBILE | $ 75,000 |
| **AUTOMOBILE LIABILITY**<br>□ DESCRIBED AUTOMOBILES<br>□ ALL OWNED AUTOMOBILES<br>□ LEASED AUTOMOBILES **<br>□ GARAGE LIABILITY<br>□<br>** ALL AUTOMOBILES LEASED IN EXCESS OF 30 DAYS WHERE THE INSURED IS REQUIRED TO PROVIDE INSURANCE | | | | | BODILY INJURY PROPERTY DAMAGE COMBINED | $ |
| | | | | | BODILY INJURY (Per person) | $ |
| | | | | | BODILY INJURY (Per accident) | $ |
| | | | | | PROPERTY DAMAGE | $ |
| **EXCESS LIABILITY**<br>☒ UMBRELLA FORM<br>□ OTHER THAN UMBRELLA FORM | A | MPR27187919 | 2021/01/31 | 2022/01/31 | EACH OCCURRENCE | $ 3,000,000 |
| | | | | | AGGREGATE | $ 3,000,000 |
| **OTHER (SPECIFY)**<br>PROFESSIONAL LIABILITY | B | 06-112-70-14 | 2020/07/11 | 2021/07/11 | Each Claim | $ 3,000,000 |
| | | | | | Aggregate | $ 3,000,000 |
| | | | | | Deductible | $ 50,000 |
| | | | | | Retro Dates: July 11, 1997 | $ |
| | | | | | July 11, 2015 & July 11, 2017 | $ |

**DESCRIPTION OF OPERATIONS/LOCATIONS/AUTOMOBILES/SPECIAL ITEMS TO WHICH THIS CERTIFICATE APPLIES** (but only with respect to the operations of the Named Insured)

For Information Purposes Only

**CERTIFICATE HOLDER**

AESI Acumen Engineered Solutions International Inc.
a/o AESI US Inc.
775 Main Street E, Suite #1B
Milton, ON L9T 3Z3

**CANCELLATION**

Should any of the above described policies be cancelled before the expiration date thereof, the issuing company will endeavor to mail 0 days written notice to the certificate holder named to the left, but failure to mail such notice shall impose no obligation or liability of any kind upon the company, its agents or representatives.

AUTHORIZED REPRESENTATIVE

Per:______________________________

# CERTIFICATE OF LIABILITY INSURANCE

**ISSUE DATE** YYYY/MM/DD
2021/04/28

**BROKER**

**HUB International Ontario Limited**
**2265 Upper Middle Road East, Suite 700**
**Oakville, ON L6H 0G5**

**This certificate is issued as a matter of information only and confers no rights upon the certificate holder and imposes no liability on the insurer. This certificate does not amend, extend or alter the coverage afforded by the policies below.**

| | |
|---|---|
| Company A | Chubb Insurance Company of Canada |
| Company B | |
| Company C | |
| Company D | |
| Company E | |

**INSURED'S FULL NAME AND MAILING ADDRESS**
AESI Acumen Engineered Solutions International Inc.
775 Main Street E. Suite #1B
Milton, ON L9T 3Z3
Canada

## COVERAGES

This is to certify that the policies of insurance listed below have been issued to the insured named above for the policy period indicated notwithstanding any requirements, terms or conditions of any contract or other document with respect to which this certificate may be issued or may pertain. The insurance afforded by the policies described herein is subject to all terms, exclusions and conditions of such policies.

**LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS**

| TYPE OF INSURANCE | CO LTR | POLICY NUMBER | EFFECTIVE DATE YYYY/MM/DD | EXPIRY DATE YYYY/MM/DD | LIMITS OF LIABILITY (Canadian dollars unless indicated otherwise) | |
|---|---|---|---|---|---|---|
| **COMMERCIAL GENERAL LIABILITY** | | | | | EACH OCCURRENCE | $ |
| □ CLAIMS MADE | | | | | GENERAL AGGREGATE | $ |
| □ OCCURRENCE | | | | | PRODUCTS - COMP/OP AGGREGATE | $ |
| □ PRODUCTS AND/OR COMPLETED OPERATIONS | | | | | PERSONAL INJURY | $ |
| □ PERSONAL INJURY | | | | | EMPLOYER'S LIABILITY | $ |
| □ EMPLOYER'S LIABILITY | | | | | TENANT'S LEGAL LIABILITY | $ |
| □ TENANT'S LEGAL LIABILITY | | | | | NON-OWNED AUTOMOBILE | $ |
| □ NON-OWNED AUTOMOBILE | | | | | HIRED AUTOMOBILE | $ |
| □ HIRED AUTOMOBILE | | | | | | |
| **AUTOMOBILE LIABILITY**<br>□ DESCRIBED AUTOMOBILES | | | | | BODILY INJURY PROPERTY DAMAGE COMBINED | $ |
| □ ALL OWNED AUTOMOBILES<br>□ LEASED AUTOMOBILES ** | | | | | BODILY INJURY (Per person) | $ |
| □ GARAGE LIABILITY | | | | | BODILY INJURY (Per accident) | $ |
| □<br>** ALL AUTOMOBILES LEASED IN EXCESS OF 30 DAYS WHERE THE INSURED IS REQUIRED TO PROVIDE INSURANCE | | | | | PROPERTY DAMAGE | $ |
| **EXCESS LIABILITY**<br>□ UMBRELLA FORM | | | | | EACH OCCURRENCE | $ |
| □ OTHER THAN UMBRELLA FORM | | | | | AGGREGATE | $ |
| **OTHER (SPECIFY)**<br>Cyber | A | 82616072 | 2021/04/28 | 2022/04/28 | Each Cyber Incident Limit | $ 2,000,000 |
| | | | | | Aggregate - all cyber incidents | $ 2,000,000 |
| | | | | | Retention | $ 20,000 |
| | | | | | Retro Date - April 28 2021 | $ |
| | | | | | | $ |

**DESCRIPTION OF OPERATIONS/LOCATIONS/AUTOMOBILES/SPECIAL ITEMS TO WHICH THIS CERTIFICATE APPLIES** (but only with respect to the operations of the Named Insured)

For Information Purposes Only

**CERTIFICATE HOLDER**

AESI Acumen Engineered Solutions International Inc.
775 Main Street E, Suite #1B
Milton, ON L9T 3Z3

**CANCELLATION**

Should any of the above described policies be cancelled before the expiration date thereof, the issuing company will endeavor to mail 0 days written notice to the certificate holder named to the left, but failure to mail such notice shall impose no obligation or liability of any kind upon the company, its agents or representatives.

AUTHORIZED REPRESENTATIVE

Per:____________________

AESIINC-S3 CGRANZOW

ACORD

# CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)
3/4/2021

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

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

| | | |
|---|---|---|
| PRODUCER License # 0019304-1<br>Hub International Midwest East<br>1591 Galbraith Ave SE<br>Grand Rapids, MI 49546 | CONTACT NAME:<br>PHONE (A/C, No, Ext): (616) 233-4111<br>E-MAIL ADDRESS: | FAX (A/C, No): (616) 233-4110 |
| | INSURER(S) AFFORDING COVERAGE | NAIC # |
| | INSURER A : Hartford Insurance Group | 914 |
| INSURED<br>AESI-US Inc<br>1990 Lakeside Pkwy Ste 250<br>Tucker, GA 30084 | INSURER B : | |
| | INSURER C : | |
| | INSURER D : | |
| | INSURER E : | |
| | INSURER F : | |

COVERAGES CERTIFICATE NUMBER: REVISION NUMBER:

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

| INSR LTR | TYPE OF INSURANCE | ADDL INSD | SUBR WVD | POLICY NUMBER | POLICY EFF (MM/DD/YYYY) | POLICY EXP (MM/DD/YYYY) | LIMITS | |
|---|---|---|---|---|---|---|---|---|
| | □ COMMERCIAL GENERAL LIABILITY<br>□ CLAIMS-MADE □ OCCUR<br>□<br>□<br>GEN'L AGGREGATE LIMIT APPLIES PER:<br>□ POLICY □ PRO-JECT □ LOC<br>□ OTHER: | | | | | | EACH OCCURRENCE<br>DAMAGE TO RENTED PREMISES (Ea occurrence)<br>MED EXP (Any one person)<br>PERSONAL & ADV INJURY<br>GENERAL AGGREGATE<br>PRODUCTS - COMP/OP AGG | \$<br>\$<br>\$<br>\$<br>\$<br>\$<br>\$ |
| | AUTOMOBILE LIABILITY<br>□ ANY AUTO<br>□ OWNED AUTOS ONLY □ SCHEDULED AUTOS<br>□ HIRED AUTOS ONLY □ NON-OWNED AUTOS ONLY<br>□ □ | | | | | | COMBINED SINGLE LIMIT (Ea accident)<br>BODILY INJURY (Per person)<br>BODILY INJURY (Per accident)<br>PROPERTY DAMAGE (Per accident) | \$<br>\$<br>\$<br>\$<br>\$ |
| | □ UMBRELLA LIAB □ OCCUR<br>□ EXCESS LIAB □ CLAIMS-MADE<br>□ DED □ RETENTION \$ | | | | | | EACH OCCURRENCE<br>AGGREGATE | \$<br>\$<br>\$ |
| A | WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y / N<br>ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? □<br>(Mandatory in NH)<br>If yes, describe under DESCRIPTION OF OPERATIONS below | N / A | X | 81WECID1060 | 4/3/2020 | 4/3/2021 | □ PER STATUTE □ OTH-ER<br>E.L. EACH ACCIDENT<br>E.L. DISEASE - EA EMPLOYEE<br>E.L. DISEASE - POLICY LIMIT | <br>\$ 1,000,000<br>\$ 1,000,000<br>\$ 1,000,000 |
| | | | | | | | | |

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)
Waiver of Subrogation applies in favor of Northern California Power Agency.

No Owned vehicles will be used

| CERTIFICATE HOLDER | CANCELLATION |
|---|---|
| [redacted] | SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS. |
| | AUTHORIZED REPRESENTATIVE |

# APPENDIX C – STANDARD CONTRACT AND NON-DISCLOSURE AGREEMENT

AESI

www.aesi-inc.com
aesi@aesi-inc.com

# CONSULTING SERVICES AGREEMENT

**THIS AGREEMENT**, made as of the ________ day of ___________, (year)________, by and between **AESI–US, Inc. (“AESI”)**, a corporation and validly existing under the laws of the State of Georgia and _________________________________ (“Client”) and organized and validly existing under the laws of the State of __________________________, in the Country of __________________________.

**WITNESSETH**

**WHEREAS**, AESI is engaged in the business of providing professional engineering and general consulting services; and
**WHEREAS,** Client desires to retain the services of AESI; and
**WHEREAS,** AESI is willing to provide Client with certain consulting services, and Client is willing to accept such services, all upon the terms and conditions contained herein.
**NOW, THEREFORE,** for and in consideration of the mutual covenants contained herein, the parties hereto hereby agree as follows:

## 1. SERVICES

This Agreement shall be applicable, to all professional engineering, engineering consulting, and other consulting services performed for or on behalf of Client by AESI as described in Scope of Work attached hereto and which is incorporated herein and made a part hereof.

AESI shall render services in a manner consistent with that degree of care and skill exercised by practicing design professionals performing similar services under the same or similar circumstances or conditions. AESI makes no further representations or any warranties, whether express or implied, as to the services rendered herein.

## 2. TERM

(a) Except as otherwise provided herein, this Agreement is effective from the date first written above and shall remain in effect until the earlier of (i) termination in writing by either party or (ii) upon completion of the Services specified in the Scope of Work and payment of all amounts owing to AESI for such Services.

(b) This Agreement may be terminated upon the receipt of thirty (30) days’ written notice of such termination by either party from the other. In the event of any termination under this subparagraph (b), AESI shall be compensated as provided herein for all Services rendered up to and including the date of receipt of notice of termination.

## 3. RESPONSIBILITIES OF CLIENT

With regard to the Services, Client, without limitation, shall:

(a) designate and authorize an officer or other agent of Client to act on Client’s behalf in all matters reasonably related to the project;

1990 Lakeside Pkwy
Suite 250
Tucker, Georgia
USA 30084
P·770.870.1630
F·770.870.1629

775 Main Street E
Suite 1B
Milton, Ontario
Canada L9T 3Z3
P·905.875.2075
F·905.875.2062

(b) provide AESI with all criteria and necessary information to perform the Services;

(c) furnish to AESI all existing studies, reports, and other data available to Client pertinent to the project;

(d) obtain for AESI's use additional reports, data, or information as may be reasonably required by AESI;

In performing Services hereunder, AESI shall have the right to justifiably rely on any and all such studies, reports, data, and services provided to AESI by or on behalf of Client.

## 4. BREACH

In the event either party hereto breaches any of the provisions of this Agreement, the non-breaching party at its option may give the breaching party written notice of such breach and shall allow the breaching party reasonable time to cure such breach. In the event such breach is not cured within said time, this Agreement shall terminate, and Client shall compensate AESI for all Services performed or contracted for up to and including the date of the termination of this Agreement.

## 5. COMPENSATION

AESI shall be compensated for Services in accordance with Fee Schedule attached hereto and which is incorporated herein and made a part hereof.

## 6. PAYMENT

AESI shall submit statements to Client for all charges and Services rendered by AESI and for costs incurred by AESI as provided in Fee Schedule hereto. Client agrees to pay promptly to AESI all amounts stated on each such statement. If payment is not received by AESI within thirty (30) days after AESI's delivery of such statement to Client by Mail or otherwise, the amounts due to AESI may include an additional monthly charge equal to 1.0% of the total invoice. Such monthly charge shall accrue on all amounts due from said thirtieth (30th) day through the date on which such statement is paid in full; provided, however, that in no event shall such charge exceed the maximum legal rate allowable by law. Client understands and agrees that in the event of non-payment, AESI may, after giving written notice to Client, suspend Services under this Agreement. The failure of AESI to impose any such charges or suspend any Services for any period of time shall not constitute a waiver of AESI's right to do so at any future date.

In the event Client fails to pay AESI all amounts which become due under this Agreement, or fails to perform any of its obligations hereunder, and AESI refers such matter to an attorney, Client agrees to pay, in addition to any amounts due hereunder, any and all reasonable costs incurred by AESI as a result of such action, including reasonable attorneys' fees.

## 7. DOCUMENTS, SOFTWARE, SYSTEMS, AND PROCESSES

(a) Unless otherwise provided in Scope of Work, all documents provided by AESI to Client pursuant to this Agreement are instruments of service with respect to a particular project and are not intended or represented to be suitable for reuse by Client or others. Client understands and agrees that any such reuse by Client without the written verification and authorization by AESI of such reuse shall be at Client's sole risk and without liability or legal exposure to AESI.

(b) Unless otherwise provided in Scope of Work, all software, systems, and processes formulated or developed by AESI in connection with a project pursuant to this Agreement are the sole property of AESI. The Client shall not make any proprietary claims to such software, systems, processes or items, but shall have the rights to use for its own business purposes.

(c)  Without limitation, AESI shall not be liable for any suits or claims for infringement of any patent rights or copyrights resulting from AESI's infringement of such rights in connection with any Project Assignment based upon an invention, design, process, product, or device designed by Client or provided to AESI by Client.

The Client agrees to defend, indemnify and hold AESI harmless from and against any and all claims, losses, liabilities and damages arising out of or resulting from the unauthorized use, reuse or alteration of the AESI's documents without AESI's involvement.

## 8.  COST ESTIMATES

Opinions of probable costs, financial evaluations, feasibility studies, economic analyses of alternate solutions, and utilitarian considerations of operations and maintenance costs prepared by AESI hereunder shall be made on the basis of AESI's best judgment as a consulting firm in accordance with generally accepted standards.  Client understands and agrees that AESI's opinions, evaluations, studies, analyses, and considerations are often based on conditions over which AESI has no control and that any such studies, analyses, evaluations, and opinions of probable costs prepared by AESI must of necessity be speculative.  Accordingly, AESI in no way warrants or represents that any of such studies, analyses, evaluations, or opinions of probable costs will not vary as a result of such conditions.

## 9. INDEMNIFICATION AND INSURANCE

(a)  Client understands and agrees that Client shall immediately indemnify and hold AESI and its subcontractors harmless against and in respect to, without limitation, any and all actions, suits, proceedings, demands, assessments, judgments, costs, expenses, losses or attorneys' fees (hereinafter referred to as "Liabilities") arising out of, in connection with, or as a result of the performance of Services by AESI  on behalf of Client; provided, however, that such indemnification shall not apply to the extent AESI is liable for any such Liability due to AESI's negligence or willful misconduct in breach of this contract.

(b)  Without limitation, Client understands and agrees that in the event Client is required to indemnify AESI under the provisions of this Paragraph 9 for Services, or costs or expenses associated thereunder, the terms and conditions for compensation of AESI contained in Paragraph 5 hereof shall be controlling where applicable and to the fullest extent possible.

## 10.  PROJECT ASSIGNMENTS

(a)  Client understands and agrees that all Services provided by AESI to Client shall be upon the terms and conditions contained in this Agreement.  Client understands and agrees and further warrants and represents to AESI that such Services shall only be performed pursuant to the terms and conditions of this Agreement and may only be amended as provided herein.

(b)  The Scope of Work to this Agreement specifies the duties and responsibilities of AESI pursuant to this Agreement.  To the extent there is a conflict between this Agreement and the Scope of Work, this Agreement shall prevail.

(c)  Any project schedule, as it pertains to the project, and any subsequent modification thereto shall be prepared with AESI's concurrence.  AESI shall not be liable for any damages (consequential or otherwise) caused by delays in work, irrespective of cause.

(d)  AESI agrees to commence work on the project as scheduled and to comply with the project schedule as mutually agreed upon by Client and AESI.  Client agrees that it shall furnish AESI with all data necessary to AESI's performance of the Services and fulfill its responsibilities and obligations hereunder in a timely manner. Client further agrees that if Client fails to fulfill its responsibilities and obligations in a timely manner hereunder, AESI shall be due an extension of time to such project schedule to the extent affected by such failure.

(e) If Services required as a result of a change requested by the Client and mutually agreed to by the parties extending the time required for completion of the project, the time allocated for the Project Assignment shall be adjusted accordingly.

(f) AESI may maintain a sealed and confidential copy of project documentation to support its ability to respond to government or regulatory proceedings or investigations involving AESI that are directly related to work outlined by this Agreement. Any Confidential Information retained in accordance with the preceding sentence may be retained for a period of time appropriate to state or provincial jurisdiction where the associated work was done or was applicable to and during such period shall remain subject to all of the provisions of this Agreement.

## 11. SUBCONTRACTORS

AESI may, upon obtaining the Client's consent, retain qualified subcontractors from time to time to assist in the performance of Services under this Agreement.

## 12. CONTRACTUAL RELATIONS

Nothing contained in this Agreement or any amendments hereto shall create or cause any contractual relationship or liability between AESI and any third parties.

## 13. SPECIAL AND CONSEQUENTIAL DAMAGES

Notwithstanding anything else to the contrary in this Agreement, neither AESI nor Client shall be liable to the other for any special, indirect, incidental or consequential damages, including, without limitation, any principal, interest, loss of anticipated revenues, earnings or profits, increased costs of operation or construction, costs of procurement of substitute goods or services, loss by reason of shutdown or non-operation due to late completion or otherwise, fines, penalties, or other regulatory or judicial judgments, whether or not any such loss or damage is caused by the fault or negligence of AESI or Client and whether or not arising out of this Agreement, even if AESI or Client has been advised of the possibility of any such loss or damage.

## 14. GENERAL

This Agreement between AESI and Client contains the entire agreement of the parties hereto regarding the subject matter hereof, and no representation, inducement, promise or agreement, oral or otherwise, between the parties hereto regarding the subject matter hereof, not embodied herein, shall be of any force or effect. The provisions hereof shall inure to the benefit of and be binding upon the parties hereto, their legal representatives, successors, and permitted assigns.

## 15. SEVERABILITY

If any clause or provision of this Agreement is held or deemed to be illegal, invalid, or unenforceable under present or future laws effective during the term hereof, then and in that event, it is the intention of the parties hereto that the remainder of this Agreement shall not be affected thereby, and it is also the intention of the parties hereto that in lieu of each clause or provision of this Agreement that is illegal, invalid, or unenforceable, there be deemed to have been added as a part of this Agreement, a clause or provision as similar in terms to such illegal, invalid, or unenforceable clause or provision as may be possible, and at the same time, be legal, valid, and enforceable. All rights, powers, and privileges conferred hereunder upon the parties hereto shall be deemed cumulative of and in addition to those provided by law.

## 16. CAPTIONS

The captions in this Agreement are added as a matter of convenience only and shall not be considered in the construction, interpretation, or enforcement of any provision hereof.

## 17. ASSIGNMENTS

This Agreement may not be assigned by either party without the written approval of the other party; provided, however, approval of such assignment shall not be unreasonably withheld.

## 18. WAIVER

Any waiver at any time by either party hereto of its rights with respect to the other party or with respect to any matter arising in connection with this Agreement shall not be considered a waiver with respect to any subsequent default or matter.

## 19. NOTICES

All notices required to be given in writing under this Agreement shall be deemed delivered when deposited in the mail with first class postage prepaid unless otherwise provided herein.

Such notice if being given to AESI shall be addressed to:

**{Enter Name}**
**AESI–US, Inc.**
**1990 Lakeside Parkway, Suite 250**
**Tucker, Georgia**
**30084**

and if being given to Client shall be addressed to:

Either party may change its respective notice address by written notice as specified above.

## 20. LIMITATION OF LIABIITY

To the fullest extent permitted by law, the total liability of AESI and its officers, directors, shareholders, and employees to Client for any and all injuries, claims, losses, expenses, or damages whatsoever arising out of or in any way related to AESI's services, the project, or this Agreement, from any cause whatsoever, including but not limited to the negligence, errors, omissions, strict liability, breach of contract, misrepresentation, or breach of warranty of AESI or AESI's officers, directors, shareholders, and employees, shall not exceed the total compensation received by AESI under this Agreement.

## 21. GOVERNING LAW

This Agreement shall be governed by and construed and enforced in accordance with the laws of the State of Georgia.

**IN WITNESS WHEREOF**, the parties hereto have entered into this Agreement as of the date first written above.

Authorized Signature on behalf of:

CLIENT

Signature: ______________________

Name: ______________________

Title ______________________

Date: ______________________

Witness (if required)

Signature: ______________________

Name: ______________________

Title ______________________

Date: ______________________

Authorized Signature on behalf of:

**AESI-US, Inc.**

Signature: ______________________

Name: ______________________

Title ______________________

Date: ______________________

Witness (if required)

Signature: ______________________

Name: ______________________

Title ______________________

Date: ______________________

# NON-DISCLOSURE AGREEMENT

**THIS AGREEMENT** made between the **AESI-US, Inc.,** a Georgia corporation hereafter referred to as “AESI”, and the second party henceforth identified as the “Corporation”.

**WHEREAS** AESI and the Corporation have each determined that there is a mutual need and benefit to exchange selected information and each party desires to protect the confidentiality of any information exchanged.

**NOW, THEREFORE**, for and in consideration of the mutual promises contained within this document, the parties hereby agree as follows:

## 1. DEFINITIONS

For the purposes of this Agreement:

"Confidential Information" means information and data which meets both of the following conditions: (i) all technical or business information and data, whether oral or written, in whatever media or form, which is disclosed, directly or indirectly, by either party to the other party; and (ii) if such information or data is marked "private", "restricted”, "confidential", "proprietary" (or otherwise marked or described so as to indicate confidentiality). If the information is provided in oral form by the disclosing party, then the disclosing party must issue a written document declaring that the subject information is to be treated as confidential.

This designation as confidential applies to the information or data whether in its original form or whether it is converted to different forms or combined with additional information, and including any information relating to third parties contained therein, and any notes, memoranda, summaries, analyses, compilations or any other writings relating thereto prepared relative thereto by the receiving party or on its behalf.

## 2. OBLIGATIONS ARISING FROM DISCLOSURE

During the course of the business relationship established between the parties pursuant to this Agreement, each party may disclose to the other party or permit the other party access to certain Confidential Information, either directly or indirectly. Each disclosure of Confidential Information will be made or permitted upon the basis of the confidential relationship established between the parties by this Agreement and upon each party's agreement that, unless otherwise specifically authorized in writing by the other, it will:

(i) use the Confidential Information solely for the purpose for which it was disclosed;

(ii) take all reasonable care and precautions to keep the Confidential Information confidential, such care and precautions being at least as great as the care and precautions that it takes to protect its own confidential or proprietary information;

(iii) not disclose, or allow the disclosure of, any Confidential Information before or after termination of this Agreement, except as permitted by this Agreement;

(iv) restrict disclosure of the Confidential Information only to its employees or other personnel, advisors, consultants and agents (collectively known as, "Representatives") with a need to know the Confidential Information and who are bound to maintain the Confidential Information as confidential;

(v) notify each Representative that receives any Confidential Information of the requirements of this Agreement and of the restrictions on use and disclosure of Confidential Information imposed by this Agreement;

(vi) take reasonable care and precautions to ensure that no Representative breaches or causes or allows to be breached any of the receiving party's obligations hereunder and direct each Representative to abide by the terms of this Agreement;

(vii) not use, or allow to be used, any Confidential Information to compete with or in a manner detrimental or adverse to the commercial interests of the disclosing party;

(viii) except in connection with the purpose for which Confidential Information is disclosed, not copy or duplicate such Information or knowingly allow anyone else to copy or duplicate such Information;

(ix) upon request by the disclosing party, made before or after termination of this Agreement, the receiving party shall, as specified by the disclosing party, either: a) promptly return such Confidential Information to the disclosing party; or b) certify as destroyed, the Confidential Information in whatever form and regardless of whether such Confidential Information was made or compiled by the receiving party or furnished by the disclosing party, together with all copies howsoever made; and

(x) Notwithstanding the foregoing, the receiving party shall be entitled to keep, subject always to all the provisions of this Agreement, one copy of any notes, analyses, reports or other written material prepared by, or on behalf of, the receiving party that contain Confidential Information for its records.

## 3. EXCEPTIONS

The obligations under this Agreement shall not apply to any Confidential Information that the receiving party can demonstrate to the disclosing party's reasonable satisfaction:

(i) became public and generally known through no act or omission of the receiving party or its Representatives;

(ii) was in legitimate possession of the receiving party prior to its disclosure by the disclosing party to the receiving party;

(iii) that the receiving party is required by law, through judicial or arbitration process to disclose, provided that prior to disclosing any Confidential Information, the receiving party shall promptly (unless compelled by law to act expeditiously) notify the disclosing party of such requirement to disclose and take such steps as are reasonably necessary, and cooperate with the disclosing party, to lawfully limit such disclosure and to maintain the confidentiality of the Confidential Information in the hands of the receiving party, including obtaining appropriate protective orders; or

(iv) is approved in writing by the disclosing party for release or other use by the receiving party according to the terms set out in such written approval.

The burden of demonstrating that the provisions of this Section 3 permit a disclosure to a third party shall be upon the receiving party.

## 4. DISCRETIONARY DISCLOSURE

Each party acknowledges that, irrespective of any provisions contained with this Agreement, each party maintains the sole and absolute discretion to determine what, if any, Confidential Information it will release to the other party. The receiving party acknowledges that the Confidential Information disclosed in any manner whatsoever is proprietary to the disclosing party.

## 5. NO WARRANTY

Each party warrants that it has the requisite authorization to enter into this Agreement.

Each party warrants that it has the right to disclose any Confidential Information disclosed to the other party.

Each party acknowledges that the other party makes no other representation or warranty in relation to any Confidential Information disclosed including, without limiting the generality of the foregoing, as to its adequacy, accuracy, or suitability for any purpose and, except as expressly agreed in writing, shall not be liable for any loss or damage arising from the use of the Confidential Information howsoever caused.

## 6. INTELLECTUAL PROPERTY

Each party acknowledges and agrees that all Confidential Information shall be owned solely by the disclosing party. Each party further agrees that nothing contained in this Agreement shall be construed as granting any rights, by license or otherwise, under any intellectual property rights in, or concerning any of, the disclosing party's Confidential Information.

## 7. EQUITABLE REMEDIES

In the event of a breach or threatened breach of any term of this Agreement, the receiving party agrees that the harm suffered or that may be suffered by the disclosing party would not be compensable by monetary damages alone and, accordingly, that the disclosing party shall, in addition to other available legal or equitable remedies, be entitled to the issuance of immediate injunctive relief, specific performance and any other remedies available in law or equity for such breach or threatened breach of the receiving party's obligations hereunder. If the receiving party is proven to have violated the obligations of this Agreement, the receiving party shall reimburse the disclosing party for all reasonable costs and expenses, including reasonable legal fees and disbursements, incurred by the disclosing party in attempting to enforce the obligations under this Agreement of the receiving party or its Representatives.

## 8. INDEPENDENT ACTIVITIES

Each party, as a disclosing party, understands that the receiving party may currently or in the future be developing information internally, or receiving information from a third party that may be similar to the disclosing party's Confidential Information. Accordingly, nothing in this Agreement shall be construed as a representation or warranty that the receiving party will be in violation of the provisions of this Agreement if it develops products or services, or has products or services developed for it, or enters into any arrangement that, without violation of any of the provisions of this Agreement, compete with the products or services which are contemplated by, or which are the subject of, the disclosing party's Confidential Information or the purpose for which Confidential Information was disclosed.

## 9. NO IMPLIED OBLIGATIONS

Neither this Agreement, nor the disclosure or receipt of any Information, shall imply or confirm any intention to enter into any contract or other business relationship, or to purchase any product or service, by either of the parties or any commitment by either of the parties with respect to the present or future development, production or distribution of any product or service.

## 10. TERMINATION AND SURVIVAL

Either party may terminate this Agreement at any time upon prior written notice to the other party. In the event that this Agreement is terminated, this Agreement shall not apply to any Confidential Information disclosed after such termination but shall, notwithstanding the termination of this Agreement, continue to apply to any and all Confidential Information disclosed prior to the termination of this Agreement for a period of 3 years.

## 11. MISCELLANEOUS

Governing Law: This Agreement shall be governed by and construed in accordance with the laws of the State of Georgia exclusively and without reference to principles of conflict of laws and in accordance with the laws of the State of Georgia and the laws of the United States, applicable therein, excluding laws relating to choice of laws.

Jurisdiction: The parties agree that the Courts of the State of Georgia shall have exclusive jurisdiction in reference to any matters herein and agree to the jurisdiction of the Courts of the State of Georgia. The Federal Arbitration Act (“FAA”) will supersede state laws to the extent inconsistent. The Arbitrator(s) shall have no authority to apply the law of any other jurisdiction.

No Waiver: Failure of a party to insist upon strict adherence to any term of this Agreement on any occasion or the waiver of a breach of this Agreement in any instance shall not deprive the party of the right thereafter to insist on strict adherence to that term or any other term in this Agreement or be construed as a waiver of any subsequent breach, whether or not similar.

Severability: Should any provision of this Agreement be determined to be void, invalid or otherwise unenforceable by any court of competent jurisdiction, such determination shall not affect the remaining provisions of this Agreement which shall remain in full force and effect.

Inurement: This Agreement shall be binding upon and inure to the benefit of the parties hereto, their respective successors and permitted assigns.

Headings: The headings contained in this Agreement are for convenience of reference only and shall not affect the interpretation or meaning of this Agreement.

Entire Agreement: This Agreement constitutes the entire agreement regarding Confidential Information between the parties hereto with respect to the matters herein contained.

Amendments: No modification or addition to this Agreement shall be valid unless made in writing and signed by duly authorized representatives of each of the parties.

Counterparts: This Agreement may be executed in any number of counterparts with the same effect as if the parties signed the same document. All counterparts will be construed together and will constitute one and the same Agreement.

Execution: This Agreement may be executed by the parties and transmitted by email or facsimile transmission and will be for all purposes effective as if the parties executed and delivered one original Agreement.

**IN WITNESS WHEREOF,** the parties hereto have executed and delivered this Agreement on, and effective as of, this ____ day of ____________________, 20__.

**AESI-US, Inc.**

**By:** ________________________________________________

**Name:** ________________________________________________

**Title:** ________________________________________________

________________________________________________

**(Insert name of the Corporation)**

**By:** ________________________________________________

**Name:** ________________________________________________

**Title:** ________________________________________________

DEANDORTON

+

# ERIE COUNTY WATER AUTHORITY

# Proposal for Cybersecurity Risk and Vulnerability Assessment

**June 11, 2021**

# TABLE OF CONTENTS

*Part 1* ........................................................................................ *1*

*Part 2* ........................................................................................ *2*

*Part 3* ........................................................................................ *10*

# PART 1

**Item 1 - Name of Organization**
Dean Dorton Allen Ford, PLLC

**Item 2 - Name and Title of Contact Person**
Jason Miller
Business and Technology Consulting Director

**Item 3 - Business Address**
250 West Main Street
Suite 1400
Lexington, KY 40507

**Item 4 - Telephone Number**
859.425.7626

**Item 5 - Email Address**
jmiller@ddaftech.com

**Item 6 - Fax Number**
859.425.3626

# PART 2

## Item 1 - Consultant Business Form

1. *Identify the Consultant's business or corporate structure:*

   **Date and State of Formation**
   1921 in Kentucky

   **Name of General Partners**

   - David Bundy, President
   - Bill Kohm, Assurance Director
   - Joe Johnston, Tax Director
   - Lance Mann. Assurance Director
   - Mike McCreary, Tax Director
   - Jason Miller, Business and Technology Consulting Director
   - Jen Shah, Tax Director
   - Mike Shepherd,Tax Director
   - Adam Shewmaker, Healthcare Consulting Director
   - David Smith, Tax Director
   - Jim Tencza, Assurance Director

   **Type of Partnership**
   Professional Limited Liability Company

   **Principal Place of Business**
   Lexington, Kentucky

   **EIN**
   27-3858252

2. *Identify the number of years your entity has been in business:*
   100

3. *Identify whether your business or coporate structure has changed in the past years:*
   The business structure has not changed in the past five years at Dean Dorton

4. *Identify the type and coverage amount of all insurance policies:*
   The following list includes the types and coverage amounts of all of the insurance policies at Dean Dorton:

   - Cyber Liability (coverage $5,000,000, $10,000 deductible)
   - Professional Liability ($6,000,000 per claim/$6,000,000 annual aggregate/$200,000 deductible)
   - Employee Dishonesty (included in professional liability policy $1,500,000/$500 deductible)
   - Professional Liability - Excess ($4,000,000 Excess Only; no additional deductible)
   - Property/General Liability/Umbrella (general liability $2,000,000; umbrella $7,000,000)
   - Workers Compensation (coverage of $1,000,000)
   - Directors, Officers, and Fiduciary ($1,000,000 per claim/$1,000,000 annual aggregate/$10,000 deductible)
   - Employment Practices ($2,000,000 per claim/$2,000,000 annual aggregate/$10,000 deductible)

# PART 2

5. *Identified the name, address, and contract information for three (3) companies that the Consultant has performed similar services to those being sought by the Authority.*

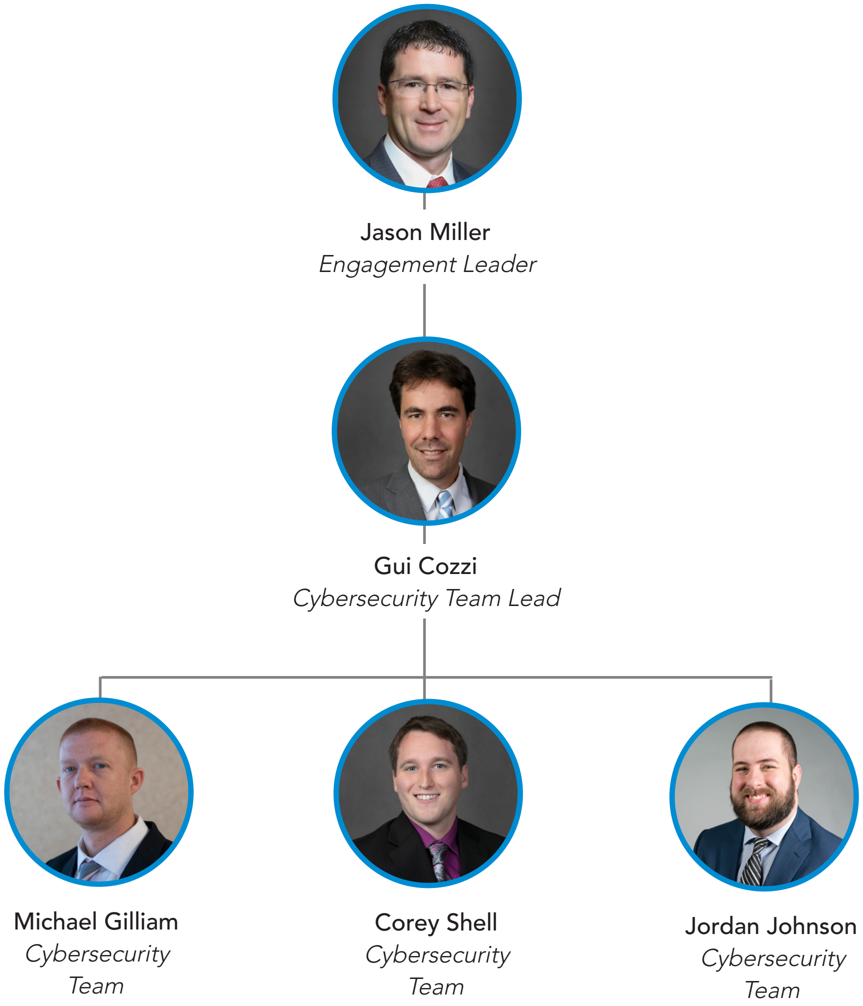
| Organization | Type of Engagement | Contact/Title | Phone/Email | Address |
|---|---|---|---|---|
| **Berea College** | GLBA Remediation, IT Policy Development, IT Risk Assessment | Phillip Logsdon<br>Chief Information Officer | 859.985-3886<br>logsdonp@berea.edu | 210 Center Street<br>Berea, KY 40403 |
| **Jefferson County Public Schools** | IT Risk Assessment, Security Assessment, Penetration Testing, Internal IT Audit Services | Jodi Renn<br>Director of Internal Audit | 502.500.5930<br>jodell.renn@jefferson.kyschools.us | 3332 Newburg Road<br>Louisville, KY 40218 |
| **Louisville Metro Government** | Information Security Risk Assessment and Penetration Testing Services | James Meece<br>Chief Information Security Officer | 502.574.3658<br>james.meece@louisvilleky.gov | 527 W. Jefferson Street<br>Louisville, KY 40202 |

6. ***If you are a certified, minority and/or women owned business, submit a copy of the certification.***
Dean Dorton is not a minority or women owned business.

# PART 2

### Item 2 - Consultant Team

Dean Dorton strongly believes that a team approach to this project provides the best possible deliverable for Dean Dorton. As such, we will compile a team that consists of members from our Technology Consulting Group. The combined experience of this group will provide a fully qualified team that understands the compliance, technical, and practical aspects of undertaking a comprehensive IT Cybersecurity Risk and Vulnerability Assessment. Individual biographies are included on the following pages for each team member who has been identified as a key resource to be used on the Authority's project. Other staff may be leveraged as needed.



Jason Miller
*Engagement Leader*

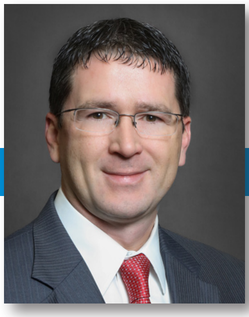
Gui Cozzi
*Cybersecurity Team Lead*

Michael Gilliam
*Cybersecurity Team*

Corey Shell
*Cybersecurity Team*

Jordan Johnson
*Cybersecurity Team*

# JASON D. MILLER



*Business and Technology Consulting Director*
859.425.7626
jmiller@ddaftech.com
Fayette County, Kentucky

## *Professional Experience*

During his college career and since that time, Jason has been providing technology and business consulting services to clients. Upon graduating from college, he spent three years in software development for a publicly traded international software company. He has been with Dean Dorton since 2001, where he has helped clients of all sizes and in various industries with technology and business management needs. Jason is currently responsible for overseeing the design, implementation, and support of business networks for Dean Dorton's clients. He is also responsible for managing the evaluation, implementation, and support of accounting and business management software solutions for clients.

In addition to his general technology and business consulting experience, Jason has over 18 years of experience in IT auditing. He leads the firm's IT audit function for its traditional audit engagements, System and Organization Controls (SOC) reporting engagements, and internal IT audit outsourcing, as well as other specialized IT assessment and audit projects. Jason assists our clients on Payment Card Industry Data Security Standards (PCI DSS) compliance matters.

Most recently, Jason has been instrumental in building the firm's dedicated cybersecurity services team. This team provides outsourced information security office services and cybersecurity assessment services.

## *Industry Expertise*

Jason focuses primarily in the government, healthcare, equine, legal services, nonprofit, and natural resources industries.

## *Professional Activities*

American Institute of Certified Public Accountants, Technology Section
Lexington Young Professionals Association

## *Community Involvement*

Trinity Hill United Methodist Church, Parish Relations Committee Chair
Lexington Christian Academy, Finance Committee

## *Special Honors and Achievements*

National Student Employee of the Year, 1998
Leadership Lexington Graduate, 2008
Upstream Academy, Emerging Leaders Program, 2009-2012

## *Education*

Bachelor of Science in Industrial Technology Management, 1998, Berea College, Berea, Kentucky

# GUI COZZI, CISSP, CISA, CRISC

*Cybersecurity Practice Lead*
859.425.7649
gcozzi@ddaftech.com
Fayette County, Kentucky

## *Professional Experience*

Gui has 20 years of experience in cybersecurity and successfully implements pragmatic and risk-based security programs to meet compliance with organizations' security requirements. Gui leads a team responsible for delivering enterprise cybersecurity services and personally specializes in information security program development, implementation, and assessment. His work is focused on positioning organizations to successfully identify and manage their information security risks.

Prior to joining Dean Dorton, Gui served in various Information Security leadership roles including implementing the Security Risk Management program for one of the nation's largest health systems, leading teams of cybersecurity consultants, and serving as Chief Information Security Officers for organizations in various industries.

## *Industry Expertise*

Gui has extensive experience in healthcare, financial services, public sector, and biotech industries.

## *Speaking Engagements*

- "Anatomy of an Attack" and "Ask the Expert Panel," 2019 Kentucky Chamber of Commerce Cybersecurity Conference
- "GDPR," 2018 AIKCU Business Officers' Fall Meeting
- "How to Build and Maintain an Efficient Cybersecurity Program," 2018 Institute of Internal Auditors – Louisville Chapter; 2018 Information Technology Managers' Association Meeting
- "Cybersecurity Threats Update," 2018 Dean Dorton Equine Tax & Accounting Update; 2018 Dean Dorton Board Oversight and Risk Management Seminar

## *Professional Activities*

Information Systems Audit and Control Association (ISACA) Kentuckiana Chapter, Board Member
ISACA International, Topic Leader on Risk Management
International Information Systems Security Certification Consortium (ISC2)
InfraGard
Kentucky Health Information Exchange, Privacy and Security Committee

## *Certifications*

Certified Information Systems Security Professional (CISSP)
Certified Information Systems Auditor (CISA)
Certified in Risk and Information Systems Control (CRISC)

## *Community Involvement*

Georgetown Football Club, Corporate Sponsorship
Bluegrass Pony Club, Volunteer

## *Education*

Master of Business Administration in Management and Strategy, 2009, Western Governors University, Salt Lake City, Utah
Bachelor of Science in Business Management, 2007, Western Governors University, Salt Lake City, Utah

# MICHAEL GILLIAM, ISC2, CISSP

*Cybersecurity Manager*
859.425.7794
mgilliam@ddaftech.com
Fayette County, Kentucky

## *Professional Experience*

Michael's professional background includes six years working on the blue team (security operations) side of security as well as six years working on the red team (conducting technical security assessment and penetration tests).

Michael has extensive experience with vulnerability and patch management, computer forensics, incident response, security awareness training and development, network intrusion detection, and technical security assessments (including penetration testing). He also holds a security clearance.

## *Industry Expertise*

Michael's qualifications include several security related designations and detailed knowledge of technical security tools, technologies, and best practices. His current experience includes creating, maintaining, and deploying security solutions protecting networks, systems, and information assets for federal and state government agencies, as well as private sector organizations in the healthcare and financial industries.

## *Certifications*

International Information Systems Security Certification Consortium (ISC2)
Certified Information Systems Security Professional (CISSP)
EC-Council Certified Ethical Hacker
CompTIA Security+
CompTIA Network+
Information Assurance Certification Review Board - Certified Computer Forensics Examiner
Snort Certified Professional

## *Education*

Bachelor of Science, Telecommunications System Management - Network Security, 2009, Murray State University, Murray, Kentucky
Associate of Applied Science, Computer Networking, 2006, Bluegrass Community and Technical College, Lexington, Kentucky

# COREY SHELL, CISSP, CEH, CHFI

*Cybersecurity Senior Consultant*
859.425.7749
cshell@ddaftech.com
Fayette County, Kentucky

## *Professional Experience*

Corey has 10 years of combined information technology and cybersecurity experience. He has a passion for cybersecurity and helping his clients to identify their risks and determine their cybersecurity preparedness. Corey specializes in ethical hacking, vulnerability management, and information security program development, implementation, and assessment.

Corey's previous IT security experience in the financial sector helped him to understand the complex compliance issues and cybersecurity risks that financial institutions face. Prior to joining Dean Dorton, he served as a manager and team lead for cybersecurity projects, leading teams of cybersecurity consultants, and served as the Virtual Information Security Officer (vISO) for organizations in various industries.

## *Industry Expertise*

Corey has extensive experience in healthcare, financial services, public sector, and biotech industries.

## *Speaking Engagements*

"Achieving a Cybersecure Organization" KyCPA Community Bank Update (2018)
"Introduction to the FFIEC Cybersecurity Assessment Tool" Webinar (2016)

## *Professional Activities*

Information Systems Audit and Control Association (ISACA) Kentuckiana Chapter, Board Member
International Information Systems Security Certification Consortium (ISC2)
InfraGard

## *Certifications*

Certified Information Systems Security Professional (CISSP)
Certified Ethical Hacker (CEH)
Computer Hacking Forensic Investigator v8 (CHFI)

## *Education*

Master of Science in Information Security and Assurance, 2017, Western Governors University, Salt Lake City, Utah
Bachelor of Science in Business Information Systems, Cum Laude, 2014, Indiana Wesleyan University, Marion, Indiana

# JORDAN JOHNSON

*Cybersecurity Consultant*
859.425.7659
jjohnston@deandorton.com
Fayette County, Kentucky

## *Professional Experience*

Jordan has more than five years of Information Technology experience, with roles ranging from IT Support Technician, System Engineer, to Systems Administrator. Jordan currently works to manage CrowdStrike and various Cybersecurity control implementations for various clients.

## *Industry Expertise*

Jordan has vast experience working with clients in different industries including manufacturing, government, and managed services.

## *Certifications*

CrowdStrike Certified Falcon Aministrator
Security+

## *Education*

Bachelor of Science in Cybersecurity, 2019, University of Cumberlands, Williamsburg, KY

# PART 3

### Item 1 - Proposed Scope of Services

Based on our review of the requirements described in the 2021 Authority RFP, it is our understanding the Authority has expressed interest in Cybersecurity assessment services. Dean Dorton's Cybersecurity team is ready to assist the Authority in addressing these critical needs.

The goals of this engagement are to show areas for improvement in critical information systems, use business impact analysis and technical findings to drive long term strategic planning, as well as assess the effectiveness of the Authority's current security controls against known TTP (Tactics, Techniques and Procedures). Dean Dorton is proposing to deliver a Cybersecurity assessment that includes external, web application, wireless, and internal security testing services.

***Cybersecurity Assessments***

Dean Dorton's Cyber Security Assessment Services are designed to provide organizations specific information about the state of their Information Security posture and to validate that key controls are working as expected.

Our methodology follows project management best practices so you know at any point of time during the project what is going on, what the next steps are, and when you will receive your Security Assessment report. Our commitment to you is to deliver the Security Assessment Report when we said we would and to provide an easy-to-read report with incredibly insightful and actionable information.

***External Security Assessment (Black Box)***

The External Security Assessment is performed from outside the organization's security perimeter, usually from the Internet. The External Security Assessment can also include an optional Social Engineering Testing to see how likely users fall to phishing and other scamming techniques used to start cyber-attacks often resulting in data breaches. During the External Assessment, we work closely with your IT department to make sure that all critical systems are in scope for the review. The External Security Assessment will be executed as follows:

***External Security***

- Attack Surface Analysis
- Secure Configuration Analysis
- Organizational Information Gathering
- People Information Gathering
- Technical Information Gathering
- Web Service Protections (DoS, WAF, IPS)
- Reputation Analysis
- Network Layer Vulnerabilities
- Application Layer Vulnerabilities

Objectives:

1. Identify all known systems and network and application layer vulnerabilities that could be exploited by an external hacker
2. Meet security assessment requirements for regulated entities but it is now common practice across all industries
3. Recommend additional controls to improve the external cybersecurity posture

Assumptions:

1. Up to 500 live IP addresses

# PART 3

***Web Application Penetration Test***

The Web Application Penetration Test is a dynamic analysis of custom developed web application code as it exists when running live. The tests are conducted in coordination with Authority IT staff, and can include both authenticated and unauthenticated dynamic analysis of the web site. The Web Application Penetration Test will cover the following security domains for web applications:

***Web Application Security***

- Reconnaissance and Information Gathering
- Security Testing and Analysis
- Test Handling of Input
- Fuzzing Input
- Testing for Cross-Site Scripting (XSS)
- Injection Attempts (where applicable), to include SQL injection
- Reflection Attempts
- Application Hosting Review
- Testing for Weak/Insecure Encryption
- Testing for Authentication Bypasses

Objectives:

1. Discover new (previously unknown) vulnerabilities that may exist in Authority web configuration or code

Assumptions:

1. Four (4) Web Applications

# PART 3

***Internal Security Assessment (White Box)***

The Internal Security Assessment is conducted from an organization's internal network in coordination with the Information Technology team. In addition to the identification of vulnerabilities, the Internal Security Assessment also encompasses deep-dive security reviews of specific areas to include security configuration management, hardening, and best practice reviews. The Internal Security Assessment has components to help identify risks posed from common sources.

***Infrastructure Security***

- Communications Security
- Warning Banner for Untrusted Email
- Email Content Filtering
- Implement DMARC and Enable Receiver-Side Verification
- Block Unnecessary File Types
- Physical Security
- Access Controls
- Auditing Controls
- Environmental Controls

***Network Security***

- Configuration Review
- Out of Band Management Network
- Vulnerability Identification
- Web Application Firewall
- Firewall Configuration Review
- Firewall ACL Review
- Web Content Filtering
- Network Intrusion Detection / Prevention
- Physical Connectivity Review
- Network Segmentation
- DMZ Review
- VPN Review

***Wireless Security***

- Guest Network Segmentation
- Physical Placement of Access Points
- Wirelesss Intrusion Detection/ Prevention System
- Wireless Authentication/Encryption Review
- Wireless Exposure Strengths
- Wireless Infrastructure Management Access Review
- Vulnerability Analysis
- Heatmapping

***Endpoint Security***

- IoT Security
- OS Hardening Review
- Mobile Code Review
- Weak Protocols Review
- File Share Review
- BIOS Security Review
- Full Disk Encryption Review
- Remote Worker Review
- Malware Protection Assessment
- Exploit Prevention
- Patch Management Agent Audit
- Workstation Communication
- Removable Media Controls
- Vulnerability Analysis

***Active Directory Security Review***

- DNS Query Logging
- Use of DNS Filtering Services
- DNS Vulnerabilities
- Block Internet Access to DC
- Domain Functional Level
- Domain Trusts Review
- Administrator Rights Review
- Skeleton Key Review
- Risky SPN's
- Risky SID Review
- Delegated Access Review

***Account Security***

- Inactive User Accounts Review
- Password Not Required
- Administrative Groups Review
- Tiered Administrative Account
- Service Account Review
- Continuous Monitoring of Privileged Groups Review
- Least Privilege
- Legacy Authentication Protocols Remote Services (VPN, Mail, Etc.)
- Group Policy Preferences Review
- Password Policy
- Password Storage and Sharing
- Domain Password Management
- Local Password Management
- Password Audit

***Internal Security Assessment (White Box) - continued***

Objectives:

1. Identify risks posed from NIST defined common threat sources: Adversarial, Accidental, Environmental, and Structural
2. Meet security assessment requirements for regulated entities
3. Recommend additional controls to improve the internal cybersecurity posture
4. Conduct Penetration Testing (non-exploitive) of a sampling of devices

Highlights:

- **Web Content Filtering** – Dean Dorton security analysts will test up to three different web content filtering profiles to determine any potential bypasses in the current deployment, or areas of strengthening required to reduce organizational risk.
- **Network Intrusion Detection/Prevention** – Dean Dorton security analysts will simulate malicious traffic and connections to known Command & Control servers with the goal of determining if your internal network security team (or outsourced provider) has the capability to detect, and is monitoring the events generated if you were to have an infected system connect to your internal network.
- **Mobile Code Review** – Today's malware often relies on scripts that users are tricked into running. Dean Dorton will review PowerShell and Office Macro settings to identify risks.
- **Full Disk Encryption Review** – Dean Dorton will identify laptops connected during the testing window and identify if they are protected with Bitlocker or any custom full disk encryption solution.
- **Endpoint Protections** – Dean Dorton will work with your IT team to identify your specific endpoint protections (Patch Management Agents, Exploit Prevention, EDR, DLP agents) and provide an audit that identifies systems that are missing these expected protections (and if they are running the latest version).
- **File Share Review** – With ransomware on the rise, it is critical your organization understand your internal network file share attack surface. Unstructured data residing on these file shares is at risk from compromised workstations if left unprotected. Dean Dorton will enumerate these weaknesses and provide a comprehensive map for remediation.
- **Tiered Access Review** – According to the 2019 Verizon Data Breach Report, Credential theft is on the rise. To help mitigate these threats, Microsoft recommends implementing a Tiered Access model for privileges to create hard security boundaries for account access. Dean Dorton will evaluate your organizations implementation and provide details on implementation gaps that may exist.
- **Active Directory ACL Review** – Attackers are getting cleverer by the day; just because an account does not have Domain Administrator rights, does not mean that there is not a path for that account to grant themselves permissions. Dean Dorton will perform a detailed, recursive analysis of granted permissions to groups for each account to identify accounts that are indirectly a high risk for the organization.
- **Password Audit** – Dean Dorton security analysts will work to identify Active Directory domain accounts that have chosen weak passwords, and would expose the organization to a risk of online brute force attacks.

Assumptions:

1. 100 servers
2. 175 workstations
3. 100 network devices (sampling deep dive configuration review)
4. Two (2) locations in scope for Wireless Security survey/heat mapping
5. All systems can be scanned from a single physical location

### Item 2 - Hardware and Software Requirements

Dean Dorton uses a wide variety of commercial, open source, and custom developed tooling to conduct testing. To provide for complete coverage, Dean Dorton uses application and network layer vulnerability scanners. Dean Dorton requested, and was granted, administrative level access to systems to be able to perform authenticated vulnerability scans which greatly increase the depth of the assessment to include detailed audits of endpoint security controls, as well as client side vulnerabilities and privilege escalation issues. Dean Dorton may use some of the following tools in this engagement:

BURPSUITE 2.0
nessus® Professional
PowerShell
NMAP
MASS SCAN
metasploit®
algosec
NIPPER STUDIO
EXPLOIT DATABASE
OFFENSIVE® security

# PART 3

### Item 3 - Timeframe for Deliverables

### Reporting Requirements

Dean Dorton will work with the Authority to ensure that the Security Assessment report is accurate, comprehensive, and delivered on a timely basis. Dean Dorton anticipates that the engagement's timeline will be as follows:

1. Kickoff call (include identification of host targets)
2. External Security Assessment (two weeks of testing)
3. Web Application Penetration Testing (one week of testing)
4. Internal Security Assessment (two to three weeks of testing)
5. Draft Report delivery (will occur within two weeks after all testing is complete)

The Report will include the following sections:

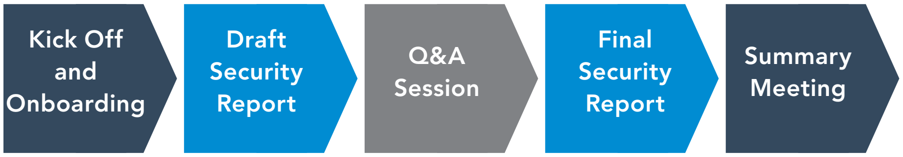
- Executive summary with business impact analysis
- Technical summary of findings, including critical vulnerabilities and applicable controls
- Projected solutions and costs
- Summary meeting/post mortem to discuss findings

Dean Dorton will work closely with the Authority to minimize the risk of disruption to business operations that could be caused by these assessment procedures. The service necessarily involves the use of network tools and techniques designed to detect security vulnerabilities, and it is impossible to identify and eliminate all the risks involved with the use of these tools and techniques.

Dean Dorton will finalize all its assessment activity and documentation of the security assessment into a final deliverable for the Authority that includes remediation recommendations. It is our understanding that this report is intended for the information and use of the Authority and is not intended to be, nor should be, used by anyone other than these parties.

### Schedule

Dean Dorton has prepared a draft of an engagement schedule, assuming a late third quarter start date that can be adjusted based on further discussions with the Authority team.



Kick Off and Onboarding

Draft Security Report

Q&A Session

Final Security Report

Summary Meeting

**Pre-Assessment Work**

8/2/2021 - 8/6/2021

**External Security Assessment**

8/9/2021 - 8/20/2021

**Web Application Security Assessment**

8/23/2021 - 8/27/2021

**Internal Security Assessment**

9/7/2021 - 9/18/2021

**Timeline is an estimation and will be impacted by the Authority team start date, availability, and responsiveness*

### Item 4 - Price Structure

| Service | Fees |
|---|---|
| External Security Assessment | $8,000 |
| Internal Security Assessment | $22,000 |
| **TOTAL** | **$30,000** |

*Additionally, the Authority will be invoiced for all out-of-pocket administrative and travel expenses, including mileage.*

### Terms

This engagement does not anticipate the compilation, review, or audit of financial records or financial statements. At no time shall any member of the Dean Dorton team make any management decisions on behalf of the Authority. We will only provide technical expertise, support and recommendations to management throughout this engagement. It will be your responsibility to assign a resource to act as our primary contact and to be responsible for making all decisions on behalf of the Authority.

In the unlikely event that differences concerning our services or fees should arise that are not resolved by mutual agreement, in order to facilitate resolution of the differences and to save all parties time and expense, the Authority and Dean Dorton agree to try in good faith to settle their differences by mediation administered by the American Arbitration Association under the Dispute Resolution Rules for Professional Accounting and Related Services Disputes before resorting to litigation. In the event that litigation cannot be avoided, the Authority and Dean Dorton agree not to demand a trial by jury.

If any portion of this letter is held to be void or otherwise unenforceable, in whole or in part, the remaining portions of this letter shall remain in effect.

Thank you again for the opportunity to assist Authority in these matters. If you have any questions related to this proposal, please let me know.

# Cybersecurity Risk & Vulnerability Assessment

## REDACTED

**Prepared for:**

**Erie County Water Authority**

**June 11, 2021**

**Prepared by:**
**JANUS Software, Inc.**
d/b/a JANUS Associates
2 Omega Drive
Stamford, CT 06907
Contact: Patricia Fisher
Phone: 203-251-0200
Email: patfisher@janusassociates.com

# Table of Contents

**INTRODUCTORY COVER LETTER** .......... **1**

**INTRODUCTION** .......... **3**

**PART 1** .......... **3**

**PART 2** .......... **3**

ITEM 1 – CONSULTANT BUSINESS FORM .......... 3

ITEM 2 – CONSULTANT TEAM .......... 5

**PART 3** .......... **35**

ITEM 1 – PROPOSED SCOPE OF SERVICE .......... 35

OVERVIEW .......... 35

JANUS' APPROACH AND METHODOLOGY .......... 36

PRELIMINARY ACTIVITIES .......... 42

TARGETED ATTACK EXPLOITS .......... 44

EVALUATING CHANGES .......... 46

INTERNAL ASSESSMENT .......... 46

WIRELESS ASSESSMENT .......... 48

VOICE OVER INTERNET PROTOCOL (VOIP) .......... 49

POLICY AND PROCEDURE REVIEW .......... 50

ITEM 2 – HARDWARE AND SOFTWARE REQUIREMENTS .......... 50

ITEM 3 – TIMEFRAME FOR DELIVERABLES .......... 51

ITEM 4 – PRICE STRUCTURE .......... 55

**QUALIFICATIONS AND EXPERIENCE** .......... **62**

JANUS CAPABILITIES .......... 64

ASSESSING RISK .......... 68

**MANAGEMENT PLAN** .......... **71**

PROJECT MANAGEMENT APPROACH .......... 72

**REFERENCES AND PRIOR WORK EXPERIENCE** .......... **76**

REFERENCES .......... 76

PAST PERFORMANCE .......... 76

**NEEDS FROM AUTHORITY STAFF** .......... **82**

**ASSUMPTIONS** .......... **82**

**OTHER ITEMS** .......... **84**

SECURITY MEASURES .......... 84

BONDING AND BACKGROUND CHECK PROCEDURES .......... 85

CHANGE ORDER PROCESS .......... 85

**APPENDICES** .......... **86**

APPENDIX A – TOOLS .......... 86

APPENDIX B – SAMPLE REPORT .......... 92

APPENDIX C – CLIENT COMMENTS .......... 99

This proposal has been redacted.

JANUS requests that sections in our proposals titled Methodology, Approach, Deliverables, and Cost (or any language associated with them) including graphics and/or charts within those sections be treated as Proprietary/Trade Secrets. This information relates to JANUS' main line of business and the disclosure of which would cause irreparable harm to our business by providing a competitive advantage to other companies.

JANUS deems information related to our employees (in tables, biographies, and resumes) as Protected, and contact information related to our clients as Confidential. Due to the personal nature of, and to prevent other companies from attempting to recruit our employees we do not reveal their names; and as a security company we do not openly reveal our clients' contact information.

JANUS
ASSOCIATES

certified
WBENC
WOMEN'S BUSINESS ENTERPRISE

June 11, 2021

Mr. Terrence D. McCracken
Secretary to the Authority
Erie County Water Authority
295 Main Street, Room 350
Buffalo, NY 14203

Dear Mr. McCracken:

JANUS Software, Inc., d/b/a JANUS Associates (JANUS) is pleased to present the Erie County Water Authority (the Authority) with this proposal for a Cybersecurity Risk and Vulnerability Assessment.

Since being founded in 1988, JANUS has had our core competency providing leading edge information security services and has extensive experience in performing the types of security services requested by the Authority. We regularly provide similar services for federal, state and local government entities, private sector businesses, higher education, and not-for-profit organizations. Examples of recent similar projects include the Massachusetts Water Resources Authority, South Central Connecticut Regional Water Authority, New York State Dormitory Authority, New York State Teachers' Retirement System, Central District Transportation Authority, amongst many others.

Over our entire history, we have built a well-deserved reputation for high quality, "on-time, within budget" performance and for consistently high client satisfaction. These attributes are due to the skills and professionalism of JANUS staff and to our firm's dedication to delivering quality services in complex environments, providing leading edge experience and true value for clients – while remaining free of any vendor affiliations. As a result, our recommendations are totally focused on your needs, and are not associated with selling tools, or vendor offerings.

You may very well receive lower cost proposals. However, in cybersecurity, these low-cost alternatives come with their own price – which is lack of skill – and skill is the key element in cybersecurity services which can assist you in avoiding breaches and attacks. In addition, our clients report to us that these lower priced alternatives always result in higher costs because work is left undone which our client must then figure out and complete. With JANUS, you will not receive more thorough assessments or stronger

IT security services at a fair price designed to protect your assets than those offered by JANUS. We have also been informed by our clients that we offer more detailed (and thorough) analysis in our assessments and consulting. We are passionate about doing the right thing for you and protecting your environment at the level needed.

Thank you for allowing JANUS the opportunity to submit this proposal. We are ready to begin this project, and JANUS management and staff look forward to working with your team to meet your security goals and objectives and to exceed expectations as a service provider.

Sincerely,

Patricia A. P. Fisher

Patricia A. P. Fisher
President & CEO

# INTRODUCTION

JANUS has studied your Request for Proposals (RFP) and the answers to questions. We have structured our response to take both these into consideration. Having completed a number of large, recent water utility security assessments, we hope to be able to guide the Erie County Water Authority (the Authority) along a strong path to improved security and maturity in your program. We hope you speak with our other water authority clients. We believe they will reinforce our position as a very caring company, with extremely competent technical expert staff, and who focuses our work around constantly helping you reinforce your controls, understand better what will serve you well, and strategically comprehend what resource outlays will best serve your interests.

JANUS understands how to perform what you need and we will always focus on making sure all our staff remains centered on what will serve you best.

# PART 1

| | |
|---|---|
| **Item 1 – Name of Organization** | JANUS Software, Inc.<br>d/b/a JANUS Associates |
| **Item 2 – Name and Title of Contact Person** | Patricia A. P. Fisher<br>President & CEO |
| **Item 3 – Business Address** | 2 Omega Drive<br>Stamford, CT 06907 |
| **Item 4 – Telephone No.** | 203-251-0200 |
| **Item 5 – Email Address** | patfisher@janusassociates.com |
| **Item 6 – Fax No.** | 203-251-0222 |

# PART 2

## *Item 1 – Consultant Business Form*

1. Identify the Consultant's business or corporate structure:

| | |
|---|---|
| **Date and State of Incorporation** | JANUS Associates, Inc. was established December 16, 1988 in the State of Florida and incorporated as JANUS Software, Inc. on February 26, 1990 in the State of Florida |
| **List Names and Title of Executive Officers** | Patricia A. P. Fisher, President & CEO<br>Lyle A. Liberman, Chief Operating Officer |
| **Principal Place of Business** | 2 Omega Drive<br>Stamford, CT 06907 |
| **List all Related Principal or Subsidiary Corporations** | N/A |
| **Closed or Publicly Traded** | Closed |

| | |
|---|---|
| **EIN** | [Redacted] |

2. Identity the number of years your entity has been in business.

JANUS has been in business for over 32 years.

3. Identity whether your business/corporate structure has changed in the past five years and if yes, describe the change.

There have not been any changes to JANUS' corporate structure in the past five years.

4. Identity the type and coverage amount of all insurance policies.

JANUS maintains the following insurance policies:

- Internet Liability – Aggregate $5,000,000
- Cyber Liability – Aggregate $5,000,000
- Commercial General Liability – Each Occurrence $2,000,000; Medical Expenses $5,000; Personal & Adv. Injury $2,000,000; General Aggregate $4,000,000; Products - Comp/OP AGG $4,000,000
- Automobile Liability – Combined Single Limit $1,000,000; Underinsured Motorist $1,000,000
- Umbrella Liability/Excess Liability – Each Occurrence $5,000,000; Aggregate $5,000,000
- Workers' Compensation and Employers' Liability – E.L. Each Accident $1,000,000; E.L. Disease - EA Employee $1,000,000; E.L. Disease - Policy Limit $1,000,000
- Crime Discovery Basis – Employee Theft $1,000,000

5. Identified the name, address, and contract information for three (3) companies that the Consultant has performed similar services to those being sought by the Authority.

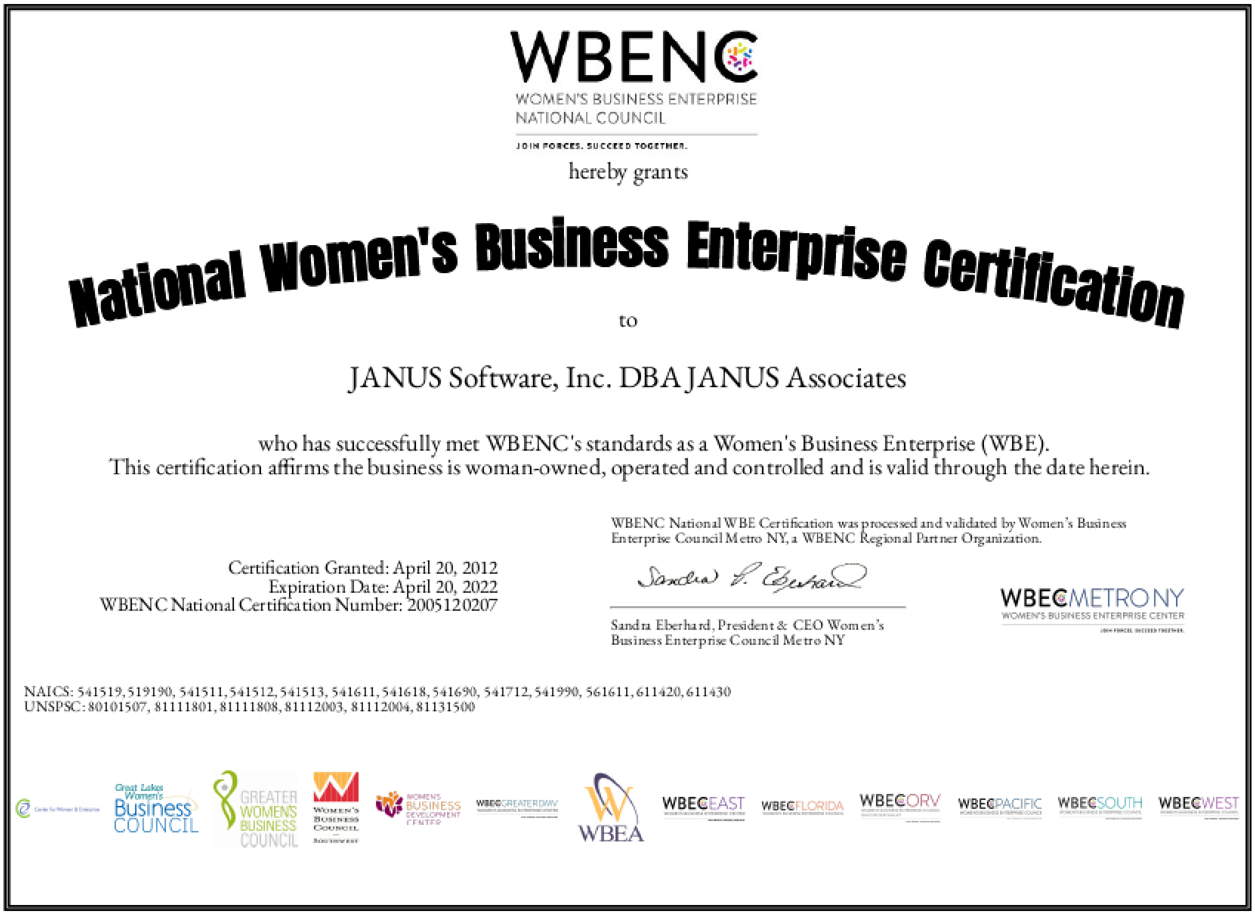
[Redacted]

[Redacted]

[Redacted]

6. If you are a certified, minority and/or women owned business, submit a copy of the certification.

JANUS has many certifications including a national WBENC certificate and will provide others upon request, including from New York City.



WBENC
WOMEN'S BUSINESS ENTERPRISE
NATIONAL COUNCIL
JOIN FORCES. SUCCEED TOGETHER.

hereby grants

National Women's Business Enterprise Certification

to

JANUS Software, Inc. DBA JANUS Associates

who has successfully met WBENC's standards as a Women's Business Enterprise (WBE).
This certification affirms the business is woman-owned, operated and controlled and is valid through the date herein.

Certification Granted: April 20, 2012
Expiration Date: April 20, 2022
WBENC National Certification Number: 2005120207

WBENC National WBE Certification was processed and validated by Women's Business Enterprise Council Metro NY, a WBENC Regional Partner Organization.

Sandra L. Eberhard

Sandra Eberhard, President & CEO Women's Business Enterprise Council Metro NY

WBEC METRO NY
WOMEN'S BUSINESS ENTERPRISE CENTER

NAICS: 541519, 519190, 541511, 541512, 541513, 541611, 541618, 541690, 541712, 541990, 561611, 611420, 611430
UNSPSC: 80101507, 81111801, 81111808, 81112003, 81112004, 81131500

## *Item 2 – Consultant Team*

Identify the individuals whose professional services will be utilized to undertake a comprehensive IT Cybersecurity Risk and Vulnerability Assessment, including thoroughly reviewing the current state of the Authority's information technology security, developing a vulnerability mitigation plan, and developing a prioritized road map of activities to enhance the Authority's future Cybersecurity position.

JANUS anticipates assigning the following personnel to this project (they are all JANUS employees). This is the type of project where experts are required, not simply consultants. Therefore, JANUS is proposing a dynamic group of highly skilled personnel who have participated in multiple information security projects that are similar to your request. Additional personnel will be added, if needed and with the Authority's approval, to fulfill requirements as needed, or to meet timing needs.

JANUS will not be utilizing any subcontractors for this project.

| Name and Place of Residence | Project Role | Scope of Responsibility | Length of Time with JANUS |
|---|---|---|---|
| Patricia Fisher<br>Stamford, CT | Executive Oversight | Oversight of the project | 32 Years |
| [Redacted]<br>West Hartford, CT | Project Manager | Project management | 22 Years |
| [Redacted]<br>Indian Trail, NC | Subject Matter Expert | Policy/process/program consulting | 8 Months |
| [Redacted]<br>Miami, FL | Subject Matter Expert | Technical consulting | 4 Years |
| [Redacted]<br>Severn, MD | Subject Matter Expert | Technical consulting | 5 Years |
| [Redacted]<br>Chesapeake, VA | Subject Matter Expert | Technical consulting | 8 Months |
| [Redacted]<br>Brick Township, NJ | Subject Matter Expert | Policy/process/program consulting | 3 Months |
| [Redacted]<br>Potomac, MD | Subject Matter Expert | Technical consulting | 3 Years |

### Executive Oversight

**Patricia Fisher** has a background of over 32 years of information security and technology involvement, including experience in both technical and management roles. She has designed applications, managed application design, managed IBM's accounting technology, directed large data centers for IBM, where she also served for several years as the Executive Assistant to IBM's Chief Information Officer and managed the Information Security & Business Continuity Programs for IBM's Latin American and Canadian sites. In 1988 she founded JANUS Associates, Inc., the first independent firm in the United States specializing in information risk management, Information Technology controls, security and business continuity for government and industry. Serving clients throughout the U.S. and internationally, she has a long history of providing strong leadership in the IT and security fields. She formerly served on the audit committee of the New York City Housing Authority as its IT and security expert; is on the Board of the Connecticut Technology Council; and serves as a member of the International Information Security Standards guidance board. Ms. Fisher holds both a B.A. (Maxwell School of Economics) and M.B.A. from Syracuse University and completed extensive post-masters work at Pennsylvania State University in Computer Science. She holds CGEIT (Certified in the Governance of Enterprise Information Technology) and CRISC (Certified in Risk of Information Security Controls) certifications from ISACA as well as the MBCI certification from the Business Continuity Institute.

Ms. Fisher will bring a strong executive oversight capability to the overall project and will focus on the Authority's needs while the Project Manager will focus on moving the tasks forward. She will conduct regular checkpoints with the on-site members of the team (and your staff as appropriate) to determine status, review risks, and understand possible issues. The JANUS Project Manager and Oversight Executive will also meet with your appropriate Project Manager as needed to discuss concerns (if any), where efficiencies may be incorporated, etc. to ensure that the JANUS team is undertaking what the Authority needs to result in a successful project.

### Project Management

[Redacted]

### Project Team

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

Note: Please see resumes provided on the following pages for relevant qualifications and experience, etc.

## Resumes

**Function and Specialization**
Executive Oversight Management

- IT Governance
- Project Management
- Strategic Analysis
- Risk Management
- Security Analysis/Assessment

**Clearance**
Top Secret Clearance – Inactive

**Representative Clients**
Commonwealth of Massachusetts
Centers for Medicare & Medicaid Services
Community Health Network of Connecticut
Commonwealth of Pennsylvania
Capital District Transportation Authority
City of Naperville (IL)
Wicomico County Public Schools (MD)
Travis County (TX)

**Certification(s)**
CGEIT – Certified in the Governance of Enterprise IT (ISACA)
CRISC – Certified in Risk and Information Security Controls (ISACA)
MBCI – Member, Business Continuity Institute

**Education**

# Patricia A. P. Fisher

**Background**
Ms. Fisher has 32 years with JANUS where she specializes in both the governance of Information Technology and information security and risk management projects, providing analysis and strategic advice to executive boards and leadership teams of JANUS' clients. Her time with JANUS was preceded by 11 years at IBM as Country Manager, Information Security & Business Continuity for Latin America and Canada. Prior to that she also managed large corporate Data Centers for IBM as well as large-scale application development projects. She has led a wide variety of projects over many years for government entities and not-for-profit customers, and is a highly sought after speaker and writer of articles. Ms. Fisher is a former member of the New York City Housing Authority's Audit Committee and served as the IT expert for the Committee.

**Experience**
**JANUS Software, Inc. (d/b/a JANUS Associates)** **December 1988 – Present**

- Completed security process improvement project for large transit authority.
- Performed CISO services for regional healthcare firm to assist it to drive needed security programs.
- Conducted high level strategic Information Technology review of state contractor firm to assist in developing budget, setting priorities, analyze staffing, and determine comprehensiveness of policies and procedures.
- Project oversight manager of Current-State/Future-State IT assessment for large state agency.
- Project oversight executive for major Independent Verification and Validation project for State Department of Revenue.
- Project oversight executive for information security contract for large federal healthcare organization.
- Advises senior executives at Fortune 100 companies and federal agencies on IT risk, staffing, and security initiatives.
- Led major corporate business and technology IT technical and business justification projects.
- Advised insurance clients on HIPAA, IT security requirements.
- Formulated and led team to design biometric identity management product.
- Designed Risk Management programs, methods for large organizations.
- Managed establishment of Risk Management program for federal agency.
- Advised senior security management of large financial institutions on corporate governance, organizational structure.

B.A., Economics, (Maxwell School) Syracuse University

M.B.A., Marketing, Syracuse University

Post Masters Computer Science and Doctoral Studies, Pennsylvania State University & State of New York at Albany

- Managed large information security projects for various public and private clients.
- Designed and provided executive and employee training throughout U.S. for large television/news organization.
- Defined and oversaw execution of technical IT business justification process for large commercial financial organization.
- Performed one-on-one executive information security tutoring for large corporations.
- Performed agency-wide information security strategic program review for large federal health agency.
- Defined information technology/security strategies for various large client organizations.
- Designed and performed information security training sessions for corporate clients.
- Developed standardized risk assessment evaluation methodology for federal healthcare agency.
- Managed general support system and application HIPAA system control assessment process for CMS.
- Led security risk assessments/penetration tests for major multi-national and government clients.
- Performed Business Impact Analyses for Fortune 100 corporations, large banks, brokerages.
- Led security penetration tests and vulnerability analyses for international and U.S. clients.
- Completed Disaster Recovery Plans to fulfill prime contractor requirements for federal agency systems.
- Performed security/recoverability audit for international bank.
- Advised clients on improvements in security awareness programs; developed tools/techniques for training.
- Developed software sensitivity certification and governance process for NASA's International Space Station project.
- Conducted certifications of adequacy of Commercial-off-the-shelf and custom software/systems to meet NASA security/recovery criteria for contractors.
- Managed security sensitivity certification process for large federal prime contractor.
- Designed continuity test plans for various clients and monitored test execution.
- Conducted risk analyses, policy and procedure development, education, business continuity planning for commercial and governmental organizations.
- Performed strategic security administration study for Fortune 100 insurance firm.

**International Business Machines, Inc. August 1977 – December 1988**
**Information Security Program Manager**

- Performed critical consulting role during planning and justification of major disaster recovery proposal that resulted in present IBM hot-site offering.
- Consulted with key international and domestic IBM customers regarding recovery needs, information security problems.
- Conducted U.S.-wide fraud audit resulting in criminal prosecution.
- Managed international information security program for IBM internal Latin American sites.
- Designed and conducted international training programs for information security initiatives.

- Advised senior level executives on country/site security status throughout Latin America and Canada.
- Directed short-term assignees from Latin countries.
- Supervised budget/financial aspects and risk management of international program.
- Developed measurement techniques to achieve proper level of control.
- Designed series of security metrics to measure improvements in IBM program.
- Developed strategic/business focus for America's Group advising on security and selling IBM approach.
- Structured disaster recovery offerings to market to key customers (domestic and Latin).
- Provided security consulting services for IBM key customers.
- Conducted customer educational seminars for senior executives, staffs and information security personnel.
- Managed multi-divisional financial planning, product inventory, and pricing applications.
- Managed financial accounting Information Technology services for largest IBM division.
- Performed technical assessment and final financial approval for multi-divisional capital requests (in excess of $230 million per quarter).
- Revised methodology for quarterly capital investment process resulting in release of dollars to the IBM divisions.
- Operated large headquarters data center, 107 staff upon completion of assignment (operations, systems support, networking, information center, etc.).
- Managed staffing reduction of 25% over three years while consistently achieving 99.9% availability with sub-second response to 1800 users.
- Directed planning requirements for new IBM major computer center site.
- Managed data center recovery programs.
- Divisional management of United Way campaign – achieving highest participation/contribution rate ever in IBM while managing to lowest expenditure in the entire corporation.
- Designed state-of-the-art computer command center off raised floor.

**Other Experience and Professional Accomplishments**

**Professional Education**

Goldman Sachs 10,000 Small Businesses Graduate

IBM President's Class

IBM Advanced Middle Manager's Class

IBM Advanced Business Institute

**Awards, Honors, Service**

Connecticut Technology Council Vice-Chair; Board of Directors (2011 – current); Chair of Cyber Security Committee (2013 – current)

Community Action Award (Volunteer of the Year), Connecticut Technology Council, December 2013.

Blue Ribbon Panel member for Criminal Justice curriculum, University of Saint Joseph (current).

Former Member, Audit Committee of the Board of Directors, New York City Housing Authority.

Finalist, Women of Innovation.

Outstanding Contribution Award, Fairfield County American Heart Association.

Outstanding Service Award, Fairfield County Cub Scouts.

Selected as national delegate to National Science Foundation special conference on the Role of Community Colleges in Cyber Security Education.

Committee member, Norwalk Community College, information security curriculum committee.

Chosen as national best practices committee member, Disaster Recovery Institute, Business Impact Analysis.

Chosen as national best practices committee member, Disaster Recovery Institute, Recovery Strategy.

President, Independent Computer Consultants, Fairfield/Westchester.

Outstanding Speaker Award, College and University Machine Records Conference.

**Selected Publications/Presentations**

Cyber Risk in Captive Insurance Organizations, 2014

Information Security Governance, Eastern European National Information Security Conference, Czech Republic, Keynote Speaker on information security governance and program maturity, 2013

Guest Lecturer on Information Security, Risk, and Governance: Boston University MBA Program, 2010

“HIPAA and HITECH Rules, The New World,” presentation and webinar, Stamford, CT, October 2009

“HITECH and Information Security” webinar, International Association of Outsourcing Professionals, July 2009

“Information Security in the American Recovery and Reinvestment Act and HITECH” presentation, May 2009

“Outsourcing in Today’s New Risk Averse Climate,” October 2008

“Information Security in the Power Industry” webinar, Large Public Power Utility Council, July 2007

“Power Industry Concerns” webinar to Chief Information Officers of major power producers in the U.S., July 2007

“Recovery and Security,” International Association of Outsourcers Conference, February 2006

Curriculum Advisory Committee, Norwalk Community College, 2003-2006

Keynote address, Information Security Conference, Norwalk Community College, April 2005

“Information Security Before 9/11 and After,” multiple presentations, 2002, 2003

“Securing Web Based Transactions,” E-Gov Conference, Tysons Corner, Virginia, March 2001

“Security Weaknesses in the Power Industry,” White Paper, October 2000

“Security Needs for E-Business,” American Public Power Association, Phoenix, October 2000

“What Penetration Studies Will Teach You,” ISACA, Orlando, Florida, July 2000

“Penetration Testing - Why Executives Just Don’t Get It,” CA-World, New Orleans, July 1999

“Millennium Mayhem,” Disaster Recovery Journal, August 1998

“The Realities of Conducting a Business Impact Analysis,” IBM Business Recovery Summit, San Francisco, May 1998

“Penetration Testing - Why Executives Just Don’t Get It,” CA-World, New Orleans, May 1998

“The Realities of Conducting a Business Impact Analysis,” Disaster Recovery Institute, Atlanta, September 1997

| | |
|---|---|
| | "Security Review of Netview," Internal Auditing Alert, June 1997<br>"Why computer System Penetration Tests Are Needed," Internal Auditing Alert, January 1997<br>"How to Conduct A Business Impact Analysis," Disaster Recovery Journal, Summer 1996<br>"Securing MVS," Chapter of Securing Client/Server Networks, McGraw-Hill, 1996<br>"How to Sell Security to Management," Computer Security Institute, November 1995<br>"Operating System Controls," Chapter of the Security Manager's Handbook, Auerbach Publishers, 1993<br>"Security and Controls Will Improve the Bottom Line," Security Management, May 1992<br>"Controlling Access: A Tiger-Team Approach," Crisis Magazine, January - February 1992<br>"Information Security in a Short-term Focused World," Crisis Magazine, January - February, 1991<br>**Selected Interviews/Appearances**<br>Regional News Network (RNN): Richard French Live, panel discussion regarding NSA Ruling, December 18, 2013<br>Radio Free Europe, "Viruses – Why People Write Them," January 30, 2004<br>Information Architect Newsletter, "Mainframe Connectivity to the Internet," February 4, 2002<br>WFDD Radio, "Cyber-terrorism," January 29, 2002<br>"Security & Business Continuity Since 9/11," Connecticut Bar Association, November 2001<br>ABC Radio, "Terrorism," September 11, 2001<br>Many other interviews and appearances, May 1995 - July 2001, details provided upon request. |

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

# PART 3

## *Item 1 – Proposed Scope of Service*

Describe the scope of service, which the Consultant would recommend to the Authority, to undertake a comprehensive IT Cybersecurity Risk and Vulnerability Assessment. The scope should include the following elements, along with such elements will be performed on-site or off-site:

(a) Review of current state of the Authority's information technology security,
(b) Development of a vulnerability mitigation plan,
(c) Development of a prioritized road map of activities to enhance the Authority's future Cybersecurity position,
(d) Best practice methodologies to ensure a standardized risk mitigation approach that will offer the highest risk reduction potential, complementing the "Framework for Improving Critical Infrastructure Cybersecurity", developed by the National Institute for Standards and Technology (NIST),
(e) Assessment that includes but not limited to:

- Test for susceptibility to Advanced Persistent Threats (APTs) such as viruses, malware, Trojan horses, botnets, and other targeted attack exploits.
- Evaluate the Authority's current threat posture including antivirus and Intrusion Detection and Prevention (IDP) capabilities.
- Evaluate the Authorities planned changes and improvements to the threat surface and assist identifying and addressing security concerns.
- Review the Authority's current Supervisory Control and Data Acquisition (SCADA) water systems for security vulnerabilities.
- Review wireless network system components for security vulnerabilities, validating system-specific operating systems and firmware versions for known exploits and recommend upgrades, updates, and mitigations.
- Review current system-specific operating systems and firmware versions for known exploits and recommend upgrades, updates, and mitigations. This includes firewalls, switches and routers, Microsoft Active Directory, email and file servers, web servers, wireless routers, WAN, VPN, VoIP, and CCTV systems.
- Assess VoIP network system components for security vulnerabilities, validating system-specific operating system and firmware versions and reviewing for known exploits.
- Review existing IT policies and procedures and make recommendations for changes and/or additional policy and procedure development.
- Execute and review internal network vulnerability scans and external vulnerability and penetration scans and make recommendations to reduce the threat attack surface.
- Recommend or assist in selection of vulnerability scan software for purchase/license for continued use by the Authority after the assessment is complete.

## *Overview*

You have requested a comprehensive IT cybersecurity risk and vulnerability assessment, producing a current state of the information technology security, a vulnerability mitigation plan, and development of a prioritized Roadmap. That is exactly the type of work that JANUS does every week for our clients. We regularly work in NIST as well as all the frameworks, methodologies, and standards that are currently utilized.

We also regularly develop System Security Plans (SSP) as well as Plans of Action & Milestones (POA&Ms) and Roadmaps to guide progress on your goals, as required by your Request for Proposal (RFP). We have many clients who can attest to our assessments and the value they bring to helping you determine what you need to embark upon to achieve your security goals. Because our staff has so many years of experience, they have significant expertise in understanding what you need to protect and where you might be having issues.

Our reports are clear and concise. We provide executive summaries that are graphical to provide a quick overview of what executives need to be concerned with and we also present highly detailed findings and recommendations that will lead technical people to correct conclusions about remediation steps that should be undertaken.

## *JANUS' Approach and Methodology*

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

### Blended Methodology

[Redacted]

## Team Effort and Knowledge Transfer

We consider each engagement a team effort; i.e., an effort shared by us and our client. We will work diligently to ensure that we impart as much knowledge to Authority staff as we can during the project period so that the on-going value of the project is even greater than anticipated. This has been a highly successful strategy for our clients in the past. We believe knowledge transfer is an important component of our work.

[Redacted]

[Redacted]

[*]

[Redacted]

## Technical Currency and Results

[Redacted]

[*] We will provide a suggested format.

[Redacted]

[Redacted]

### Non-Destructive Analysis

[Redacted]

### Testing

[Redacted]

[Redacted]

[Redacted]

[Redacted]

### Manual Verification

[Redacted]

1

## *Preliminary Activities*

[Redacted]

### *Pre-Kickoff*

[Redacted]

[Redacted]

### ***Kickoff Meeting***

[Redacted]

### ***Post-kickoff Activities***

[Redacted]

Any open questions are typically addressed within three days of the kickoff meeting.  At that point we will finalize our plan and be deep into preparation.

### Communications Plan

[Redacted]

## *Targeted Attack Exploits*

[Redacted]

### *Approach*

[Redacted]

[Redacted]

## *Evaluating Changes*

We will examine your planned changes to the threat surface and provide you with our recommendations regarding these improvements and changes. As part of the deliverables, we will also focus on identifying and discussing how you can address your security concerns.

## *Internal Assessment*

[Redacted]

[Redacted]

[Redacted]

## *Wireless Assessment*

[Redacted]

[Redacted]

## Voice over Internet Protocol (VoIP)

[Redacted]

[Redacted]

## *Policy and Procedure Review*

[Redacted]

## *Item 2 – Hardware and Software Requirements*

(a) Describe the required hardware and/or software necessary to implement Consultant's plan, if any.
(b) Describe the limitations of the service and/or equipment, if any.
(c) Identify whether the required hardware and/or software will be provided by Consultant or the Authority.

[Redacted]

## Item 3 – Timeframe for Deliverables

Provide a timeframe for completing the following deliverables:

1. Project Management Deliverables:
   (a) Work Breakdown Schedule (WBS) including tasks,
   (b) Schedule and dependencies, and
   (c) Weekly Status Reports including risks and progress reports.
2. Report: A written report documenting:
   (a) Executive summary detailing the Authority's Cybersecurity position, including a comparative scorecard of findings,
   (b) Results of vulnerability testing performed,
   (c) Identified cybersecurity vulnerabilities, gaps, and mitigation plans,
   (d) A prioritized road map of activities, developed in conjunction with Authority's IT staff to enhance the Authority's future cybersecurity position.

### Deliverables

[Redacted]

## ***Assessment Draft Details***

[Redacted]

[Redacted]

[Redacted]

## ***Report Summaries***

[Redacted]

[Redacted]

[Redacted]

***Technical Detail Report***

[Redacted]

[Redacted]

### ***Status Reports***

[Redacted]

### ***Form of the Deliverables***

[Redacted]

### ***Plan of Actions and Milestones (POA&M)/Roadmap***

[Redacted]

## Projected Solutions and Costs

3. Projected solutions and costs:

(a) Provide an estimated range, based upon previous experience, of the total services costs to implement the proposed solutions,
(b) Include a Rate Sheet that specifies and itemizes the cost for each proposed component, including all licensing, support, maintenance, and hosting fees, and
(c) For subscription-based services, provide annual pricing.

We have provided an estimated project plan illustrating how we anticipate that the project might take place. This can be adjusted, based on your needs, but it should provide a view of how similar projects have proceeded, based on our years of experience and the detailed level of work that today's environments require.

We utilize a blended rate structure of $165.00/hour for the subject matter experts and management and $145.00/hour for quality assurance.

Please see the estimated project plan below for our estimated total service costs. Itemization is included in the project plan. Since no travel is required, we have added not travel costs.

## *Item 4 – Price Structure*

### Detailed Description of Price Structure

1. Provided a detailed description of the Consultant price structure or pricing option for the services to be provided by the Consultant.

| | Task Name | Work | Start | Finish | Cost | Predecessors |
|---|---|---|---|---|---|---|
| **1** | | **272.5 hrs** | **Mon 7/12/21** | **Tue 8/31/21** | **$44,902.49** | |
| 2 | | 0 hrs | Mon 7/12/21 | Mon 7/12/21 | $0.00 | |
| **3** | | **53 hrs** | **Mon 7/12/21** | **Wed 7/21/21** | **$8,745.00** | |
| **4** | | **4 hrs** | **Mon 7/12/21** | **Tue 7/13/21** | **$660.00** | |
| 5 | | 4 hrs | Mon 7/12/21 | Tue 7/13/21 | $660.00 | 2 |
| **6** | | **49 hrs** | **Tue 7/13/21** | **Wed 7/21/21** | **$8,085.00** | |
| 7 | | 6 hrs | Tue 7/13/21 | Wed 7/14/21 | $990.00 | 5 |
| 8 | | 1 hr | Wed 7/14/21 | Wed 7/14/21 | $165.00 | 7 |
| 9 | [REDACTED} | 6 hrs | Wed 7/14/21 | Thu 7/15/21 | $990.00 | 8 |
| 10 | | 4 hrs | Thu 7/15/21 | Thu 7/15/21 | $660.00 | 9 |
| 11 | | 8 hrs | Thu 7/15/21 | Fri 7/16/21 | $1,320.00 | 10 |
| 12 | | 10 hrs | Fri 7/16/21 | Mon 7/19/21 | $1,650.00 | 11 |
| 13 | | 8 hrs | Mon 7/19/21 | Tue 7/20/21 | $1,320.00 | 12 |
| 14 | | 2 hrs | Tue 7/20/21 | Wed 7/21/21 | $330.00 | 13 |
| 15 | | 4 hrs | Wed 7/21/21 | Wed 7/21/21 | $660.00 | 14 |
| **16** | | **156 hrs** | **Wed 7/21/21** | **Wed 8/18/21** | **$25,740.00** | |
| **17** | | **11 hrs** | **Mon 7/26/21** | **Fri 7/30/21** | **$1,815.00** | |
| 18 | | 0 hrs | Mon 7/26/21 | Tue 7/27/21 | $0.00 | 30 |
| 19 | | 0 hrs | Tue 7/27/21 | Wed 7/28/21 | $0.00 | 18 |
| 20 | | 5 hrs | Wed 7/28/21 | Thu 7/29/21 | $825.00 | 19 |
| 21 | | 6 hrs | Thu 7/29/21 | Fri 7/30/21 | $990.00 | 20 |
| 22 | | 4 hrs | Wed 7/21/21 | Thu 7/22/21 | $660.00 | 15 |
| 23 | | 6 hrs | Fri 7/30/21 | Fri 7/30/21 | $990.00 | 21 |
| 24 | | 12 hrs | Wed 7/21/21 | Thu 7/22/21 | $1,980.00 | 14 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 25 | | 2 hrs | Thu 7/22/21 | Thu 7/22/21 | $330.00 | 24 |
| 26 | | 2 hrs | Thu 7/22/21 | Fri 7/23/21 | $330.00 | 25 |
| 27 | | 4 hrs | Fri 7/23/21 | Fri 7/23/21 | $660.00 | 26 |
| 28 | | 1 hr | Fri 7/23/21 | Fri 7/23/21 | $165.00 | 27 |
| 29 | | 4 hrs | Fri 7/23/21 | Mon 7/26/21 | $660.00 | 28 |
| 30 | | 4 hrs | Mon 7/26/21 | Mon 7/26/21 | $660.00 | 29 |
| **31** | | **20 hrs** | **Fri 7/30/21** | **Wed 8/4/21** | **$3,300.00** | |
| 32 | | 4 hrs | Fri 7/30/21 | Mon 8/2/21 | $660.00 | 23,21 |
| 33 | | 2 hrs | Mon 8/2/21 | Mon 8/2/21 | $330.00 | 32 |
| 34 | | 4 hrs | Mon 8/2/21 | Tue 8/3/21 | $660.00 | 33 |
| 35 | | 8 hrs | Tue 8/3/21 | Wed 8/4/21 | $1,320.00 | 34 |
| 36 | | 0 hrs | Wed 8/4/21 | Wed 8/4/21 | $0.00 | 35 |
| 37 | | 2 hrs | Wed 8/4/21 | Wed 8/4/21 | $330.00 | 36 |
| **38** | | **28 hrs** | **Wed 8/4/21** | **Mon 8/9/21** | **$4,620.00** | |
| 39 | | 5 hrs | Wed 8/4/21 | Wed 8/4/21 | $825.00 | 37 |
| 40 | | 16 hrs | Thu 8/5/21 | Fri 8/6/21 | $2,640.00 | 39 |
| 41 | | 2 hrs | Mon 8/9/21 | Mon 8/9/21 | $330.00 | 40 |
| 42 | | 5 hrs | Mon 8/9/21 | Mon 8/9/21 | $825.00 | 41 |
| **43** | | **10 hrs** | **Mon 8/9/21** | **Wed 8/11/21** | **$1,650.00** | |
| 44 | | 4 hrs | Mon 8/9/21 | Tue 8/10/21 | $660.00 | 42 |
| 45 | [REDACTED] | 6 hrs | Tue 8/10/21 | Wed 8/11/21 | $990.00 | 44 |
| 46 | | 4 hrs | Wed 8/11/21 | Wed 8/11/21 | $660.00 | 45 |
| **47** | | **40 hrs** | **Wed 8/11/21** | **Wed 8/18/21** | **$6,600.00** | |
| 48 | | 4 hrs | Wed 8/11/21 | Thu 8/12/21 | $660.00 | 46 |
| 49 | | 4 hrs | Thu 8/12/21 | Thu 8/12/21 | $660.00 | 48 |
| 50 | | 6 hrs | Thu 8/12/21 | Fri 8/13/21 | $990.00 | 49 |
| 51 | | 4 hrs | Fri 8/13/21 | Fri 8/13/21 | $660.00 | 50 |
| 52 | | 6 hrs | Fri 8/13/21 | Mon 8/16/21 | $990.00 | 51 |
| 53 | | 16 hrs | Mon 8/16/21 | Wed 8/18/21 | $2,640.00 | 52 |
| **54** | | **2 hrs** | **Thu 8/12/21** | **Thu 8/12/21** | **$330.00** | |
| 55 | | 0 hrs | Thu 8/12/21 | Thu 8/12/21 | $0.00 | 48 |
| 56 | | 2 hrs | Thu 8/12/21 | Thu 8/12/21 | $330.00 | 55 |
| 57 | | 2 hrs | Thu 8/12/21 | Thu 8/12/21 | $330.00 | 56 |
| **58** | | **48.5 hrs** | **Thu 8/12/21** | **Tue 8/31/21** | **$7,942.50** | |
| 59 | | 22 hrs | Thu 8/12/21 | Tue 8/17/21 | $3,630.00 | 57 |
| 60 | | 6 hrs | Tue 8/17/21 | Wed 8/18/21 | $990.00 | 59 |
| **61** | | **20.5 hrs** | **Wed 8/18/21** | **Tue 8/31/21** | **$3,322.50** | |
| 62 | | 6 hrs | Wed 8/18/21 | Wed 8/18/21 | $990.00 | 60 |
| 63 | | 2 hrs | Wed 8/18/21 | Thu 8/19/21 | $290.00 | 62 |
| 64 | | 1 hr | Thu 8/19/21 | Thu 8/19/21 | $165.00 | 63 |
| 65 | | 8 hrs | Thu 8/19/21 | Thu 8/19/21 | $1,320.00 | 64 |
| 66 | | 0 hrs | Thu 8/26/21 | Fri 8/27/21 | $0.00 | 64FS+5 days |
| 67 | | 2 hrs | Fri 8/27/21 | Fri 8/27/21 | $330.00 | 66 |
| 68 | | 1 hr | Fri 8/27/21 | Fri 8/27/21 | $145.00 | 67 |
| 69 | | 0.5 hrs | Fri 8/27/21 | Tue 8/31/21 | $82.50 | 68 |
| **70** | | **15 hrs** | **Fri 7/30/21** | **Tue 8/31/21** | **$2,474.99** | |
| 71 | | 6 hrs | Fri 7/30/21 | Thu 8/12/21 | $990.00 | 17 |
| 72 | | 8 hrs | Fri 7/30/21 | Mon 8/16/21 | $1,319.99 | 17 |
| 73 | | 1 hr | Tue 8/31/21 | Tue 8/31/21 | $165.00 | 69 |

## Invoicing

Invoicing for the assessment is requested as follows:

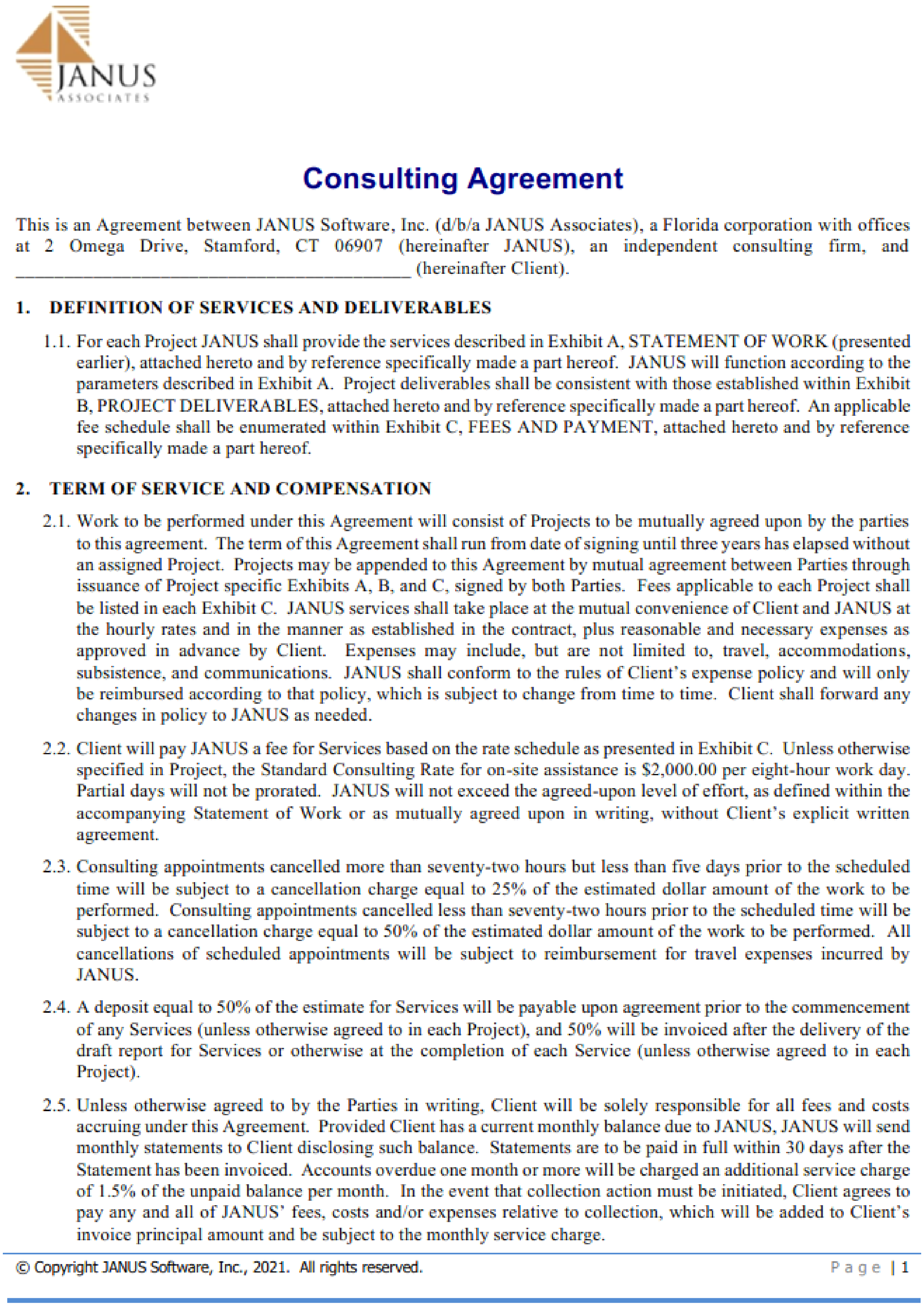
30% upon completion of the preparation period
50% upon completion of the field work
15% upon submission of the draft report
5% upon submission of the final report

### Payment Terms

1% discount on fees if paid in 10 days.  Net 30.

### JANUS' Consulting Agreement

2. If the Consultant has a standardize agreement used for such services, include a copy with the Proposal.



JANUS
ASSOCIATES

## Consulting Agreement

This is an Agreement between JANUS Software, Inc. (d/b/a JANUS Associates), a Florida corporation with offices at 2 Omega Drive, Stamford, CT 06907 (hereinafter JANUS), an independent consulting firm, and ________________________________________ (hereinafter Client).

**1. DEFINITION OF SERVICES AND DELIVERABLES**

1.1. For each Project JANUS shall provide the services described in Exhibit A, STATEMENT OF WORK (presented earlier), attached hereto and by reference specifically made a part hereof. JANUS will function according to the parameters described in Exhibit A. Project deliverables shall be consistent with those established within Exhibit B, PROJECT DELIVERABLES, attached hereto and by reference specifically made a part hereof. An applicable fee schedule shall be enumerated within Exhibit C, FEES AND PAYMENT, attached hereto and by reference specifically made a part hereof.

**2. TERM OF SERVICE AND COMPENSATION**

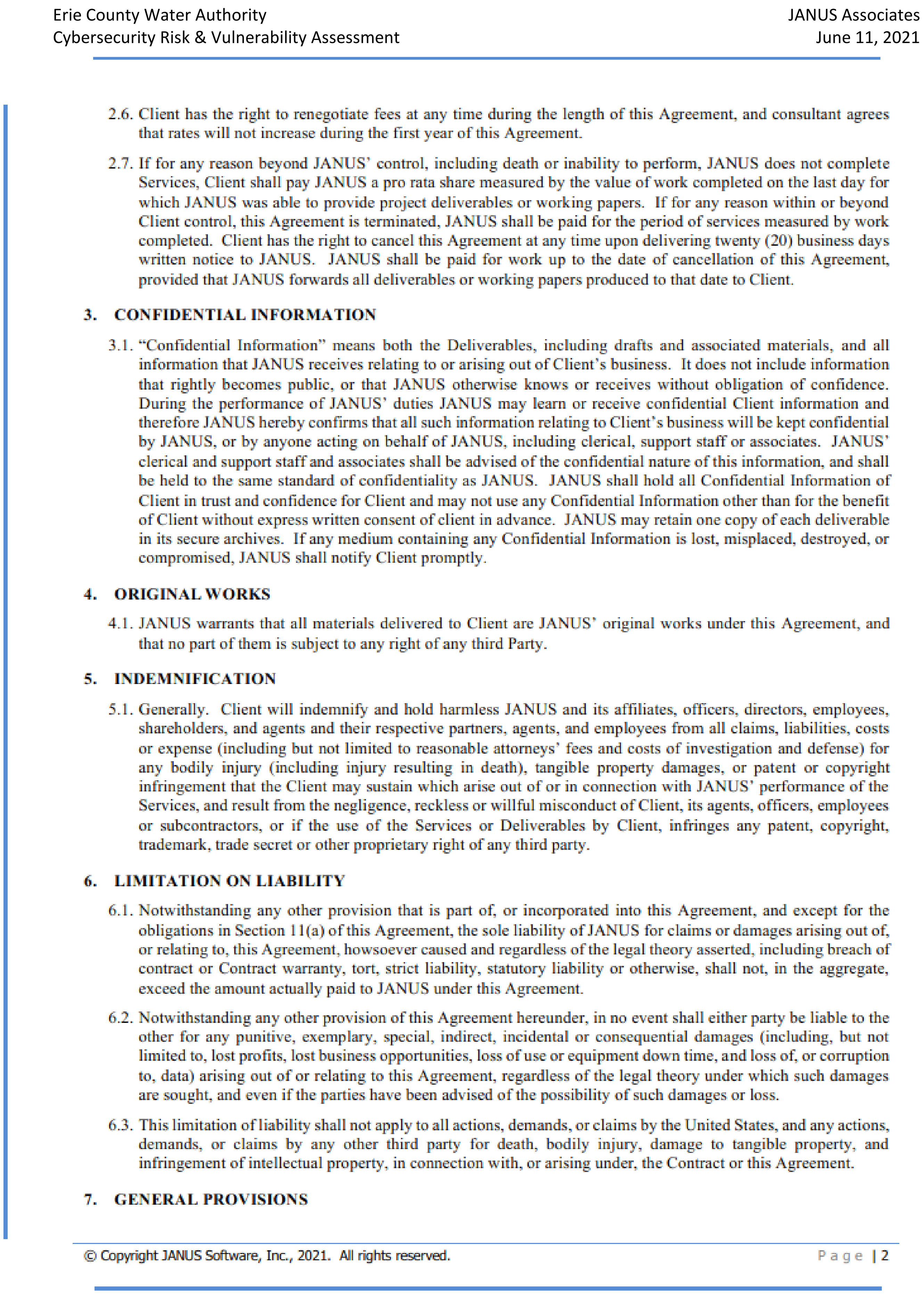
2.1. Work to be performed under this Agreement will consist of Projects to be mutually agreed upon by the parties to this agreement. The term of this Agreement shall run from date of signing until three years has elapsed without an assigned Project. Projects may be appended to this Agreement by mutual agreement between Parties through issuance of Project specific Exhibits A, B, and C, signed by both Parties. Fees applicable to each Project shall be listed in each Exhibit C. JANUS services shall take place at the mutual convenience of Client and JANUS at the hourly rates and in the manner as established in the contract, plus reasonable and necessary expenses as approved in advance by Client. Expenses may include, but are not limited to, travel, accommodations, subsistence, and communications. JANUS shall conform to the rules of Client's expense policy and will only be reimbursed according to that policy, which is subject to change from time to time. Client shall forward any changes in policy to JANUS as needed.

2.2. Client will pay JANUS a fee for Services based on the rate schedule as presented in Exhibit C. Unless otherwise specified in Project, the Standard Consulting Rate for on-site assistance is $2,000.00 per eight-hour work day. Partial days will not be prorated. JANUS will not exceed the agreed-upon level of effort, as defined within the accompanying Statement of Work or as mutually agreed upon in writing, without Client's explicit written agreement.

2.3. Consulting appointments cancelled more than seventy-two hours but less than five days prior to the scheduled time will be subject to a cancellation charge equal to 25% of the estimated dollar amount of the work to be performed. Consulting appointments cancelled less than seventy-two hours prior to the scheduled time will be subject to a cancellation charge equal to 50% of the estimated dollar amount of the work to be performed. All cancellations of scheduled appointments will be subject to reimbursement for travel expenses incurred by JANUS.

2.4. A deposit equal to 50% of the estimate for Services will be payable upon agreement prior to the commencement of any Services (unless otherwise agreed to in each Project), and 50% will be invoiced after the delivery of the draft report for Services or otherwise at the completion of each Service (unless otherwise agreed to in each Project).

2.5. Unless otherwise agreed to by the Parties in writing, Client will be solely responsible for all fees and costs accruing under this Agreement. Provided Client has a current monthly balance due to JANUS, JANUS will send monthly statements to Client disclosing such balance. Statements are to be paid in full within 30 days after the Statement has been invoiced. Accounts overdue one month or more will be charged an additional service charge of 1.5% of the unpaid balance per month. In the event that collection action must be initiated, Client agrees to pay any and all of JANUS' fees, costs and/or expenses relative to collection, which will be added to Client's invoice principal amount and be subject to the monthly service charge.



2.6. Client has the right to renegotiate fees at any time during the length of this Agreement, and consultant agrees that rates will not increase during the first year of this Agreement.

2.7. If for any reason beyond JANUS' control, including death or inability to perform, JANUS does not complete Services, Client shall pay JANUS a pro rata share measured by the value of work completed on the last day for which JANUS was able to provide project deliverables or working papers. If for any reason within or beyond Client control, this Agreement is terminated, JANUS shall be paid for the period of services measured by work completed. Client has the right to cancel this Agreement at any time upon delivering twenty (20) business days written notice to JANUS. JANUS shall be paid for work up to the date of cancellation of this Agreement, provided that JANUS forwards all deliverables or working papers produced to that date to Client.

## 3. CONFIDENTIAL INFORMATION

3.1. "Confidential Information" means both the Deliverables, including drafts and associated materials, and all information that JANUS receives relating to or arising out of Client's business. It does not include information that rightly becomes public, or that JANUS otherwise knows or receives without obligation of confidence. During the performance of JANUS' duties JANUS may learn or receive confidential Client information and therefore JANUS hereby confirms that all such information relating to Client's business will be kept confidential by JANUS, or by anyone acting on behalf of JANUS, including clerical, support staff or associates. JANUS' clerical and support staff and associates shall be advised of the confidential nature of this information, and shall be held to the same standard of confidentiality as JANUS. JANUS shall hold all Confidential Information of Client in trust and confidence for Client and may not use any Confidential Information other than for the benefit of Client without express written consent of client in advance. JANUS may retain one copy of each deliverable in its secure archives. If any medium containing any Confidential Information is lost, misplaced, destroyed, or compromised, JANUS shall notify Client promptly.

## 4. ORIGINAL WORKS

4.1. JANUS warrants that all materials delivered to Client are JANUS' original works under this Agreement, and that no part of them is subject to any right of any third Party.

## 5. INDEMNIFICATION

5.1. Generally. Client will indemnify and hold harmless JANUS and its affiliates, officers, directors, employees, shareholders, and agents and their respective partners, agents, and employees from all claims, liabilities, costs or expense (including but not limited to reasonable attorneys' fees and costs of investigation and defense) for any bodily injury (including injury resulting in death), tangible property damages, or patent or copyright infringement that the Client may sustain which arise out of or in connection with JANUS' performance of the Services, and result from the negligence, reckless or willful misconduct of Client, its agents, officers, employees or subcontractors, or if the use of the Services or Deliverables by Client, infringes any patent, copyright, trademark, trade secret or other proprietary right of any third party.

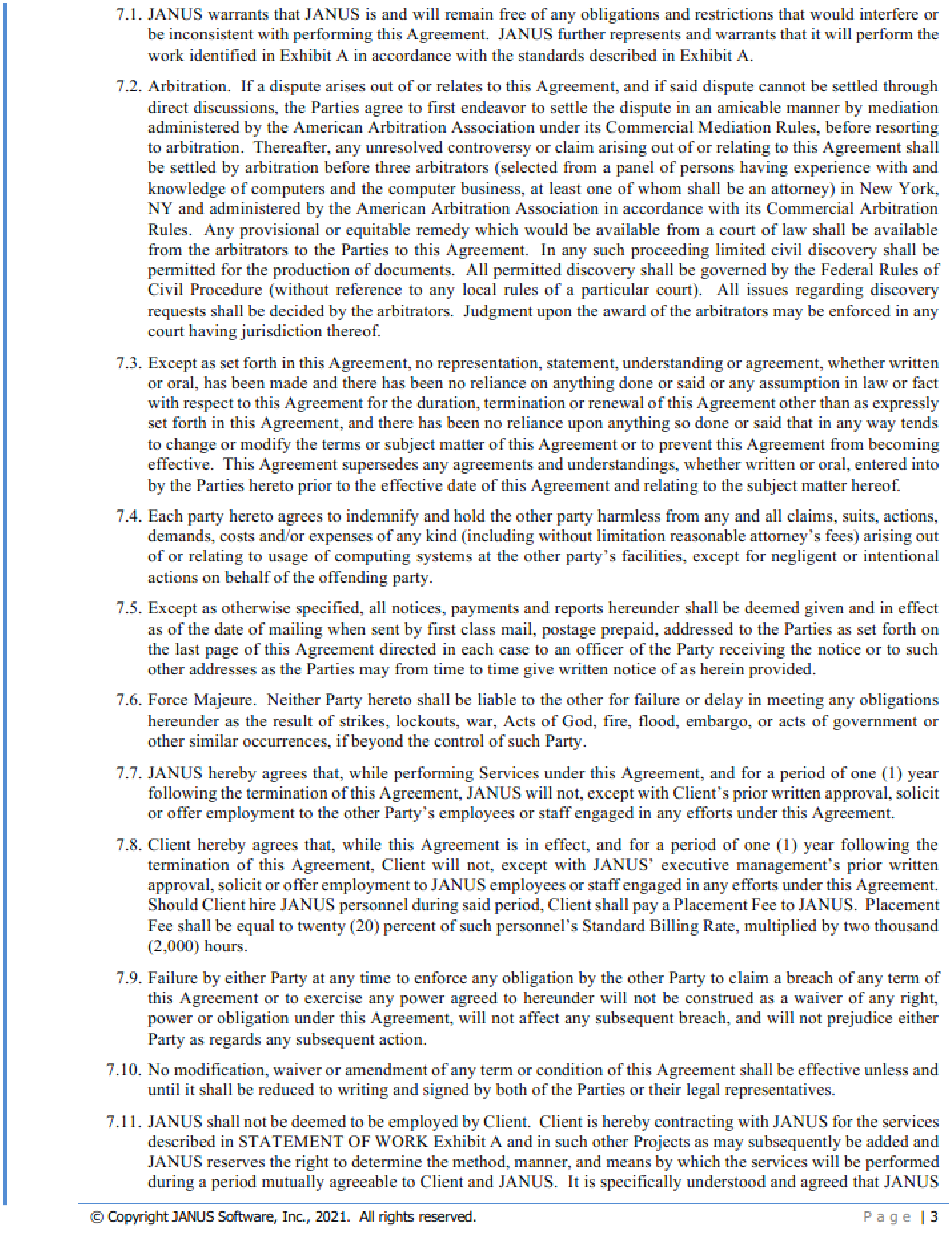
## 6. LIMITATION ON LIABILITY

6.1. Notwithstanding any other provision that is part of, or incorporated into this Agreement, and except for the obligations in Section 11(a) of this Agreement, the sole liability of JANUS for claims or damages arising out of, or relating to, this Agreement, howsoever caused and regardless of the legal theory asserted, including breach of contract or Contract warranty, tort, strict liability, statutory liability or otherwise, shall not, in the aggregate, exceed the amount actually paid to JANUS under this Agreement.

6.2. Notwithstanding any other provision of this Agreement hereunder, in no event shall either party be liable to the other for any punitive, exemplary, special, indirect, incidental or consequential damages (including, but not limited to, lost profits, lost business opportunities, loss of use or equipment down time, and loss of, or corruption to, data) arising out of or relating to this Agreement, regardless of the legal theory under which such damages are sought, and even if the parties have been advised of the possibility of such damages or loss.

6.3. This limitation of liability shall not apply to all actions, demands, or claims by the United States, and any actions, demands, or claims by any other third party for death, bodily injury, damage to tangible property, and infringement of intellectual property, in connection with, or arising under, the Contract or this Agreement.

## 7. GENERAL PROVISIONS



7.1. JANUS warrants that JANUS is and will remain free of any obligations and restrictions that would interfere or be inconsistent with performing this Agreement. JANUS further represents and warrants that it will perform the work identified in Exhibit A in accordance with the standards described in Exhibit A.

7.2. Arbitration. If a dispute arises out of or relates to this Agreement, and if said dispute cannot be settled through direct discussions, the Parties agree to first endeavor to settle the dispute in an amicable manner by mediation administered by the American Arbitration Association under its Commercial Mediation Rules, before resorting to arbitration. Thereafter, any unresolved controversy or claim arising out of or relating to this Agreement shall be settled by arbitration before three arbitrators (selected from a panel of persons having experience with and knowledge of computers and the computer business, at least one of whom shall be an attorney) in New York, NY and administered by the American Arbitration Association in accordance with its Commercial Arbitration Rules. Any provisional or equitable remedy which would be available from a court of law shall be available from the arbitrators to the Parties to this Agreement. In any such proceeding limited civil discovery shall be permitted for the production of documents. All permitted discovery shall be governed by the Federal Rules of Civil Procedure (without reference to any local rules of a particular court). All issues regarding discovery requests shall be decided by the arbitrators. Judgment upon the award of the arbitrators may be enforced in any court having jurisdiction thereof.

7.3. Except as set forth in this Agreement, no representation, statement, understanding or agreement, whether written or oral, has been made and there has been no reliance on anything done or said or any assumption in law or fact with respect to this Agreement for the duration, termination or renewal of this Agreement other than as expressly set forth in this Agreement, and there has been no reliance upon anything so done or said that in any way tends to change or modify the terms or subject matter of this Agreement or to prevent this Agreement from becoming effective. This Agreement supersedes any agreements and understandings, whether written or oral, entered into by the Parties hereto prior to the effective date of this Agreement and relating to the subject matter hereof.

7.4. Each party hereto agrees to indemnify and hold the other party harmless from any and all claims, suits, actions, demands, costs and/or expenses of any kind (including without limitation reasonable attorney's fees) arising out of or relating to usage of computing systems at the other party's facilities, except for negligent or intentional actions on behalf of the offending party.

7.5. Except as otherwise specified, all notices, payments and reports hereunder shall be deemed given and in effect as of the date of mailing when sent by first class mail, postage prepaid, addressed to the Parties as set forth on the last page of this Agreement directed in each case to an officer of the Party receiving the notice or to such other addresses as the Parties may from time to time give written notice of as herein provided.

7.6. Force Majeure. Neither Party hereto shall be liable to the other for failure or delay in meeting any obligations hereunder as the result of strikes, lockouts, war, Acts of God, fire, flood, embargo, or acts of government or other similar occurrences, if beyond the control of such Party.

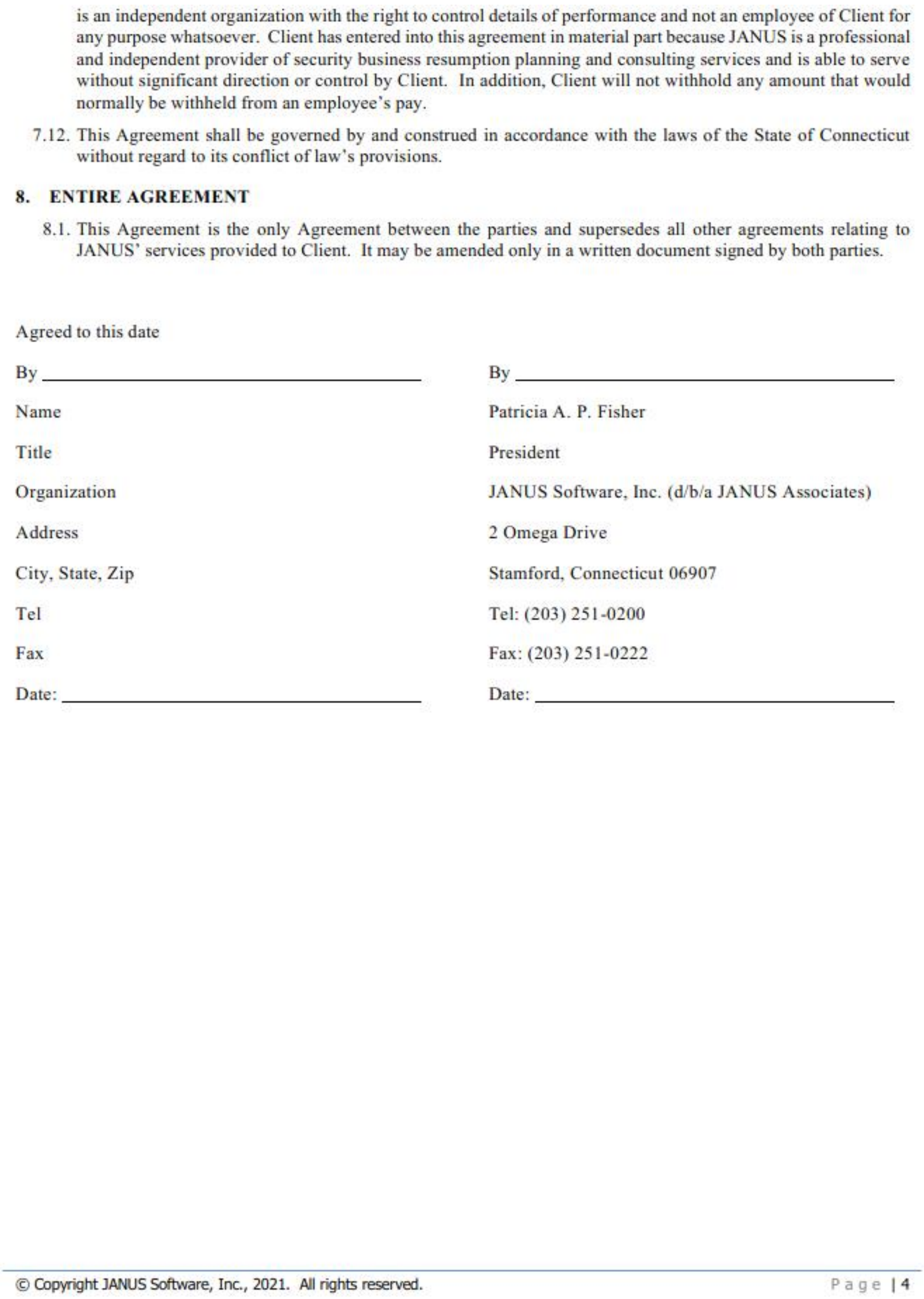
7.7. JANUS hereby agrees that, while performing Services under this Agreement, and for a period of one (1) year following the termination of this Agreement, JANUS will not, except with Client's prior written approval, solicit or offer employment to the other Party's employees or staff engaged in any efforts under this Agreement.

7.8. Client hereby agrees that, while this Agreement is in effect, and for a period of one (1) year following the termination of this Agreement, Client will not, except with JANUS' executive management's prior written approval, solicit or offer employment to JANUS employees or staff engaged in any efforts under this Agreement. Should Client hire JANUS personnel during said period, Client shall pay a Placement Fee to JANUS. Placement Fee shall be equal to twenty (20) percent of such personnel's Standard Billing Rate, multiplied by two thousand (2,000) hours.

7.9. Failure by either Party at any time to enforce any obligation by the other Party to claim a breach of any term of this Agreement or to exercise any power agreed to hereunder will not be construed as a waiver of any right, power or obligation under this Agreement, will not affect any subsequent breach, and will not prejudice either Party as regards any subsequent action.

7.10. No modification, waiver or amendment of any term or condition of this Agreement shall be effective unless and until it shall be reduced to writing and signed by both of the Parties or their legal representatives.

7.11. JANUS shall not be deemed to be employed by Client. Client is hereby contracting with JANUS for the services described in STATEMENT OF WORK Exhibit A and in such other Projects as may subsequently be added and JANUS reserves the right to determine the method, manner, and means by which the services will be performed during a period mutually agreeable to Client and JANUS. It is specifically understood and agreed that JANUS



is an independent organization with the right to control details of performance and not an employee of Client for any purpose whatsoever. Client has entered into this agreement in material part because JANUS is a professional and independent provider of security business resumption planning and consulting services and is able to serve without significant direction or control by Client. In addition, Client will not withhold any amount that would normally be withheld from an employee's pay.

7.12. This Agreement shall be governed by and construed in accordance with the laws of the State of Connecticut without regard to its conflict of law's provisions.

## 8. ENTIRE AGREEMENT

8.1. This Agreement is the only Agreement between the parties and supersedes all other agreements relating to JANUS' services provided to Client. It may be amended only in a written document signed by both parties.

Agreed to this date

| | |
|---|---|
| By ______________________________ | By ______________________________ |
| Name | Patricia A. P. Fisher |
| Title | President |
| Organization | JANUS Software, Inc. (d/b/a JANUS Associates) |
| Address | 2 Omega Drive |
| City, State, Zip | Stamford, Connecticut 06907 |
| Tel | Tel: (203) 251-0200 |
| Fax | Fax: (203) 251-0222 |
| Date: ____________________________ | Date: ____________________________ |

## QUALIFICATIONS AND EXPERIENCE

Founded in 1988, JANUS is America's longest operating information risk management and IT security firm. JANUS serves a wide range of clients in government, utility, healthcare, education, and industry and brings the best practices of all sectors to our projects. JANUS is a privately held, woman-owned small business (WOSB) headquartered in Stamford, CT with additional locations in West Hartford, CT; Brick Township, NJ; Baltimore, MD; Washington, D.C. area; Charlotte, NC; Miami, FL; and Lubbock, TX.

Although we are certified by a variety of state and local government bodies as a woman-owned, small business we have remained in business for over 32 years due to the excellence of our offerings, our dedication to our clients, our vendor neutral results, our flexibility to meet evolving customer needs, and our ability to compete with the largest security organizations to bring needed solutions to our customers. We have focused on information security, forensics, security engineering, business resilience, and associated services as our core business since our founding and possess the depth and experience required to fulfill the Authority's requirements for this project and into the future.

As an independent organization that focuses on risk, information security, and penetration testing, we have a natural affinity to protect our clients and bring improvements to your business processes –all designed to help you achieve excellence. We have provided similar services for multiple water companies and energy organizations and so, have a good understanding of the type of environment and Supervisory Control and Data Acquisition (SCADA) needs that you have. We are specialists in Information Technology (IT) and risk assessment and as such, we understand that helping the Authority discover risks early and then making practical recommendations for mitigating them is one of the best ways we can add value to your business and protect it. We have broad experience across numerous utility and municipal, state and federal government entities, as well as educational, commercial, and transportation entities, and we believe our values and skill sets will exceed the Authority's expectations for this project.

[Redacted]

[Redacted]

A benefit of our projects is the high-quality level of the results, including our reports. We are well regarded for our reports which include sections written in plain English to help foster understanding for those who are not technically inclined. While all consulting firms position themselves as providing high quality, we have formal client feedback and independent evaluations that reinforce this concept. This translates into a high return on investment for the Authority.

To provide a clearer understanding of JANUS' relationship with our clients and our thorough deliverables, we include the following quotes from comments by our clients.

JANUS clients were asked to rate our knowledge and expertise (**10 = best; 1 = worst**):

### Wyoming State Agency

**Question #/Question** **Rating**

| | |
|---|---|
| 2. Rate the firm's knowledge and expertise. | **RATING: 10** |
| **Comments:** JANUS has demonstrated its subject matter expertise each time we have engaged their services. They have also assisted with issues arising in other areas while they were on site. [Redacted] is a State agency consisting of four divisions. Within those divisions there are over one hundred programs and five direct care facilities. | |

### Massachusetts State Agency

**Question #/Question** **Rating**

| | |
|---|---|
| 9. Rate the knowledge of the vendor's assigned staff and their ability to accomplish duties as contracted. | **RATING: 10** |
| **Comments:**<br>Outstanding! | |

### Federal Agency

**Question #/Question** **Rating**

| | |
|---|---|
| 9. Rate the knowledge of the vendor's assigned staff and their ability to accomplish duties as contracted. | **RATING: 10** |
| **Comments:**<br>Janus has a veteran staff that saw very little turnover. Key personnel remained on the project throughout each project. Over the eleven years that I worked with Janus, key personnel left on the rare occasion due to health reasons or changes in their personal lives that required a physical move. Often they still remained on the project assisting with the completion remotely. New experienced staff was brought on board to continue Janus' quality of service. In addition, the staff has experience across all levels of information security from the mainframe, mid-tier, desk-top to all current mobile and network technologies. This was particularly important in an agency that employs all of the above. Janus' management style is very hands-on and regularly met to discuss the project status and make any necessary adjustments based on the technical direction of the Project Officer. | |

JANUS consistently receives customer comments similar to these and will ensure that our work for the Authority remains equally diligent and thorough.

The breadth of JANUS' technical consulting work includes virtually every business process and every information system. Our extensive knowledge of information systems includes all major technical platforms: Windows (all versions), UNIX, Linux, Novell, Apple/Macintosh, and IBM as well as a variety of proprietary operating systems, e.g., GE and Honeywell as well as mobile and tablet.

Having completed many projects that require vision, management, remediation, development, and IT systems analyses and assessment of large, complex organizational requirements, JANUS' consultants understand how to determine true need, which often differs from the stated need. Our consultants blend what they hear with what they observe, factor in the challenges, and produce a clear and cost-benefit conclusion for clients. A statement by a Commonwealth of Massachusetts Technology Director was that every time he left the room from a JANUS meeting, he felt smarter as a result of our assistance and advice.

## *JANUS Capabilities*

JANUS' long commitment to improving infrastructure, IT networking, application, and security, performing Independent Verification and Validation (IV&V) and risk, vulnerability, and compliance assessments as well as cyber training/awareness has resulted in our consultants having a high-level of understanding of the issues that confront complex organizations such as those of the Authority. This knowledge has been essential in establishing JANUS' standing in this field. JANUS brings a rigorous focus on excellence and proven ability to provide client-centric solutions to all projects and has the business experience to understand the relative value of information and its impact on an organization. Our firm's extensive experience within a broad spectrum of settings provides clients with an objective, balanced perspective. JANUS also assists our clients in achieving a proper balance between technology needs and cost.

For our tests and assessments, we follow processes that are geared to provide you with a set of full results and recommendations that make your follow-on work easier. This is not always done by consultants, but JANUS has specialized in security, continuity, and forensics for over 32 years. We know how to relieve some of the burden from our clients by thinking through a complete project process – and we do that. In our assessments, we also know what you will need to do to verify our findings (if we do not) – so we take on that responsibility, thus eliminating the time and expense you would need to exert following our assessments. There are consultants who will appear to offer a less expensive solution; however, rarely will that solution be complete enough to relieve you of the many follow-on resource requirements of results verification that enable you to begin remediation. We offer a holistic solution to truly meet enterprise security needs at an excellent price point.

### Service Offerings

JANUS does business throughout the U.S. focusing on information security, business continuity, regulatory compliance, and computer forensics/e-Discovery. JANUS has provided services to private industry; federal, state, and local government; not-for-profit organizations; and secondary and higher education institutions and is eminently qualified and well-positioned to continue to satisfy the Authority's cybersecurity requirements.

JANUS confronts complex technical issues with a clear understanding and appreciation for the operational business objectives of the organization and helps align and balance operational objectives with the particular needs of our clients. We also work to enhance knowledge transfer with clients, thus enhancing the lasting impact of our involvement.

JANUS responds quickly to client needs – wherever and whenever required. Clients reap the benefit of having access to JANUS senior level people who are innovative experts, not trainees. JANUS top management is available for answers to questions and quick response. As an independent, vendor-neutral entity, JANUS is not limited by product offerings and is free to identify the best solutions to specific needs, rather than force-fitting specific vendor offerings.

### Assessment Experience

JANUS has focused on security risk and vulnerability assessments within our consulting throughout our history in our quest to protect and analyze our clients' information. We have completed many hundreds. Staff has long seen the potential for major problems at clients' sites and in their systems and has striven to analyze these and/or eliminate them, depending on the project, in each of our clients' environments.

### Enterprise-Wide Systems

In early 1989, JANUS took on our first major enterprise-wide engagement by conducting a comprehensive, multi-facility review and vulnerability assessment of controls for Aetna Insurance to improve incident recovery and control processes. Follow-on projects included long-term database design and implementation, application design, strategy development and business process re-engineering.

Significant business followed with firms like Exxon and GTE Directories (now Verizon) in Texas and Florida, where JANUS conducted major business impact analyses advising staff how to manage risk. Additional assignments included assistance with financial record-keeping by locating, documenting, and categorizing assets to write-off outdated technology components, programs, and devices. Southern New England Telephone (now AT&T) had JANUS assess its physical and logical security capabilities, to determine weaknesses and to perform penetration testing and information security tasks.

### Security Management

JANUS' breadth of experience in the security marketplace makes us the ideal candidate for security testing and management assignments. JANUS staff, through our many projects, has gained a strong understanding of the issues confronting our clients' needs and desired goals; the problems that might occur during projects; the way to structure tasks to ensure they are controllable; and the management of a variety of simultaneous subtasks.  As a result, JANUS projects are completed on-time and on-budget.

### Computer Forensics

With our established reputation for ethics, credentialed experts, and our vast knowledge in the field of Information Technology, it was not surprising when the legal community began to call upon JANUS to assist in the electronic discovery of evidence – a field that has since become known as computer or digital forensics.

By the end of 1998, JANUS' assignments in investigations and fraud examinations had been combined with our work on electronic discovery and breach response/prevention services to form a separate computer forensics practice.  JANUS subsequently is the only firm in America to have played a prominent role in the adjudication of both the TJX and the Heartland breach cases as court-appointed experts.

### E-Commerce

As Internet usage increased in both business and industry, JANUS responded to clients' e-commerce needs.  Adding people to our staff who had been involved in some of the first Internet security incidents reported to the FBI, JANUS consultants were able to address increasingly complex e-commerce and Internet issues.  JANUS currently provides services such as IT security strategy, manages or oversees IT implementations, de-militarized zone design, and wireless strategy and design services, web-based consulting involving: security-conscious web design, secure web connectivity to back-office systems, virtual private network (VPN) design and implementation, biometric assessment and design, PKI enabling technologies, firewall/router/switch design implementation, and testing, illustrating a few examples.  The skills gained in providing these services directly impact the capabilities to provide leading edge technical cyber solutions.

Recognizing the sophistication and forward thinking of JANUS in the Internet area, a critically sensitive branch of the federal government chose JANUS over six vendors to architect and implement secure and anonymous connectivity to the Internet in 1999.  The challenge was to ensure that the entire operation could meet the organization's e-commerce needs and, at the same time, warrant that the internal data remained locked-away from hackers and unauthorized staff.  The client also required flexibility to conduct research via the Internet anonymously or not, whichever suited its objectives.

JANUS' initial focus on security consulting has broadened to include all areas affecting the controlled, efficient flow and design of information.

### Description of Services

We specialize in protecting clients' data and computing environments through (samples):

#### *Security Testing & Assessment*

- Application Testing

- Vulnerability & Penetration Testing
- Security Controls Assessments (SCA)
- Security Testing and Evaluation (ST&E)
- Security/Risk Assessments
- Compliance Reviews
- Social Engineering
- Wireless Assessment & Testing
- Application Code Reviews
- War Dialing
- I.C.U…MVS® Mainframe Security Auditing and Tools

### *Information Security Consulting & Controls*

- Current-State and Future-State IT and Security Assessments
- Chief Information Security Officer Services
- Future Roadmap Development
- Governance and Risk Management
- Gap and Organizational Analyses
- Network and Security Cost Analyses
- Data Classification and Inventory
- IT and Security Design/Development & System Architecture
- IT and Security Governance
- Certification & Accreditation
- Firewall Design & Implementation
- Independent Verification and Validation (IV&V)
- Program, Policy and Procedure Development
- Metrics Development and Assessment
- Wireless Security Design
- System Hardening
- Incident Response Planning
- Convergence of Logical & Physical Security
- Implementation of Security and Controls in the SDLC
- Risk Management Program Development
- Cloud Computing and Migration Risk Assessments
- Biometrics Security
- e-Discovery and Digital Forensics
- Independent Third-Party Reviews

### *Business Resilience*

- Business Continuity (BC)
- Disaster Recovery (DR)
- Continuity of Operations (COOP)
- Planning and Testing

- Business Impact Analysis (BIA)
- Privacy Impact Assessment (PIA)
- Data Breach Crisis Response

### *Education*

- Secure Web Application Analysis and Training
- General Security Awareness & Training
- Curriculum & Content Design
- Computer-Based Training (CBT) Design

## *Assessing Risk*

JANUS has a 32+ year proven track record in performing similar assessments and supporting information security needs for a wide variety of well-known organizations.

The type of services that the Authority is requesting are the type that JANUS performs every day for our clients. Similar tasks have been concluded or are underway for the following: Saint Clair County (IL); General Dynamics; Massachusetts Water Resources Authority; Fallon Health; Naperville Utility (IL); States of Minnesota and Wisconsin; Town of Nantucket; Travis County (TX), Providence Housing Authority; Texas Tech University Health Sciences Center; and the Port Authority of New York and New Jersey, to name but a few. Any of these organizations could discuss our thoroughness and capabilities with you.

JANUS performs similar services for a variety of state/municipal clients as well as utilities and many others, a small sample of which follows:

Utilities such as:

- Massachusetts Water Resources Authority
- Santee Cooper Power Company of South Carolina
- Occidental Petroleum – Permian Basin of Texas/New Mexico
- South Central Connecticut Regional Water Authority
- New York Power Authority
- Norwich (Connecticut) Public Utility
- Naperville (IL) Utility

Counties and municipalities such as:

- New York City, New York
- Putnam County, New York
- Capital District Transportation Authority of Albany, New York
- Frederick County, Maryland
- Howard County, Maryland
- Charles County, Maryland
- Westminster Schools, Atlanta, Georgia
- St. Clair County, Illinois
- Madison County, Illinois
- City of Naperville, Illinois
- Travis County, TX
- Baltimore, Maryland – Enoch Pratt Library

- City of Norwich, Connecticut

Education clients such as:

- Charles County Public Schools (Maryland)
- Wor-Wic Community College (Maryland)
- College of Southern Maryland
- Sailor Network (Maryland educational and library backbone network)
- Texas State Technical College
- University of Texas
- Texas Tech University Health Sciences Center
- Schertz-Cibolo-Universal City Independent School District (Texas)
- State University of New York Buffalo
- Harford County Public Schools (Maryland)
- Community College of Baltimore County
- Anne Arundel Community College (Maryland)
- California State University at Sacramento
- Sacred Heart University
- University of Wisconsin-Madison
- University of California at Berkeley
- The McCormack Institute of the University of Massachusetts
- University of Central Arkansas

Healthcare clients such as:

- Texas Tech University Medical Center
- Texas A&M Health Center
- State of Vermont Healthcare Exchange
- State of Minnesota Healthcare Exchange
- National Government Services, Inc. (assessments of CMS healthcare applications)
- General Dynamics (assessments of CMS healthcare applications)
- RiverSpring Health
- Memorial Sloan Kettering
- Putnam/Northern Westchester Health Benefits Consortium
- Pennsylvania Health Care Cost Containment Council
- Health & Hospitals Corporation of New York
- MD Anderson Cancer Center
- The Iowa Institutes
- The Long Island Home/Brunswick Hospital

State government organizations such as:

- Commonwealth of Massachusetts
- Commonwealth of Pennsylvania
- Commonwealth of Virginia
- State of Texas
- State of North Carolina
- State of South Carolina
- State of Maryland
- State of Delaware
- State of Minnesota
- New York State
- State of Oregon
- State of Vermont
- State of Wisconsin
- Washington State
- State of Wyoming

Federal government clients such as:

- Centers for Medicare & Medicaid Services (CMS)
- National Institute of Standards and Technology (NIST)

- Social Security Administration (SSA)
- Department of the Interior (DOI)
- Federal Trade Commission (FTC)
- Federal Reserve Board (FRB)
- Federal Deposit Insurance Corporation (FDIC)
- Railroad Retirement Board (RRB)

Insurance clients such as:

- Aetna
- The Hartford
- AXA
- Travelers
- BCBS organizations in Florida, Arkansas, New York, Pennsylvania, Washington/Alaska, South Carolina

Healthcare clients such as:

- Memorial Sloan Kettering
- Health & Hospitals Corporation of New York
- Texas A&M Health Center
- MD Anderson Cancer Center
- The Iowa Institutes
- The Long Island Home/Brunswick Hospital
- Department of Health & Human Services (S. Carolina)

Not-for-profits such as:

- The Brookings Institution
- Amnesty International
- Save the Children
- The Pine Street Inn of Boston (the largest homeless shelter system in the U.S.)

# MANAGEMENT PLAN

[Redacted]

In addition to skill, ethics is a major component of our work.  Our employees are bonded and undergo background checks (criminal and credit) prior to employment.  We also carry Errors and Omissions insurance and Cyber Liability insurance as additional levels of protection for clients.  Employees sign a five-page ethics code upon employment that defines their behavior and stresses that they are to put the needs of our clients first in all situations.

[Redacted]

## *Project Management Approach*

[Redacted]

### Project Planning

[Redacted]

[Redacted]

[Redacted]

Thorough planning and significant experience in the type of project the Authority is requesting helps to avoid the price of quality non-conformance that has been shown to add so significantly to costs. With the price of non-conformance for American business averaging 25%-30% of costs (reprocessing, reruns, unplanned service, etc.), this is a situation that is too expensive to continue. No better time exists to ensure quality than in the planning phase.

### Review, Checking, and Audit

We stress in our daily work environments the precepts of review, checking, and audit, both for our clients and ourselves. However, prevention is of even more value. We constantly stress prevention, and we assist each other in reviewing and checking tasks geared towards prevention.

### Input

We are proud to work in an environment where our employees are highly valued members of the team. Therefore, each individual has an opinion that is considered, not only management's opinion.

The result of this structure has been that all our employees feel they are free to speak up about potential problems before they become actual problems. No problem gets buried. The staff works hard and commits long hours to their projects. However, they each can clearly see the results of their involvement.

### Secure Communication

This project will require sharing confidential information. JANUS avoids using email attachments whenever possible, especially when confidential reports are being shared. To that end, JANUS will establish a secure portal dedicated to this project. Only JANUS team members and duly designated Authority staff will have access to the portal. The portal is protected by advanced encryption and access controls.

### Status Meetings

The purpose of this periodic meeting is to report on tracked project schedules, project milestones, logistics, and any metrics associated with project progress. At a high-level, actual findings and observations from the assessment and analysis can also be shared during the meeting. To be respectful of people’s time, we recommend that the meeting be attended by the core project team, with others invited as needed according to the phase of the project.

# References and Prior Work Experience

## *References*

[Redacted]

[Redacted]

[Redacted]

## *Past Performance*

| **Contract Name: Security Policy Analysis & Incident Response Planning**<br>**Customer Name: South Central Connecticut Regional Water Authority (RWA)** | | |
|---|---|---|
| **b. Contract/Purchase Order Number:** PO# 0021513 | **c. Contract Type:**<br>Firm Fixed Price | **d. Total Contract Value:**<br>$31,980.00 |
| **e. Brief Description of Work Performed:**<br>The South Central Connecticut Regional Water Authority (RWA) is a non-profit public corporation created by the Connecticut Legislature in 1977. The RWA owns more than 27,000-acres of land and provides a wide array of recreational opportunities and water-related services, including hands-on water science programs to thousands of students annually. On average, the RWA supplies 45 million gallons of water a day to a population of some 430,000 persons.<br>JANUS provided the RWA with a gap analysis of existing security policies as compared with leading practices, tailored to water utilities and SCADA environments. The primary area of interest was the development and improvement of the Security Incident Response Plan (IRP).<br>JANUS reviewed existing security policies and procedures, interviewed key subject matter experts, and assessed the preparedness of RWA to address security incidents. JANUS used authoritative references to develop the plan, including the NIST Special Publication 800-61, Revision 2: "Computer Incident Handling Guide" and the International Security Standard ISO 27002, section 16.1" Information Security | | |

Incident Management." Supplemental guidance was also aligned with NIST SP 800-86: "Guide to Integrating Forensic Techniques into Incident Response." The plan was presented in four parts:

- Definitions and Standards
- Strategies and Phases of Incident Reponses
- Standard Operating Procedures
- Appendix of supporting documents and templates

The plan provided forms and templates for managing the following incidents:

- Incident Handling Checklist
- Incident Identification Form
- Incident After Action Report

JANUS also provided a detailed analysis of existing federal and state reporting requirements for data breaches, including specific contact names and reporting procedures. A second project is currently underway.

| **f. Period of Performance:** | **g. Technical/Project Manager:** | **h. Contract Officer:** |
|---|---|---|
| March 12, 2018 – Present | [Redacted] | N/A |

**Contract Name: Security Program Analysis**
**a. Customer Name: Norwich Public Utilities (NPU)**

| **b. Contract/Purchase Order Number:** N/A | **c. Contract Type:** | **d. Total Contract Value:** |
|---|---|---|
| | Fixed | $41,836.00 |

**e. Brief Description of Work Performed:**

Norwich Public Utilities (NPU) provides four utilities to the City of Norwich – natural gas, electricity, water and wastewater collection. Established in 1904, NPU is municipally-owned and governed by a five-member Board of Commissions and Sewer Authority, who represent the best interest of the citizens they represent. NPU also provides network infrastructure for the city, including a Metropolitan Area Network (MAN) and Internet Service Provider (ISP) services.

NPU contracted JANUS to perform a review of NPU's information security program and general state of information security maturity to measure the effectiveness of existing technical security controls and to determine whether technical or operational vulnerabilities exist in its information systems.

As part of the project to assess the security program at NPU, JANUS prepared a suggested Roadmap of remediation tasks. This Roadmap expressed what the JANUS engineers anticipate will be the most important tasks for NPU to undertake to enhance its overall security program.

JANUS used authoritative security frameworks as a guide when conducting this review, including the National Institute and Standards and Technology (NIST) Special Publication (SP) 800-171: "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," NIST 800-53: "Security and Privacy Controls for Federal Information Systems and Organizations," the NIST Cybersecurity Framework, and the Critical Infrastructure Protection (CIP) standards issued by the North American Electric Reliability Corporation (NERC). The scope of the assessment included all policies, procedures and general systems architecture. The scope did not include penetration testing, comprehensive network vulnerability scanning, or technical testing of Industrial Control Systems (ICS) or Supervisory Control and Data Acquisition (SCADA) equipment.

The assessment was conducted through a combination of:

- Review of existing documentation
- Interviews with NPU staff
- On-site inspection

The assessment included observations from technical testing and security tests and audits.

Confidential documents were shared in a secure web portal provided by JANUS, dedicated to this project. Prior to the on-site inspection, JANUS reviewed 39 documents provided by NPU, categorized based on NIST 800-171 control families:

- Access Control
- Media Protection
- Awareness and Training
- Personnel Security
- Audit and Accountability
- Physical Protection
- Configuration Management
- Risk Assessment
- Identification and Authentication
- Security Assessment
- Incident Response
- System and Communications Protection
- Maintenance
- System and Information Integrity

On-site interviews and inspection took place in NPU corporate offices, from December 18 to December 22, 2017, with follow-up interviews conducted January 9, 2018. JANUS interviewed key subject matter experts in technical areas, as well as representatives from business units most likely to be impacted by information security events.

| | | |
|---|---|---|
| **f. Period of Performance:**<br>November 2, 2017 – February 15, 2018 | **g. Technical/Project Manager:**<br>[Redacted] | **h. Contract Officer:**<br>N/A |

**Contract Name: Pennsylvania OIT Security Assessment**
**a. Customer Name: Commonwealth of Pennsylvania Office of Information Technology, Enterprise Information Security**

| | | |
|---|---|---|
| **b. Contract/Purchase Order Numbers:** IT - ITQ 4400004480<br>PO#s: 4300415165, 4300457866 | **c. Contract Type:**<br>Firm Fixed Price | **d. Total Contract Value:**<br>$157,042.23 |

**e. Brief Description of Work Performed:**

The Commonwealth of Pennsylvania Office of Information Technology (OIT) provides hosting, datacenter services, and information security services for all state agencies in the Commonwealth.

JANUS has completed three projects for the Commonwealth over three years.
**Project 1**: Provided external penetration testing and vulnerability assessment for the entire range of Commonwealth Internet facing hosts for dozens of state agencies. Phases of the project included:

- Network and host discovery across the entire range of 65,535 possible IP addresses
- Vulnerability scan across more than 1000 active internet hosts
- Application discovery to identify more than 500 active Internet applications and web sites
- Application vulnerability scans across more than 32,000 web pages
- Penetration testing, verifying vulnerabilities and attempting exploits against the top ten most important web sites
- Wireless penetration testing for the primary physical locations
- Social engineering, attempting to bypass physical security at the datacenter

Risk assessment results were delivered in a summarized 90 page report, supported by extensive spreadsheets of technical details that enable the technical support staff to remediated vulnerabilities. JANUS completed this project with an executive level briefing to the Commonwealth CIO and CISO.

**Project 2**: In year two JANUS repeated the network discovery and web application testing across the same ranges as in year one, and provided analysis of trends in risk and remediation of those sites and applications.

JANUS then provided penetration testing against that year's more important web applications, verifying vulnerabilities and demonstrating attack vectors that place Commonwealth assets at risk.

JANUS performed a social engineering email phishing campaign against 78,000 Commonwealth employees. This test included establishing a web site that looks like a Commonwealth web site. JANUS sent emails to all employees, where the email appeared to come from a known Commonwealth source, requesting that they log onto the fake web site and entered their username and password. JANUS tracked the individuals who entered their passwords, and provided an analysis of the departments that are most at risk from social engineering attacks.

**Project 3:** In 2016 JANUS performed two projects. The Department of State (DOS) contracted JANUS to perform a security assessment, vulnerability scan, and penetration test of its web-facing voter registration applications and the Commonwealth County Network (CCN), to include local Citrix terminals. In addition to technical testing JANUS reviewed the internal architecture and used it to determine how the services interconnect, what the various operability functions are for each, how users are able to interact with the Citrix terminals, and vulnerabilities or risks that arise from that architectural approach.

Voter registration web applications were tested from September 14, 2016 to October 4, 2016 and the private CCN network was tested on-site between October 17, 2016 and October 19, 2016.

The scope of this assessment included six (6) externally facing web sites, a thin client and the private network of T1 lines used to connect in a spoke and hub configuration to the Department's election systems in Harrisburg (via a third party outsourced arrangement run out of a Virginia data center), to manage voter registration records. The Department presents a Citrix virtual terminal session that county staff use to interact with Department systems. Because each of the 47 counties have their own independently managed network, uniform assurance of network security across the entire system cannot rely solely on county network security. The Citrix/private network configuration must protect Department systems from any hacking or misconfiguration originating from one of the 47 entry points. Testing was focused on:

- External penetration testing of web applications; and
- CCN network architecture, the Citrix terminal, and its general support systems. General support systems included Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP) servers, Gateways, and other DOS information systems.

All assessments included, but were not limited to, tests for minimum technical security controls defined by authoritative security guidelines and frameworks, including the following:

- NIST Special Publication 800-53: "Recommended Security Controls for Federal Information Systems and Organizations"
- Open Web Application Security Project (OWASP) Top 10 Web Application Security Risks

The rules of engagement for this security assessment and penetration test were as follows:

- All work must be accomplished within the specified time period.
- JANUS will not authorize or execute any functional changes on client networks.
- Testing will be conducted during normal business hours.
- JANUS will provide source IP addresses from which testing will be conducted.
- The DOS will be notified of the start and end of each daily testing period.
- Testing will include automated and manual techniques.

Results from testing were shared with the PA DOS as they were discovered, in an ongoing and collaborative process that enabled DOS to address vulnerabilities as they were discovered. At the conclusion of all testing JANUS provided a final report listing all vulnerabilities and risks, in a prioritized ranking for remediation, along with detailed recommendations for remediation.

Assessment results were presented in written reports and in-person executive briefings to the CIO of the Commonwealth.

| | | |
|---|---|---|
| **f. Period of Performance:**<br>May 8, 2014 – August 15, 2014 | **g. Technical/Project Manager:**<br>[Redacted] | **h. Contract Officer:**<br>N/A |

| | | |
|---|---|---|
| May 16, 2015 – July 8, 2015<br>Voter registration web applications September 14, 2016 – October 4, 2016<br>The private CCN network was tested on-site between October 17, 2016 and October 19, 2016 | | |

## Needs from Authority Staff

When a project is agreed to specific items are regularly needed with which to carry out the project. Sometimes, clients do not attend to these details until the project has already begun and in such situations, the amount of testing and assessment or consulting contemplated in the project cannot be undertaken. We want you to obtain the most for your expenditures. Therefore, although not difficult to produce, JANUS does have the following needs:

### Access to System and Staff

- Adequate access to management and other key personnel for consultation and interviews. Very little of these people's time will be taken, but some contact will be necessary;
- Access to technical and system programming staff (if needed) during the length of the project (very little time needed);
- Access to staff who have been identified for interviews during the length of the project (usually one hour each); and
- Immediate access on a part-time basis to a security (or staff) liaison person providing interface capability to assist with questions (when needed), contact with appropriate staff, etc. (low level of support) and establishing schedules. This is typically less than one-fifth time unless the person wishes to shadow our team to increase knowledge.

### Logical and Other Access (when required)

- IP addresses relevant to project;
- User IDs/passwords for applications/operating systems (if needed);
- Authority to access network components and operating systems (as needed);
- Relevant documentation such as policies and procedures (if needed); and
- Letter of Authorization to access and test systems (format provided by JANUS when needed for the assessment).

## Assumptions

1. Timely access to all resources (system and personnel) required to complete tasks and any interviewing (provided by the Authority within three (3) business days). Lack of this will impact our ability to perform our duties and could impact contents, deliverables and schedule.
2. Commitment and support from management and project stakeholders. The Authority will designate a senior-level individual who will be authorized during the term of the project to act as the project's primary contact. This individual must have authority to make decisions about actions to be taken by JANUS on behalf of the Authority for the proposed services.
3. The Authority acknowledges and agrees that if any Authority responsibility as set forth in this proposal is not performed by the Authority then JANUS will be relieved of providing the affected

JANUS services to the extent the Authority's nonperformance impacts JANUS' ability to provide the affected services.

4. Availability of appropriate Authority staff and resources so that deliverables can be submitted, reviewed and accepted within the required timeframe.
5. The Authority Project Manager will be responsible for evaluating the appropriateness of recommendations with respect to overall needs.
6. The Authority will provide JANUS personnel with remote VPN access or install a JANUS appliance to all required internal systems where appropriate as determined by the Authority and JANUS.
7. The JANUS team will provide observations and recommendations to Authority project management during this engagement. The Authority is solely responsible for determining what changes/improvements should be implemented.
8. For pricing purposes, JANUS assumes one (1) draft and one (1) final submission of each deliverable.
9. Specific IP addresses, URLs, credentials, and other information related to test targets will be provided a minimum of ten (10) days before scheduled testing.
10. Scans will be allowed to execute to completion, including overnight execution.
11. If we are unable to complete a scan requirement specified within this proposal within thirty (30) days following commencement of the scan due to the Authority's failure to meet its obligations, the scan will be considered completed.
12. JANUS will perform work during normal business hours. Off-hours scans may be scheduled with advance notice. More than one postponement in off-hours scanning may result in scope and pricing changes.
13. Our staff will be provided proper credentials and access to conduct scans and tests.
14. Any delays to staff access will result in delayed deliveries or less test time available.
15. Permission from any cloud provider(s) must be granted.
16. The Authority acknowledges that the ability of JANUS to provide the services in accordance with the proposal (including the agreed pricing and delivery models) are contingent upon the accuracy and completeness of information, data, and applications provided by the Authority as well as the Authority's cooperation and timely performance of its obligations.
17. Any attacks; e.g., during a penetration test, that could potentially cause a system failure, be it at the system or application level, will only be performed in coordination with the Authority. If the usage of the attack has been deemed as required to provide necessary coverage and authorization is gained from the Authority's technical contact, then the attack will be performed.

# Other Items

## *Security Measures*

JANUS is highly concerned about our clients' data and always takes precautions in holding or transmitting data. We also provide a secure site for client documentation to avoid using the Internet or mail. We can deposit deliverables in this portal for secure delivery of results.

As specialists in security, networking, and recovery, we understand the need for protection of client materials. Client electronic materials are kept secured within an access controlled data center so that no client materials can be exposed to unauthorized users. Printed materials are in locked cabinets, not left in the open.

As experts in cybersecurity, each JANUS employee is much more attuned to security needs than is an average company's employees. No one needs to force our employees to change passwords (or for them to be robust). Our people use proximity card badges as a matter of course every day. We operate in a Windows server environment with high levels of security implemented. New generation firewalls (that are regularly monitored and tested) prevent unauthorized outsiders from accessing files and appropriate access privileges prevent unauthorized insiders from the same. Electronic files where client data are stored are in a locked-down file structure in a secure data center with only those who have a need-to-know having access.

In addition, when at a client site all our consultants work with encrypted laptops. Where "flash sticks" are utilized, these are also encrypted. The latest patches are applied prior to the laptops leaving our offices. Typically, prior to leaving a client site, all client data are loaded into a protected repository through a secure portal and the laptop is sanitized. In this manner, client data are not subject to loss or theft. Although this is perhaps over and above requirements for vendors, we take our responsibility as a security company very seriously and understand that we have a requirement to protect your information.

All our employees have signed confidentiality agreements and ethics statements and have undergone background checks which we also take seriously, and all client materials are stored in files based on "need-to-know" prior to access being allowed.

While transferring documentation and reports back and forth between clients and our infrastructure, we encourage use of our secure portal which will be established for the Authority for this specific task at the beginning of the project. Thus, documents can be quickly checked in or out with version control to ensure security and speed. Access to this portal is also established on a "need-to-know" basis.

## Bonding and Background Check Procedures

JANUS carries a criminal theft and fraud bond for $5,000,000 as well as liability and umbrella coverage. Our employees are bonded and undergo background checks (criminal and credit) prior to employment. We also carry both Errors and Omissions and Cyber Liability insurance as additional levels of protection for clients. Employees sign a five-page ethics code upon entry to JANUS that defines their behavior and stresses that they are to put the needs of JANUS' clients first in all situations.

In addition to background checks, many of our employees have also undergone separate background checks by federal and/or state agencies and typically often either hold, or are in the process of receiving, clearances for working with critical and sensitive data.

## Change Order Process

As part of our quality plan, we utilize a formal change management process for all changes considered to a project's scope, deliverables, timeline, and budget. The change process includes steps, responsibilities, change parameters or measurement criteria and deadlines to guide the review of proposed changes for potential impacts and appropriateness prior to acceptance. Ensuring well-structured change management processes is a basic element of quality performance. Changes usually affect delivery dates, resources and costs. As a result, they need to be agreed to by both the Authority and our management before application to the project to make sure that all entities understand what is expected of them. Major items to be addressed within the Change Order Process include change requirement, priority, impact (to project scope), budget, and schedule.

# APPENDICES

## *Appendix A – Tools*

JANUS uses a variety of commercial, shareware, and freeware tools to conduct our risk and security assessments. The following list of tools reflects a sampling of those programs that have received thorough review and are frequently used by our consultants. However, other tools and programs are being reviewed and evaluated at all times, and it is common for other tools to be used in support of client requirements. In particular, there are literally hundreds of tools that are vulnerability/issue specific (such as msadcs.pl for taking advantage of the Microsoft IIS msadcs vulnerability), and are not covered in this list. Appropriate tools will be selected as JANUS moves through the testing phases of the project to meet the needs of the specific potential vulnerability or exploit we are attempting.

JANUS' staff is encouraged to search out, develop, and introduce new tools to all testers. In this way, we maintain our expertise in the latest available toolsets while at the same time focusing our efforts on those tools that will be the most helpful, without subscribing to every tool available. However, in addition to those tools mentioned below, which are part of our toolbox, we have a tool available to address any problem that a tester may encounter. All tools used are tested in a laboratory environment and receive a thorough review prior to their use on a client site.

### Network and Packet Capture, Access, Sniffers, and Analysis Tools

[Redacted]

### Network Mapping Tools

[Redacted]

[Redacted]

### Password Crackers

[Redacted]

### System Tools

[Redacted]

[Redacted]

### Vulnerability Scanners

[Redacted]

### Web Server/Web Application Tools

[Redacted]

[Redacted]

### Wireless Testing

[Redacted]

[Redacted]

## OWASP

We also focus on the Open Web Application Security Project (OWASP) "Top Ten" in our assessments. To perform testing in this area we regularly utilize a variety of the following tools:

| Attack | Tool |
|---|---|
| • Un-validated Input | |
| • Broken Access Control | |
| • Broken Authentication and Session Management | |
| • Cross-Site Scripting (XSS) Flaws | |
| • Protocol Analysis | |
| • Buffer Overflows | |
| • Injection Flaws | |
| • Improper Error Handling | |
| • Insecure Storage | |
| • Insecure Configuration Management | |
| • Physical Intrusion | |
| • IP half-scan | |
| • Brute Force Password cracking and access violation | [REDACTED] |
| • Cisco devices with SNMP | |
| • Trojan horses | |
| • Java-based DB analysis | |
| • Interceptions; most frequently associated with TCP/IP stealing and interceptions that often employ additional mechanisms to compromise operation of attacked systems (man-in-the-middle attacks) | |
| • Spoofing (deliberately misleading by impersonating or masquerading the host identity by placing forged data in the cache of the named server i.e. DNS spoofing) | |
| • Scanning ports and services, including ICMP scanning (Ping), UDP, TCP Stealth Scanning (TCP that takes advantage of a partial TCP connection establishment protocol) | |
| • Remote OS Fingerprinting, for example by testing typical responses on specific packets, addresses of open ports, standard application responses (banner checks), IP stack parameters etc. | |
| • Network packet listening (a passive attack that is difficult to detect but sometimes possible) | |

| | |
|---|---|
| • Authority abuse; a kind of internal attack, for example, suspicious access of authorized users having odd attributes (at unexpected times, coming from unexpected addresses) | |
| • Flooding (Ping flood, mail flood, HTTP flood) | [REDACTED] |
| • Malformed URL's | |
| • Wireless Connection Attempts | |

## *Appendix B – Sample Report*

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

# *Appendix C – Client Comments*

## State of Minnesota

[Redacted]

### Maryland State Retirement Agency

[Redacted]

## Anonymous

**From:** Gxxxxxxx [mailto:gxxxxxx@xxxxx.com]
**Sent:** Friday, December 16, 2016 12:20 PM
**To:** Adam Fisher <AdamF@JanusAssociates.COM>
**Subject:** RE: Social Engineering

Great work.   These employees just finished the cyber awareness training and phishing was covered in detail so they should have known better, just goes to show you cannot stop 100%.

Thanks,
Gxxxx

**From:** Adam Fisher [mailto:AdamF@JanusAssociates.COM]
**Sent:** Friday, December 16, 2016 12:13 PM
**To:** Gxxxxxxx <gxxxxxx@xxxxx.com>
**Subject:** RE: Social Engineering

OK, then I'm stopping.  I'm into Citrix currently.

**Adam G. Fisher**
JANUS Associates, Inc.
1.203.251.0169 (w)
1.617.872.6486 (c)
1.203.251.0222 (f)
http://www.janusassociates.com

This e-mail and any files transmitted with it are the property of JANUS Associates, Inc., are confidential and, are intended solely for the use of the individual or entity to whom this e-mail is addressed. If you are not one of the named recipient(s) or otherwise have reason to believe that you have received this message in error, please notify the sender at 203-251-0200 and delete this message immediately from your computer. Do not divulge, copy, forward, or use the contents, attachments, or information without permission of JANUS Associates, Inc. Any other use, retention, dissemination, forwarding, printing, or copying of this e-mail is strictly prohibited.

### Ventus (September 2015)

[Redacted]

### Commonwealth of Massachusetts Department of Labor and Workforce Development

[Redacted]

## Wyoming Department of Health

[Redacted]

End of Document

5. Identify the name, address and contract information for 3 companies that the Consultant has performed similar services to those being sought by the Authority: Please see proposal document.

Part 2: Please see proposal document.

Part 3: Please see proposal document.

O'Connor & Drew P.C.
OCDTECH

Part 1:

- Item 1-Name of Individual or Organization: O'Connor & Drew, P.C. d/b/a OCD-Tech
- Item 2- Name and Title of Contact Person: Michael Hammond, Principal
- Item 3- Business Address: 125 Braintree Hill Office Park, Suite 102, Braintree, MA 02184
- Item 4- Telephone Number: 617-471-1120
- Item 5 - Email Address: mhammond@ocd
- Item 6 - Fax Number: 617-472-7560

Part 2: Corporation

Item 1: (a)

- Date and State of Incorporation: 3/1/1998, Massachusetts
- Name and title of executive Officers: Mark Dow, President
- Principal Place of Business: 25 Braintree Hill Office Park, Suite 102, Braintree, MA 02184
- List all related principal or Subsidiaries: N/A
- Closed or Publicly Traded: Closed
- EIN: 04-3000523

2. Identify the number of years your entity has been in business: 72 years

3. identify whether your business/corporate structure has changed in the past five years and if yes, describe the change: N/A

4. Identify the type and coverage amount of all insurance policies:

- Commercial Property Coverage: $ 1,295,414
- Commercial General Liability: $1,000,000/2,000,000
- Commercial Automobile: $1,000,000
- Worker's Comp: $500,000
- Umbrella Policy: $8,000,000
- Employment Practice Liability: $500,000
- Employee Crime: $1,000,000
- Breach/Cyber: $1,000,000
- Professional liability: $6,000,000

O'Connor & Drew P.C.
OCDTECH

TERRENCE D. MCCRACKEN
Erie County Water Authority
295 Main Street, Room 350
Buffalo, NY 14203

Dear Terrence,

## Thank you for the opportunity to serve your company. Our motto is, "Client service first."

We live our motto every day. Proudly serving clients since 1949, O'Connor & Drew, P.C. is led by a team of seventeen principals and over one hundred accounting, tax, and IT consulting professionals.

We have the research and insight to provide you with unmatched service and expertise in audit, corporate and individual taxation, business consulting, accounting, IT audit and cybersecurity, and other specialized services. To encourage professional development, our principals and staff are active in many professional and community organizations, including the American Institute of Certified Public Accountants, the Information Systems Audit and Control Association, the Cloud Security Alliance, and InfraGard. Firm members also serve as experts and regular contributors to national, local, and trade publications. In addition, our staff are regular presenters at events like Security BSides, ISSA, and industry-specific conferences.

O'Connor & Drew, P.C., and its IT Audit & Security division, OCD Tech, have long partnered with organizations to provide IT security services. Our mission at OCD Tech is to provide businesses of all sizes objective advice to allow for the most informed risk-based decisions. We are well qualified to serve your needs. A team of experienced IT Auditors and Security specialists, who have the expertise to serve you effectively and on a timely basis, will be assigned to your engagement.

We look forward to working with you and your staff. Please do not hesitate to contact us at any time with questions you may have regarding this proposal. Thank you again for this opportunity.

Very truly yours,

Michael Hammond

Michael Hammond, CISA, CRISC, CISSP

Principal, IT Audit & Security

# Information Security Services

DATE: JUNE 11, 2021

PREPARED FOR: TERRENCE D. MCCRACKEN

COMPANY: ERIE COUNTY WATER AUTHORITY

PREPARED BY: MICHAEL HAMMOND
mhammond@ocd-tech.com
(844) OCD-TECH

# Table of contents

Executive Summary 4

Our Methodology 7

Proposal Fee 12

Timeline and Project Plan 13

References / Prior Work Experience 14

Engagement Management Team 15

# Executive Summary

## ABOUT US

Established in 1949, O'Connor & Drew, P.C. is one of the most well respected regional accounting firms in the Northeast, with clients from Quebec to Hawaii. We are proud to say that we have operated independently for over seventy years. With a strong focus on government entities, higher education institutions, non-profit organizations, automobile dealerships, manufacturers, distributors, and service organizations, we are a full-service firm which thrives on our close business and individual client relationships. We are committed to providing creative, innovative solutions to help you reach your goals.

O'Connor & Drew is led by a team of seventeen principals and over one hundred accounting, tax, IT security, and consulting professionals. We have the resources to provide you with unmatched service and expertise in audit, corporate and individual taxation, information systems, business consulting, accounting, and financial services. In order to provide you with proactive and responsive IT security advice, all engagements are closely supervised by the principal-in-charge who has unique experience in and understanding of the environment in which your business operates.

To encourage professional development, our principals and staff are highly active in many professional and community organizations, including the American Institute of Certified Public Accountants, the Massachusetts Society of Certified Public Accountants, the Association of Government Accountants, the National and Eastern Associations of College and University Business Officers (NACUBO and EACUBO), and the regional Chambers of Commerce, Information Systems Audit and Control Association, ISC2, Cloud Security Alliance, InfraGard Information Technology Critical Infrastructure Working Group, and the National Defense Industrial Association. Firm members also serve as experts and regular contributors to national, local and trade publications on financial, accounting, tax, and IT matters.

## IT EXPERTISE

Organizations today depend upon information systems for nearly all aspects of their financial and operational functions. Ensuring the security of this information is important not only in meeting the needs of the organization itself, but also the needs of the organization’s stakeholders, regulators and compliance examiners. As a result, organizations must take their responsibility very seriously to properly secure client information, financial data, internal business services, external access and a myriad of other technology related assets and practices.

However, the management of IT systems and their security is complicated for large and small companies alike. Whether it is a multinational corporation addressing the control of a complex distributed architecture, or a small startup dealing with resource constraints, security must be addressed at the outset and for the duration of the system’s use.

O’Connor & Drew’s IT Audit & Security Division, OCD Tech, enables organizations to identify the current state of information security within the IT environments from management, technical, and operational perspectives. These services encompass the examination of risk, documentation, practices, networks and systems in order to provide detailed and expert advice in the safeguarding of corporate information assets and infrastructure upon which companies are dependent for most critical financial and operational services today.

## FRAMEWORKS

OCD Tech staff have decades experience in industry leading frameworks, including:

| | |
|---|---|
| AICPA Service Organization Control (SOC) 2 / 3 | Sarbanes Oxley (SOX) 404 |
| Federal Financial Institutions Examination Council (FFIEC) | Gramm Leach Bliley Act (GLBA) Safeguards Rule |
| General Data Protection Regulation (GDPR) | Massachusetts 201 CMR 17 |
| Health Insurance Portability and Accountability Act (HIPAA) | NIST Cyber Security Framework (CSF) |
| CIS CSC Top 20 Security Controls | NIST 800-53, 800-171 |
| ISO 27001/27002 | NYDFS Cybersecurity Regulation (23 NYCRR 500) |

## CREDENTIALS

The highly credentialed employees at OCD Tech hold some of the industry's leading certifications, including:

| | |
|---|---|
| Certified Information Systems Security Professional (CISSP) | Certified Information Systems Auditor (CISA) |
| Certified in Risk and Information Systems Control (CRISC) | GIAC Penetration Tester (GPEN) |
| Offensive Security Certified Professional (OSCP) | CompTIA Security+ |
| System Security Certified Practitioner (SSCP) | CompTIA Network+ |
| CSX Cybersecurity Practitioner | Microsoft Technology Associate - Security |
| CyberArk Trustee / CyberArk Defender | AWS Certified Cloud Practitioner |
| Symantec Certified Security Awareness Advocate | Apple Certified Associate |
| Qualys Certified Vulnerability Management Specialist | macOS Integration |
| Project Management Professional (PMP) | Sumo Logic Certified |
| Jamf Certified Associate | Splunk Core Certified User |

*All of our IT Audit & Security staff undergo background verification which includes checks for education, criminal history, Social Security Number trace, credit, and Office of Foreign Assets Control Blacklist checking.*

# ESTABLISHED HISTORY IN PENETRATION TESTING

## WHAT IS A CVE?

Security weaknesses in hardware and software which have been published, are given unique identifiers called "CVE numbers". CVE stands for Common Vulnerabilities and Exposures. These CVE numbers are assigned by the MITRE Corporation, a Federally Funded Research and Development Center (FFRDC), sponsored by the National Cyber Security Division of the United States Department of Homeland Security.

Security researchers who discover vulnerabilities in software and hardware are encouraged to follow a responsible disclosure process, allowing the manufacturer to fix the vulnerability and make patches available, prior to publication.

As part of our penetration testing engagements, OCD Tech has discovered multiple previously unidentified vulnerabilities in commercial software. After following a responsible disclosure process with the vendor, these findings were registered by MITRE and recorded within the National Institute of Standards and Technology (NIST) National Vulnerability Database.

| Number | Description |
|---|---|
| **CVE-2018-11628** | Data input into EMS Master Calendar before 8.0.0.201805210 via URL parameters is not properly sanitized, allowing malicious attackers to send a crafted URL for XSS. |
| **CVE-2019-7004** | A Cross-Site Scripting (XSS) vulnerability in the WebUI component of IP Office Application Server could allow unauthorized code execution and potentially disclose sensitive information. |
| **CVE-2019-19774** | Zoho ManageEngine EventLog Analyzer 10.0 SP1 before Build 12110 security restrictions bypass |
| **CVE-2020-12679** | A reflected cross-site scripting (XSS) vulnerability in the Mitel ShoreTel Conference Web Application |
| **CVE-2020-13998** | Citrix XenApp 6.5, when 2FA is enabled, allows a remote unauthenticated attacker to ascertain whether a user exists on the server, because the 2FA error page only occurs after a valid username is entered |
| **CVE-2020-5132** | SonicWall SSL-VPN products and SonicWall firewall SSL-VPN feature misconfiguration |

# Our Methodology

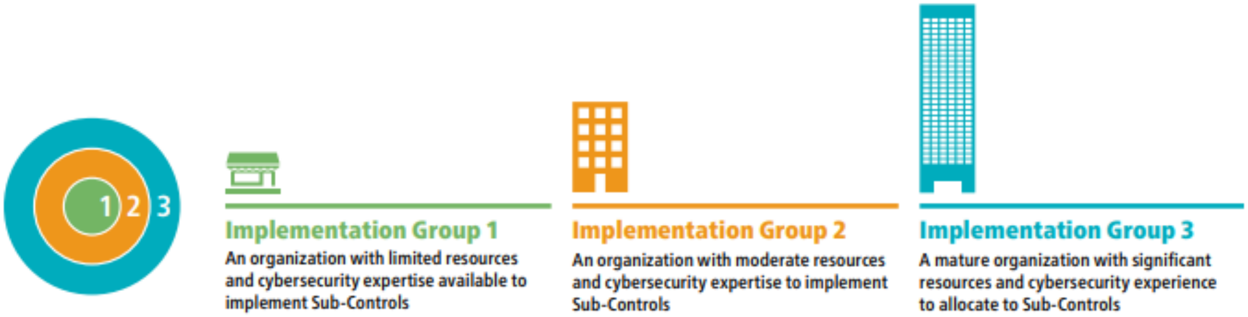
## ONSITE REVIEW - IT GENERAL CONTROLS REVIEW

The OCD Tech IT Audit and Security team are standards-driven professionals who utilize industry leading practices, security software, and tools to conduct their assessments. We leverage widely respected controls frameworks. For this engagement, we will perform the IT General Controls (ITGC) Review using the standards in the Center for Information Security's Top 20 Security Controls, further detailed below.

OCD Tech will review existing controls against standards established in the following CIS Critical Security Control domains.  The CIS Controls™ are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. The CIS Controls are developed by a community of IT experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors including retail, manufacturing, healthcare, education, government, defense, and others.

Historically the CIS Controls™ utilized the order of the Controls as a means of focusing an organization's cybersecurity activities, resulting in a subset of the first six CIS Controls referred to as cyber hygiene. However, many of the practices found within the CIS cyber hygiene control set can be difficult for organizations with limited resources to implement. This highlighted a need for a collection of best practices focused on balancing resource constraints and effective risk mitigation. As a result, CIS *recommends* the following new guidance to prioritize CIS Control utilization, known as CIS Controls Implementation Groups.

The CIS Controls™ Implementation Groups (IGs) are self-assessed categories for organizations based on relevant cybersecurity attributes. Each IG identifies a subset of the CIS Controls that the community has broadly assessed to be reasonable for an organization with a similar risk profile and resources to strive to implement. These IGs represent a horizontal cut across the CIS Controls tailored to different types of enterprises. Each IG builds upon the previous one. As such, IG2 includes IG1, and IG3 includes all of the CIS Sub-Controls in IG1 and IG2. A resource constrained organization may have to protect critical data and, therefore, implement Sub-Controls in a higher IG.

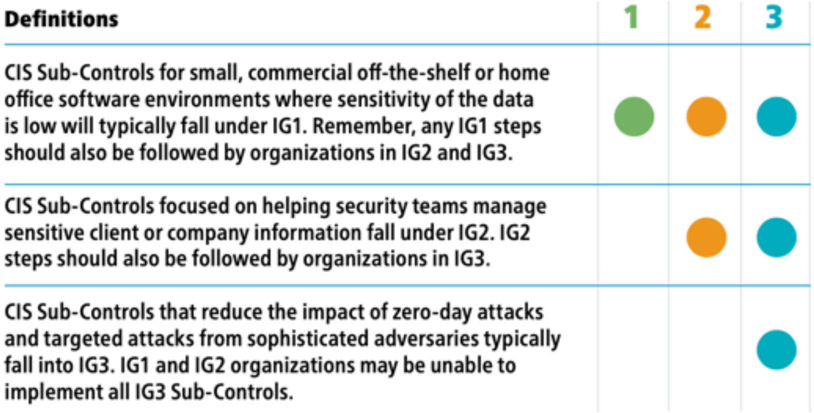


**Implementation Group 1**
An organization with limited resources and cybersecurity expertise available to implement Sub-Controls

**Implementation Group 2**
An organization with moderate resources and cybersecurity expertise to implement Sub-Controls

**Implementation Group 3**
A mature organization with significant resources and cybersecurity experience to allocate to Sub-Controls

OCD Tech will evaluate the organization against each of the sub-control areas most relevant to your organization to provide management with an understanding where they fall within their implementation group. A small to medium sized organization with limited IT and cybersecurity expertise may be comfortable establishing a baseline within IG1 with goals to meet the control requirements of IG2 and IG3. Larger organizations may feel they must be meeting or exceeding the sub-controls defined in IG2 and or IG3.



| Definitions | 1 | 2 | 3 |
|---|---|---|---|
| CIS Sub-Controls for small, commercial off-the-shelf or home office software environments where sensitivity of the data is low will typically fall under IG1. Remember, any IG1 steps should also be followed by organizations in IG2 and IG3. | ● | ● | ● |
| CIS Sub-Controls focused on helping security teams manage sensitive client or company information fall under IG2. IG2 steps should also be followed by organizations in IG3. | | ● | ● |
| CIS Sub-Controls that reduce the impact of zero-day attacks and targeted attacks from sophisticated adversaries typically fall into IG3. IG1 and IG2 organizations may be unable to implement all IG3 Sub-Controls. | | | ● |

- CSC 1: Inventory and Control of Hardware Assets - *Asset Management*
  - *Identify if the organization actively manages (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.*
- CSC 2: Inventory and Control of Software Assets - *Asset Management*
  - *Identify if the organization actively manages (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.*
- CSC 3: Continuous Vulnerability Management - *Cyber Security*
  - *Identify if the organization continuously acquire, assess, and takes action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.*
- CSC 4: Controlled Use of Administrative Privileges - *Cyber Security*
  - *Evaluate the organization's processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.*
- CSC 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers - Cyber Security

  - *Identify if the organization has established, implemented, and actively manages (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.*

- CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs - *Cyber Security*

  - *Identify if the organization collects, manages, and analyzes audit logs of events that could help detect, understand, or recover from an attack.*

- CSC 7: Email and Web Browser Protections - *Cyber Security*

  - *Identify if the organization minimizes the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.*

- CSC 8: Malware Defenses - *Cyber Security*

  - *Identify if the organization controls the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.*

- CSC 9: Limitation and Control of Network Ports, Protocols, and Services - *Cyber Security*

  - *Identify if the organization manages (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.*

- CSC 10: Data Recovery Capability - *Resiliency*

  - *Identify if the organization have processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.*

- CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches - *Cyber Security*

  - *Identify if the organization establishes, implements, and actively manages (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.*

- CSC 12: Boundary Defense - *Cyber Security*

  - *Identify if the organization detects/prevents/corrects the flow of information transferring networks of different trust levels with a focus on security-damaging data.*

- CSC 13: Data Protection - *Cyber Security*

  - *Identify if the organization have processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.*

- CSC 14: Controlled Access Based on the Need to Know - *Cyber Security*
    - *Identify if the organization have processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.*
- CSC 15: Wireless Access Control - *Cyber Security*
    - *Identify if the organization have processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANs), access points, and wireless client systems.*
- CSC 16: Account Monitoring and Control - *Cyber Security*
    - *Identify if the organization actively manages the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.*
- CSC 17: Implement a Security Awareness and Training Program - *Organizational*
    - *Validate the organization has identified for all functional roles in the organization (prioritizing those mission-critical to the business and its security), the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.*
- CSC 18: Application Software Security - *Cyber Security*
    - *Identify if the organization manages the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.*
- CSC 19: Incident Response and Management - *Resiliency*
    - *Identify if the organization protects the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.*
- CSC 20: Penetration Tests and Red Team Exercises - *Cyber Security*
    - *Identify if the organization tests the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.*

# VULNERABILITY ASSESSMENT

A Vulnerability Assessment is the process of identifying technical vulnerabilities in computers and networks as well as weaknesses in policies and practices relating to the operation of these systems. O'Connor & Drew, P.C. uses industry-leading vulnerability assessment tools to identify known weaknesses in services running on the target network. We evaluate these vulnerabilities based on validation and the risk and likelihood that an attacker could exploit them to gain control of a system.

Deliverables:

Network infrastructure security configuration and design review – We examine core network infrastructure from a configuration and design perspective, assessing security controls such as administrative access, event notification, defense-in-depth, and the protection of routing and switching environments.

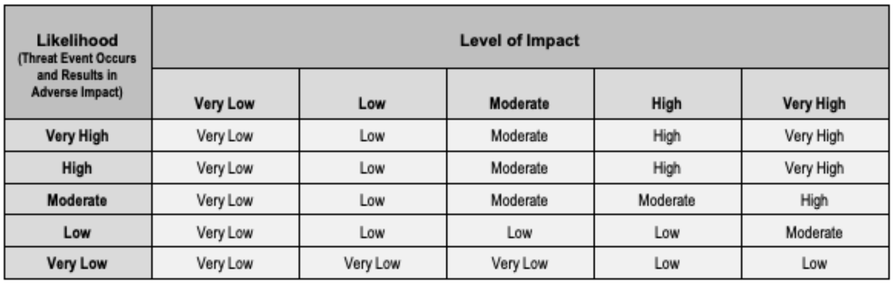
Network vulnerability scans of internal and external networks – We perform noninvasive vulnerability scans for publicly accessible networks and significant internal networks, such as server farms and backbone segments, to identify immediate system vulnerabilities.

Internal vulnerability scans of selected private and public servers – We conduct a scan of publicly accessible systems such as web servers and electronic mail gateways, as well as significant internal servers, such as application servers and file and print sharing systems, to identify vulnerabilities that cannot be found by probing external network connections.

Host vulnerability scans of desktop systems – We examine selected software images and representative desktop systems to identify security issues. Since the vast majority of systems present on corporate networks belong to end users, it is critical that desktop systems be secured against vulnerabilities that could put shared systems at risk.

## REPORT PREPARATION AND DELIVERY

Our final deliverable will include risk-ranked findings, based on the NIST 800-30 Guide for Conducting Risk Assessments, assessment scale.  This scale determines the level of risk based on a combination of likelihood and impact.  Each observation will be categorized as **VERY HIGH**, **HIGH, MODERATE, LOW,** or **VERY LOW**, based on the intersection of impact and likelihood of exploitation by a threat actor. All findings will have corresponding recommendations for improvement and remediation.



| **Likelihood** (Threat Event Occurs and Results in Adverse Impact) | **Level of Impact** | | | | |
|---|---|---|---|---|---|
| | **Very Low** | **Low** | **Moderate** | **High** | **Very High** |
| **Very High** | Very Low | Low | Moderate | High | Very High |
| **High** | Very Low | Low | Moderate | High | Very High |
| **Moderate** | Very Low | Low | Moderate | Moderate | High |
| **Low** | Very Low | Low | Low | Low | Moderate |
| **Very Low** | Very Low | Very Low | Very Low | Low | Low |

# Proposal Fee

| DESCRIPTION | FEE |
|---|---|
| **Vulnerability Assessment & Cybersecurity Risk Review***<br>**CIS Top 20 ITGC Control Review (IG3)**<br>• Test for susceptibility to Advanced Persistent Threats (APTs) such as viruses, malware, Trojan horses, botnets, and other targeted attack exploits.<br>• Evaluate the Authority's current threat posture including antivirus and Intrusion Detection and Prevention (IDP) capabilities.<br>• Evaluate the Authorities planned changes and improvements to the threat surface and assist identifying and addressing security concerns.<br>• Review the Authority's current Supervisory Control and Data Acquisition (SCADA) water systems for security vulnerabilities.<br>• Review wireless network system components for security vulnerabilities, validating system-specific operating systems and firmware versions for known exploits and recommend upgrades, updates, and mitigations.<br>• Review current system-specific operating systems and firmware versions for known exploits and recommend upgrades, updates, and mitigations. This includes firewalls, switches and routers, Microsoft Active Directory, email and file servers, web servers, wireless routers, WAN, VPN, VoIP, and CCTV systems..<br>• Assess VoIP network system components for security vulnerabilities, validating system-specific operating system and firmware versions and reviewing for known exploits.<br>• Review existing IT policies and procedures and make recommendations for changes and/or additional policy and procedure development.<br>• Execute and review internal network vulnerability scans and external vulnerability and penetration scans and make recommendations to reduce the threat attack surface.<br>• Recommend or assist in selection of vulnerability scan software for purchase/license for continued use by the Authority after the assessment is complete | **$16,500.00** |

*Required hardware (remote laptop for vulnerability scanning) and software (vulnerability scanning license) to be provided by OCD Tech

# Timeline and Project Plan

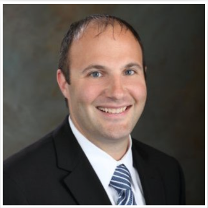
| TASK | TIMELINE |
|---|---|
| **External Vulnerability Scanning** | **1 week** |
| **Internal Vulnerability Scanning & Control Review (In Parallel)** | **2 weeks** |
| **Report Preparation, Delivery, and Review** | **2 weeks** |
| **Total Engagement Timeline** | **5 weeks** |

# References / Prior Work Experience

| ORGANIZATION | NAME | CONTACT INFO | SERVICES PROVIDED |
|---|---|---|---|
| **Bridgewater State University**<br>Approximately 10,990 students, 580 faculty & staff, 39 buildings across 278 acres | David Marion | 508-531-2389<br>dmarion@bridgew.edu | • Multi-year (2018,2019,2020) Penetration testing<br>• Vulnerability Assessment<br>• Wireless Network Assessment<br>• Simulated Insider Threat |
| **NEACH**<br>Over 4,000 active members from 400+ New England area banks, credit-unions, and corporations. Operating for nearly 50 years. | Kelley Cavanaugh | 781-321-1011<br>kcavanaugh@neach.org | • Multi-year (2016, 2017, 2018, 2019,2020) Penetration testing<br>• IT General Controls Review<br>• Vulnerability Assessment |
| **Bank*Gloucester***<br>Founded in 1887, cooperative community bank. | Patricia Natti | 978-283-8200 x 227<br>Patty Natti<br>pnatti@bankgloucester.com | • Penetration testing - external blackbox, internal grey box<br>• Blackbox phishing<br>• OSINT |
| **Peabody & Arnold**<br>Founded in 1899, Peabody & Arnold is one of Boston's oldest law firms. They are a leading regional firm with over 50 attorneys throughout the New England states (and often across the US and as far as the UK) | Gary Seiger | 617-261-5007<br>gseiger@peabodyarnold.com | • Penetration testing - external blackbox<br>• Blackbox phishing<br>• OSINT |

# Engagement Management Team

## MICHAEL HAMMOND



Michael is the Principal of IT Audit & Security at OCD Tech. With over 20 years in various strategic and operational IT positions, including 15 years designing and implementing security architecture and security controls, Michael is widely considered a foremost expert in IT security. Michael has traveled extensively as a frequent speaker on trending security topics. In addition to speaking on audit and security, Michael has performed audits and assessments on five continents spanning more than 12 regulatory authorities. Michael is also a U.S. Air Force veteran.

### AREAS OF EXPERTISE

- IT Security
- IT General Controls (ITGC)
- ISO 27001/27002, COBIT
- SOX Testing
- Server, Desktop, Storage, and Networking technologies

### EDUCATION

- University of Massachusetts Boston, Magna Cum Laude, Bachelor of Arts in Community Studies
- University of Maryland, Associates of Arts in Computer Science
- College of the Air Force, Associates of Science, Paralegal

### CERTIFICATIONS & MEMBERSHIPS

- Certified Information Systems Auditor (CISA), ISACA
- Certified in Risk and Information Systems Control (CRISC), ISACA
- Certified Information Systems Security Professional, (CISSP), ISC$^2$
- Prior certifications include Microsoft, Novell, CompTIA, and ITIL
- Member, InfraGard, a partnership between the private sector and FBI

# ROBBIE HARRIMAN

Robbie is the Senior IT Audit Manager at OCD Tech. Robbie joined the firm in May of 2016. Prior to working at O'Connor & Drew, P.C., Robbie worked in IT for other companies, including the heavily regulated casino industry. He currently travels locally and internationally working on some of OCD's largest financial services companies. He has a diverse range of experience in the IT field, with a deep background in IT systems administration and control areas.

## AREAS OF EXPERTISE

- SOX Testing, including Privilege Access Management and Direct Data Access
- IT General Controls (ITGC)
- SOX Testing
- Network Security
- LAN/WAN Administration
- Windows Domain Administration
- Backup Procedures
- Unix based Systems
- IBM iSeries

## EDUCATION

- University of Maine, Bachelor of Applied Science

## CERTIFICATIONS & MEMBERSHIPS

- Certified Information Systems Auditor (CISA) - ISACA
- Information Systems Audit and Control Association, Inc. (ISACA) member
- Southern Maine Microsoft Users Group (SMMUG) member
- ISACA CSX CyberSecurity Fundamentals certification
- CompTIA IT Fundamentals certification
- CyberArk Level 1 Trustee

# JILL KAMPERIDES

Joining the team in 2019, Jill is an IT Security Analyst focused on privately held companies and international banking clients. As lead of the penetration testing team, she utilizes her deep knowledge of programming and automation through scripting and uses that knowledge to quickly discover misconfigurations in target systems. Jill is also responsible for the OCD Tech phishing platform and oversees the maintenance of weekly client employee security awareness campaigns. Jill has contributed to the industry through CVE assignments, published articles, and speaking engagements.

## AREAS OF EXPERTISE

- IT General Controls (ITGC)
- Vulnerability assessments
- Penetration testing
- Employee Awareness and Training
- Social Engineering

## EDUCATION

- University of Massachusetts Boston, Bachelor of Arts

## CERTIFICATIONS & MEMBERSHIPS

- GIAC Certified Penetration Tester
- CyberArk Trustee Level 1
- ISACA
- InfraGard
- DoD Mandatory Controlled Unclassified Information (CUI) Certificate, Center for Development of Security Excellence, Defense Counterintelligence and Security Agency

OCD TECH, A DIVISION OF O'CONNOR & DREW, PC
25 BRAINTREE HILL OFFICE PARK, SUITE 102
BRAINTREE, MA 02184
www.ocd-tech.com • (844) OCD-TECH

Map image: http://eriecanal.org/maps.html

Date: June 11, 2021

# RESPONSE TO RFP FOR ECWA PROJECT NO. 202100116 CYBERSECURITY RISK & VULNERABILITY ASSESSMENT

Erie County
Water Authority

**Contact for RFP Response:**
**Ellen Anderson**
Government Contract and Proposal Manager
eanderson@securanceconsulting.com
P: 877.578.0215 ext. 115

SECURANCE CONSULTING
*the advantage of insight*
www.securanceconsulting.com

# TABLE OF CONTENTS

PART I 4

BUSINESS INFORMATION 5

PART II 6

CONSULTANT BUSINESS FORM 7

CONSULTANT TEAM 9

PART III 12

PROPOSED SCOPE OF SERVICE 13

BEST PRACTICE METHODOLOGIES 16

HARDWARE AND SOFTWARE REQUIREMENTS 28

TIMEFRAME FOR DELIVERABLES 29

PROJECTED SOLUTIONS AND COSTS 35

APPENDIX 37

RELEVANT CERTIFICATIONS 38

*This proposal contains confidential material proprietary to Securance Consulting. The material, ideas, and concepts contained herein are to be used solely and exclusively to evaluate the capabilities of Securance Consulting to provide assistance to Erie County Water Authority (Authority). This proposal does not constitute an agreement between Securance Consulting and the Authority. Any services Securance Consulting may provide to the Authority will be governed by the terms of a separate written agreement signed by both parties. All offers to provide professional services are valid for sixty (60) days.*

Erie County Water Authority | Cybersecurity Risk & Vulnerability Assessment

S|C SECURANCE CONSULTING

*the advantage of insight*

June 11, 2021

Terrance D. McCracken, Secretary to the Authority
Erie County Water Authority
295 Main Street, Room 350
Buffalo, New York 14203

Dear Mr. McCracken:

Thank you for considering Securance Consulting for your cybersecurity risk and vulnerability assessment. By partnering with Securance, the Erie County Water Authority (Authority) will gain key insight into the current state of its cybersecurity risk profile and a formidable ally to help protect Erie County's water, mission, people, and the extraordinary significance of its aquatic history. With Securance, the Authority can expect to receive:

**Expert knowledge of the most pernicious technology threats to water utilities.** With a top-tier team of senior cybersecurity specialists, Securance has been safeguarding American water utilities for almost two decades. Our clients include Boston Water and Sewer Commission, San Antonio Water System, Warren County Water District, City of Fort Collins Utilities, and numerous other government and municipal entities.

**A partner dedicated to the Authority's long-term success.** Your success is our success. Securance will start by fully understanding Authority's needs and then tailor an approach to achieve its objectives based on Authority's unique technology environment.

**Regular updates to Authority's Project Manager (PM).** We are committed to ensuring our clients stay fully informed throughout the assessment process. Securance will notify Authority of any urgent threats detected along the way with a priority ranking and a timeframe to address issues so that they can be handled appropriately and speedily.

**A first-class report containing actionable recommendations.** Securance produces reports detailing findings for both management and technicians and specifying remediation activities based on the latest security and controls standards and frameworks.

Securance is ready to deliver the highest level of security testing and demonstrate our commitment to Authority's mission in securing its water and cyber environment.

Thank you for including Securance in your evaluation process. Should you have any questions upon reviewing our proposal, please do not hesitate to contact me.

Professional regards,

Paul Ashe, CPA, CISA, CISSP, HCISPP
President

# PART I

# BUSINESS INFORMATION

**Name of Organization:** Securance Consulting (Securance LLC)

**Name and Title of Contact Person:** Paul Ashe, President

**Business Address**: 13904 Monroes Business Park
Tampa, Florida 33635

**Telephone No.:** 877.578.0215

**Email Address:** pashe@securanceconsulting.com

**Fax No.**: 813.328.4465

# PART II

# CONSULTANT BUSINESS FORM

## *Summary of Business*

- **Founded:** March 4, 2002 in Florida as an LLC
- **Executive officer:** Paul Ashe, President
- **Principal place of business:** Tampa, Florida
- **Principal or subsidiary corporations:** None
- **Closed or publicly traded:** Closed
- **EIN:** 03-0392503
- **Years in business:** 19 years without change in business structure
- **Insurances:**
  - Network Security & Privacy Liability, Cyber Incidents/Cyber Events: $5 million
  - Commercial General Liability: $29.260 million
  - Auto Liability: $6 million
  - Workers Compensation: $1 million

## *Similar Services Performed*

- **Boston Water and Sewer Commission**

  980 Harrison Avenue<br>
  Boston, MA 02119<br>
  Russ Murray, CIO<br>
  619.989.7669 | murrayr@BWS.org

- **Warren County Water District**

  523 U.S. Highway 31W Bypass<br>
  P.O. Box 10180<br>
  Bowling Green, KY 42102<br>
  B.J. Malone, Manager of IT/GIS<br>
  270.495.3507 | bjmalone@warrenwater.com

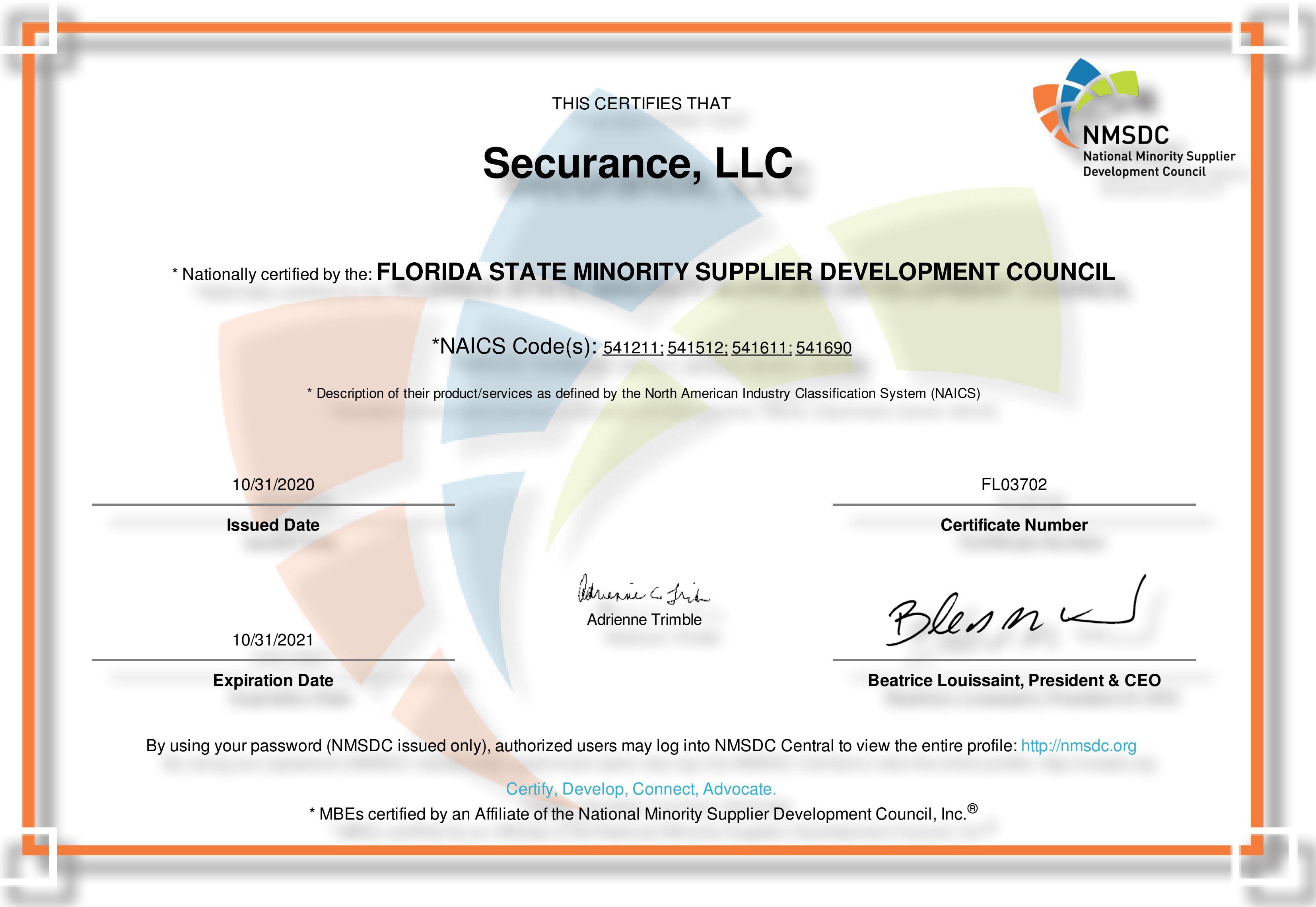
- **City of Fort Collins (Fort Collins Utilities)**

  215 North Mason Street, 2nd Floor<br>
  Fort Collins, CO 80524<br>
  Mary Evans, IT Application Services Manager - Utilities<br>
  970.221.6865 l mevans@fcgov.com

# Consultant Business Form (continued)

## MBE Certificate

*Certified Minority-Owned Business*



NMSDC
National Minority Supplier Development Council

THIS CERTIFIES THAT

**Securance, LLC**

* Nationally certified by the: **FLORIDA STATE MINORITY SUPPLIER DEVELOPMENT COUNCIL**

*NAICS Code(s): 541211; 541512; 541611; 541690

* Description of their product/services as defined by the North American Industry Classification System (NAICS)

|  |  |  |
|---|---|---|
| 10/31/2020 |  | FL03702 |
| **Issued Date** |  | **Certificate Number** |
| 10/31/2021 | Adrienne Trimble |  |
| **Expiration Date** |  | **Beatrice Louissaint, President & CEO** |

By using your password (NMSDC issued only), authorized users may log into NMSDC Central to view the entire profile: http://nmsdc.org

Certify, Develop, Connect, Advocate.

* MBEs certified by an Affiliate of the National Minority Supplier Development Council, Inc.®

# CONSULTANT TEAM

Paul has provided hands-on project management to lead Securance engagements over the past 19 years. A former IT consultant for Ernst & Young, Paul has leveraged his knowledge and experience into an effective, time- and budget-conscious project management style. He conducts cybersecurity risk and vulnerability assessments, reviews, and technology-specific vulnerability and penetration tests for clients in every industry and is an expert in implementing and assessing security frameworks.

## EDUCATION

**Master of Science**

Accounting Information Systems

**Bachelor of Science**

Accounting and Management Information Systems

## PAUL ASHE 23 Years' Experience

President and Engagement Manager

Securance Consulting — 19 Years

Hillsborough County, Florida

### CERTIFICATIONS

CISSP® CISA HCISPP®

Please see the Appendix beginning on page 47 for certifications.

### RELEVANT EXPERIENCE/SCOPE OF RESPONSIBILITY

- Cybersecurity process assessments for utilities against NIST, ISO, CIS, COBIT, ISACA, ACFE, AICPA, and IIA standards
- Technical security assessments, including: internal | external networks; industrial control systems; web- and cloud-based applications; and, device and operating system configurations
- Vulnerability management program review and design
- U.S. Government Accountability Office (GAO) framework
- Institute of Internal Audit Practice Standards
- Evaluation of policies and procedures against organizations standards and industry best practices
- System implementation audits
- Risk assessments

### RECENT PROJECTS

Boston Water and Sewer Commission

City of Fort Collins Utilities

Seminole Electric Cooperative, Inc.

Louisville Jefferson County 1778

Lewisville Deep Roots. Broad Wings. Bright Future.

WCWD Warren County Water District

## Consultant Team

### Resumes

## Chris Bunn 30 Years' Experience

Practice Director and Senior IT Security Consultant

Securance Consulting — 8 Years

Hillsborough County, Florida

Chris is an expert in IT security and risk assessment | management from best practice control frameworks to cloud security assessments to international, federal, state, and industry-specific security regulations. With more than 30 years of IT experience, Chris' expertise in improving IT processes, evaluating application security, assessing and remediating potential threats, and resolving issues caused by internal and external cyber attacks has benefited numerous city and state government entities.

**EDUCATION**

**Master of Science**

Management Information Systems

**Bachelor of Science**

Computer Science for Business

### CERTIFICATIONS

CISSP®

CHP Certified HIPAA Professional
HIPAA Academy

### RELEVANT EXPERIENCE/SCOPE OF RESPONSIBILITY

» Cybersecurity business process audits for utilities, government agencies, and corporations in various critical infrastructure sectors

» Compliance with cybersecurity and control-based frameworks, including NIST, ISO, CIS 20, and COBIT

» Evaluation of policies and procedures against organizational standards and industry best practices

» Audit program development and execution in accordance with ISACA, ACFE, AICPA, and IIA standards

### RECENT PROJECTS

City of Phoenix

CITY OF DURHAM

LOUISVILLE 1778 JEFFERSON COUNTY 1778

Boston Water and Sewer Commission

the ENERGY cooperative
Your Touchstone Energy® Partner

# Consultant Team

## Resumes (continued)

Ray, a retired Commander and Special Operations Officer for the U.S. Navy, specializes in analyzing organizational security needs, assessing existing security posture, and implementing plans to mitigate risks to an acceptable level. He has the ability to translate highly technical topics into plain language.

### EDUCATION

**Bachelor of Science**

Accounting

## Ray Resnick 20 Years' Experience

Senior IT Security Consultant

Securance Consulting — 2.5 Years

Hillsborough County, Florida

### CERTIFICATIONS

EC-Council C|EH CERTIFIED

CISSP®

CISM

CompTIA Security+ CERTIFIED • CE

CISCO CERTIFIED CCNA Security

CDPSE

### RELEVANT EXPERIENCE/SCOPE OF RESPONSIBILITY

- » Threat intelligence
- » Risk and threat analysis
- » Vulnerability assessments Penetration testing
- » Data loss prevention
- » IT security
- » Disaster recovery planning
- » Application and database security
- » Intrusion detection | intrusion prevention system deployment

### RECENT PROJECTS

WC WD Warren County Water District

PIONEER electric cooperative — A Touchstone Energy® Cooperative

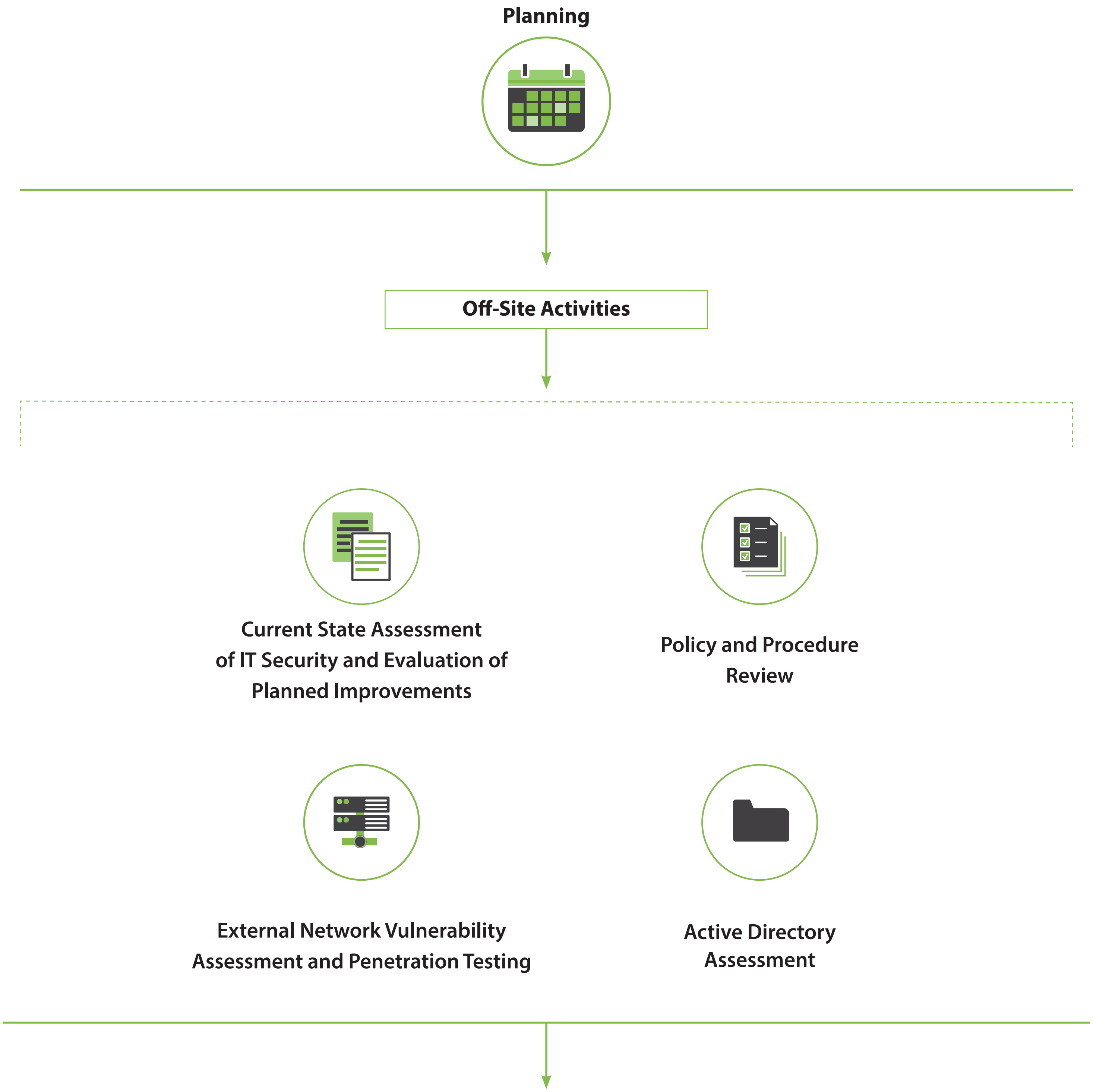
LOUISVILLE 1778 JEFFERSON COUNTY

CITY OF DURHAM

Four County Electric Membership Corporation — A Touchstone Energy® Cooperative

# PART III

# PROPOSED SCOPE OF SERVICE



Planning

Off-Site Activities

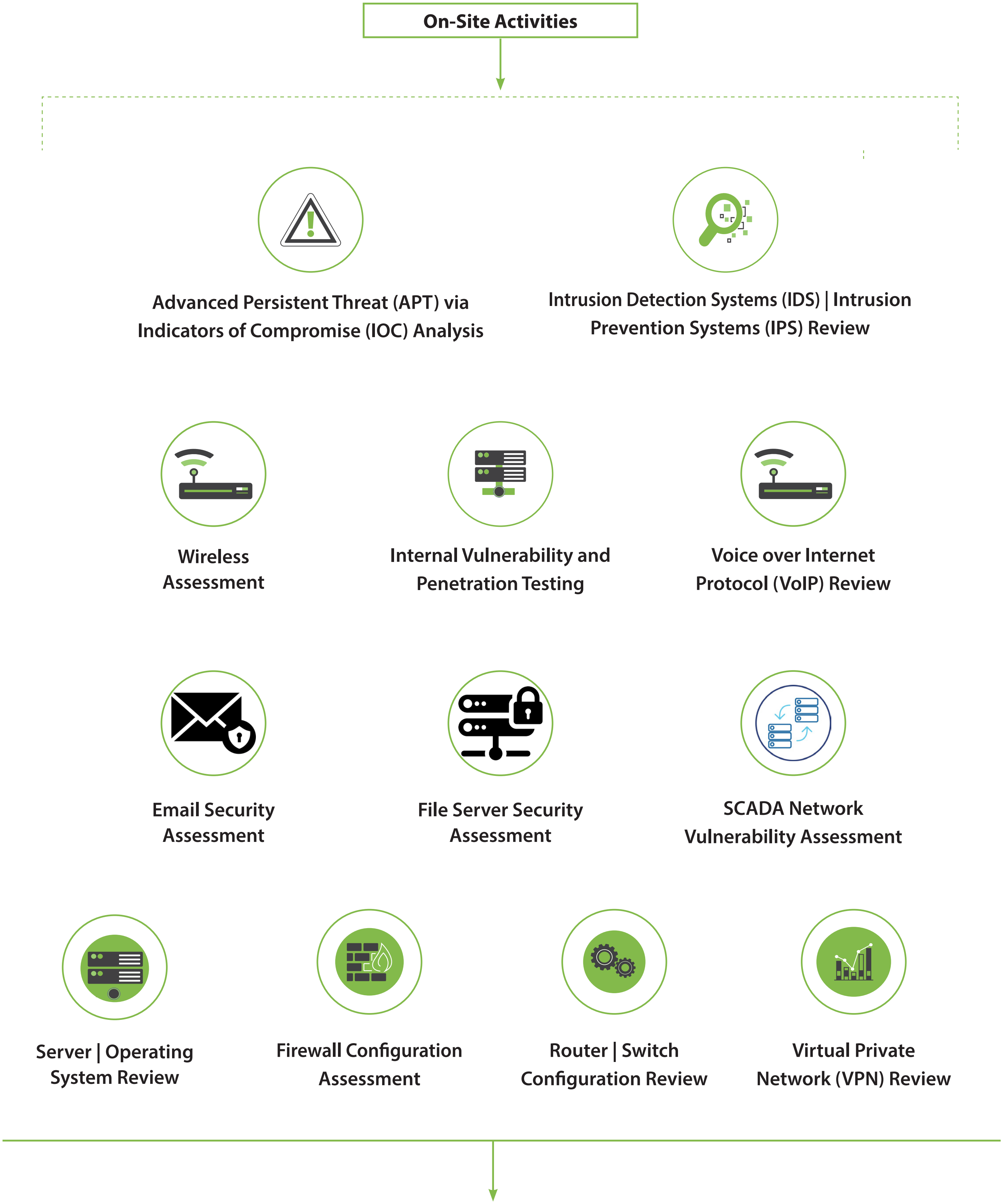
Current State Assessment of IT Security and Evaluation of Planned Improvements

Policy and Procedure Review

External Network Vulnerability Assessment and Penetration Testing

Active Directory Assessment

## Proposed Scope of Service (continued)



On-Site Activities

Advanced Persistent Threat (APT) via Indicators of Compromise (IOC) Analysis

Intrusion Detection Systems (IDS) | Intrusion Prevention Systems (IPS) Review

Wireless Assessment

Internal Vulnerability and Penetration Testing

Voice over Internet Protocol (VoIP) Review

Email Security Assessment

File Server Security Assessment

SCADA Network Vulnerability Assessment

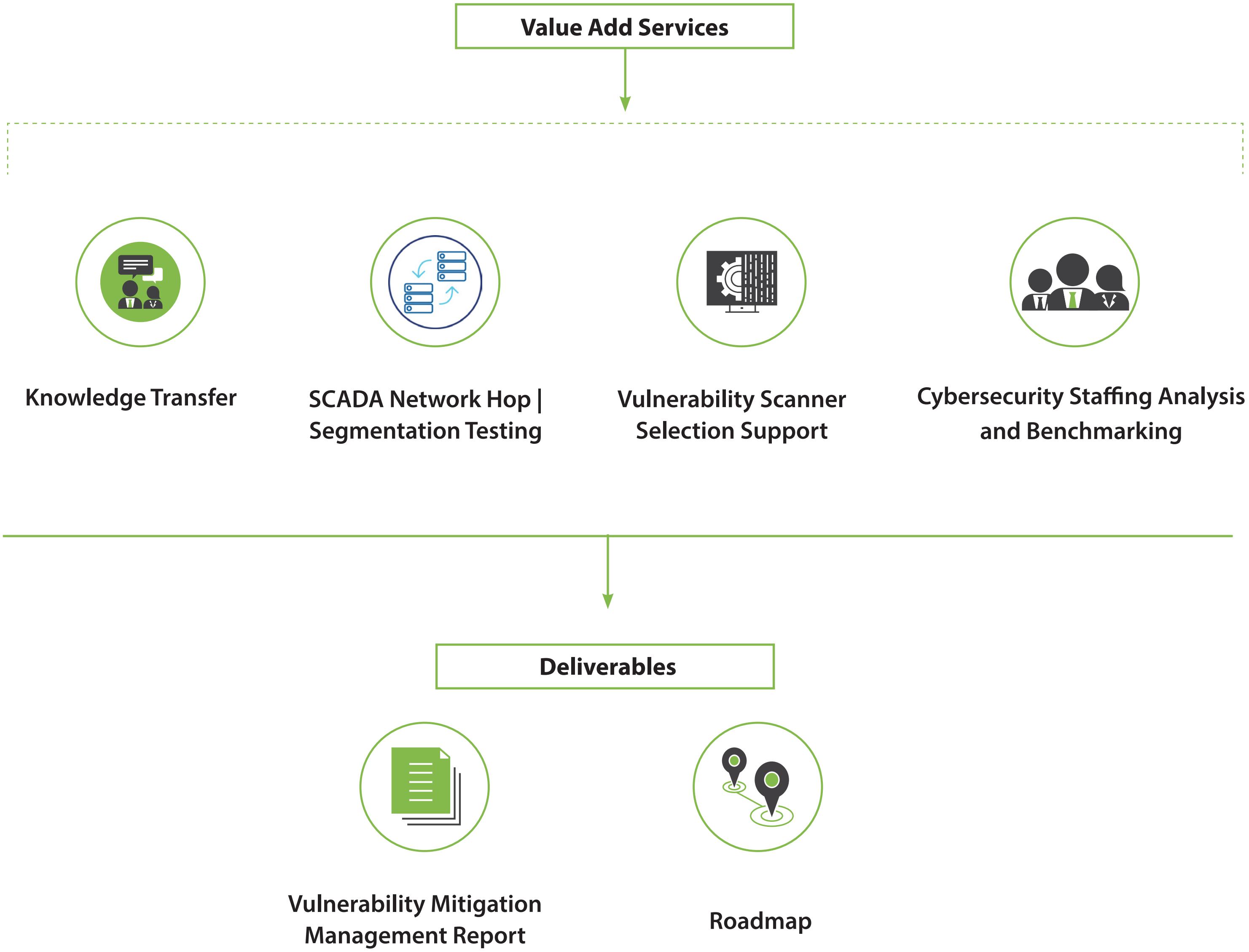
Server | Operating System Review

Firewall Configuration Assessment

Router | Switch Configuration Review

Virtual Private Network (VPN) Review

## Proposed Scope of Service (continued)



Value Add Services

Knowledge Transfer

SCADA Network Hop | Segmentation Testing

Vulnerability Scanner Selection Support

Cybersecurity Staffing Analysis and Benchmarking

Deliverables

Vulnerability Mitigation Management Report

Roadmap

# BEST PRACTICE METHODOLOGIES

## NIST CSF & CIS CSC Assessments

IT general controls (ITGC) are the foundation of the IT organization and ensure the integrity of data and processes supporting IT systems, including applications, databases, and infrastructure. Our assessment approach begins with understanding the organization's business objectives and strategies and aligns with NIST CSF and CIS CSC.

**Business and IT objectives and strategy**

- Asset management
- Business environment

**IT Governance**

- Risk assessment
- Risk management
- Supply chain risk management

**Architecture**

- Identity management, authentication, and access control

**IT operations**

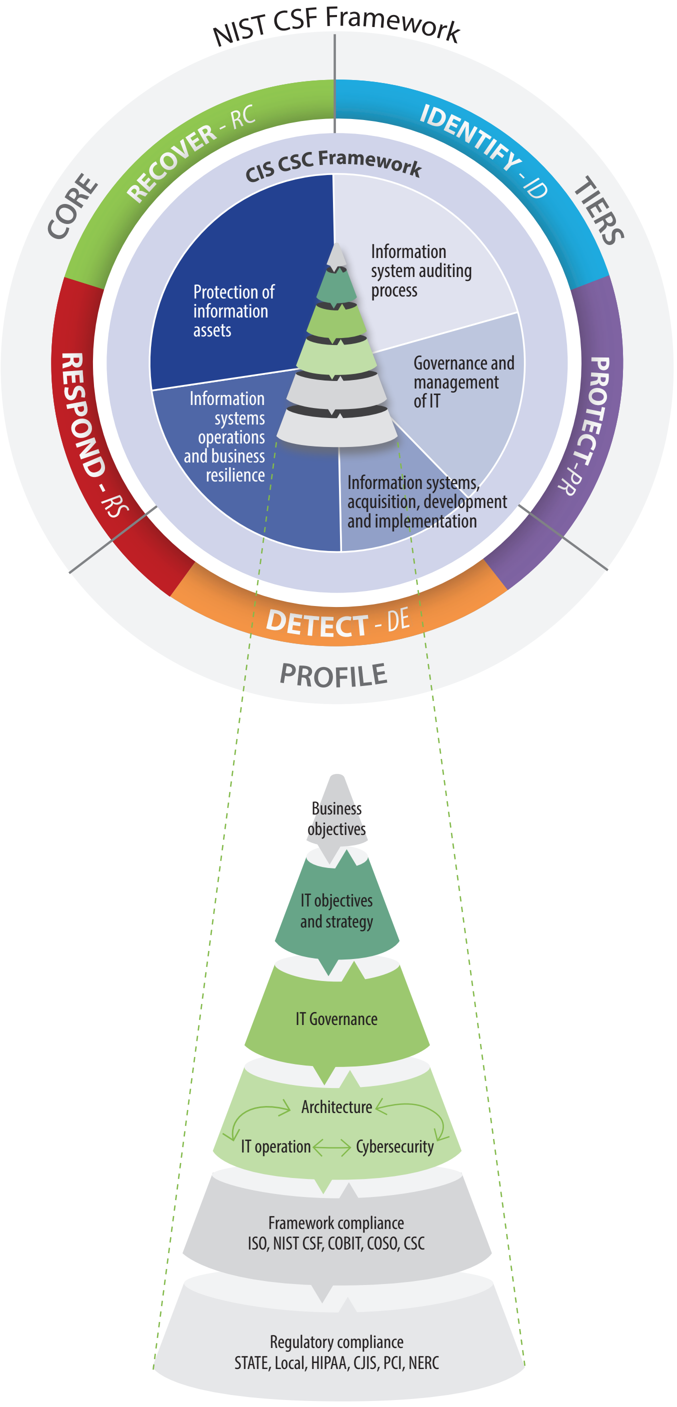
- Awareness and training
- Data security
- Information protection processes and procedures
- Maintenance
- Protective technology

**Cybersecurity program**

- Anomalies and events
- Security continuous monitoring
- Detection process
- Analysis
- Mitigation
- Improvements
- Recovery planning
- Improvements
- Communications

- **Framework compliance**

- **Regulatory compliance**


NIST CSF Framework
CORE
TIERS
PROFILE
RECOVER - RC
IDENTIFY - ID
PROTECT - PR
DETECT - DE
RESPOND - RS
CIS CSC Framework
Protection of information assets
Information system auditing process
Governance and management of IT
Information systems, acquisition, development and implementation
Information systems operations and business resilience
Business objectives
IT objectives and strategy
IT Governance
Architecture
IT operation
Cybersecurity
Framework compliance
ISO, NIST CSF, COBIT, COSO, CSC
Regulatory compliance
STATE, Local, HIPAA, CJIS, PCI, NERC

**Securance Proprietary Methodology**

# Best Practice Methodologies

## NIST CSF & CIS CSC Assessments (continued)

### Our Process

Access key people, processes, and technologies against the CIS Critical Security Controls to identify control gaps

Review IT governance documents, including IT charters, policies, procedures, standards, and guidelines

Conduct interviews with relevant IT staff to confirm IT controls and technologies that align with CIS Critical Security Controls

Perform a gap analysis of the current tier level of security and control against CIS Critical Security Controls

Develop a current state framework profile for Authority based on:

CIS Critical Security Controls tiers of:

- Basic: Control 1–6
- Foundational: Controls 7–16
- Organizational: Controls 17–20

NIST CSF tiers of:

- Tier 1: Partial
- Tier 2: Risk-informed
- Tier 3: Repeatable
- Tier 4: Adaptive

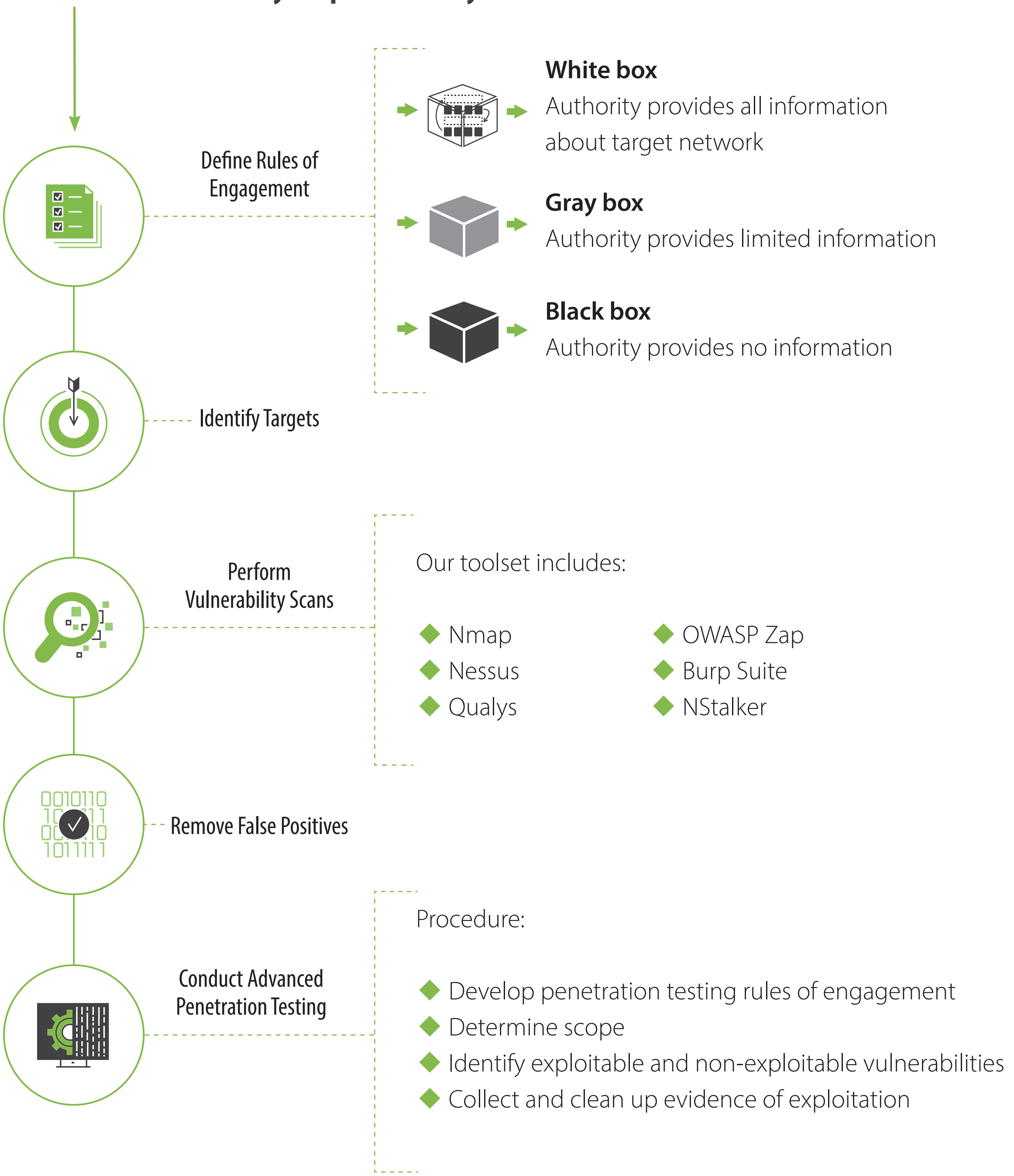
Develop a NIST CSF roadmap documenting how to improve tier level for each CIS Critical Security Control

## Best Practice Methodologies

### External | Internal Network Vulnerability Assessment and Advanced Penetration Test

Our External | Internal Network Vulnerability Assessment is aligned with industry-leading frameworks, such as NIST SP 800-115, ISSAF, OSSTMM, and OWASP.

**Securance communicates every step of the way**



Define Rules of Engagement

**White box**
Authority provides all information about target network

**Gray box**
Authority provides limited information

**Black box**
Authority provides no information

Identify Targets

Perform Vulnerability Scans

Our toolset includes:

- Nmap
- Nessus
- Qualys
- OWASP Zap
- Burp Suite
- NStalker

Remove False Positives

Conduct Advanced Penetration Testing

Procedure:

- Develop penetration testing rules of engagement
- Determine scope
- Identify exploitable and non-exploitable vulnerabilities
- Collect and clean up evidence of exploitation

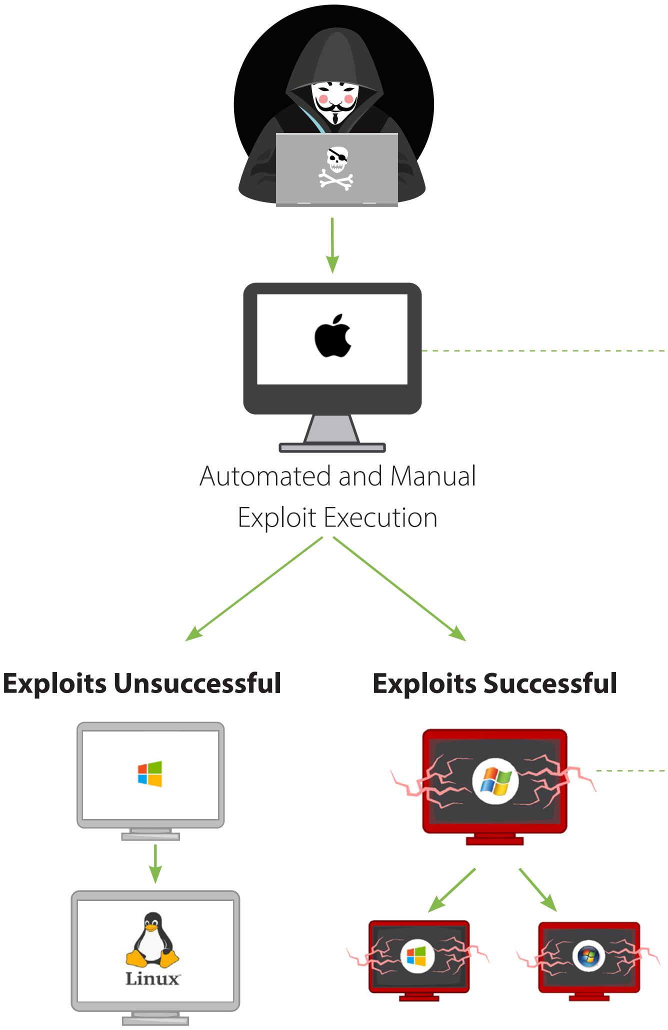
# Best Practice Methodologies

## External | Internal Network Vulnerability Assessment and Advanced Penetration Test (continued)

### Securance's Ethical Penetration Testing Process

Securance will assess Authority's network monitoring and security defense measures, including:

- Network Packet Capture
- SIEM monitoring ACL Effectiveness
- IDS | IPS Effectiveness
- Firewall Effectiveness



Automated and Manual Exploit Execution

**Exploits Unsuccessful**

**Exploits Successful**

Our toolset includes, but may not be limited to:

- Metasploit
- Core Impact
- Canvas
- Manual Exploits
- Wireshark

Other tools will be used, as required, for specific tasks.

To successfully exploit vulnerabilities, we will:

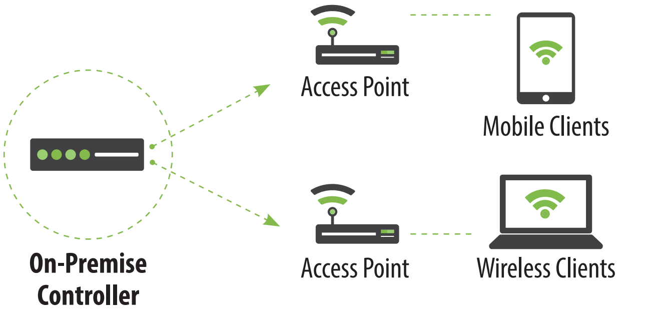
- Move laterally in the environment, evading countermeasures while remaining undetected
- Escalate account privileges, (e.g., password cracking)
- Attempt to exfiltrate data
- Leave trophy
- Clean up the environment

# Best Practice Methodologies

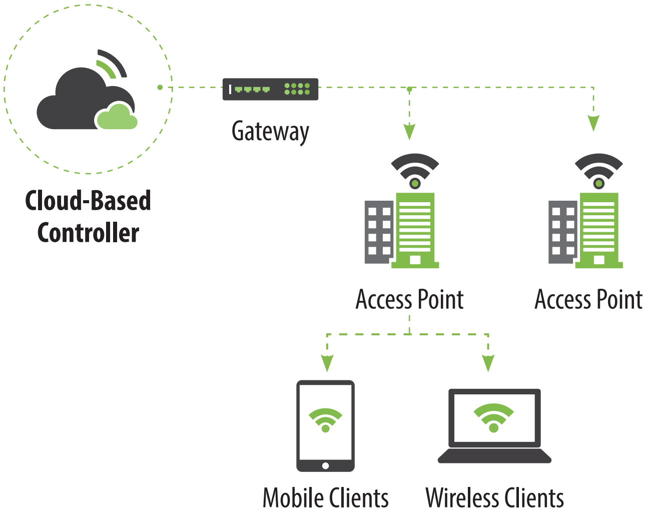
## Wireless Network Assessment

Securance assesses the configuration and security of both controller and access point-based wireless networks.

### Controller-Based Networks

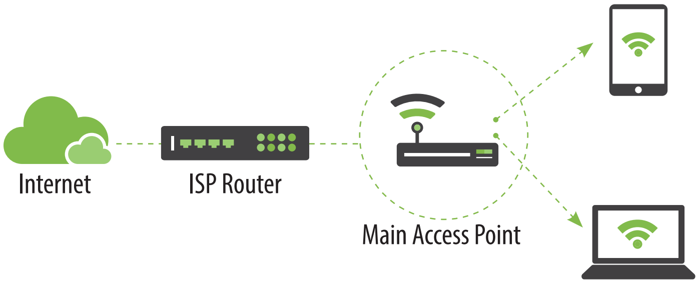


- Assess controller configurations
- Evaluate rogue access point detection and management
- Uncover or identify hidden SSIDs
- Assess encryption strength
- Review network segmentation
- Review administrative access controls and logging
- Confirm access points can only receive configurations from the controller



We will evaluate cloud-based WiFi networks to the extent allowed by the cloud provider for the controls listed above.

### Access Point-Based Wireless Networks



Our AP-based assessment is similar to our on-premise controller-based network assessment. However, because each AP has its own configuration we will assess each AP individually.

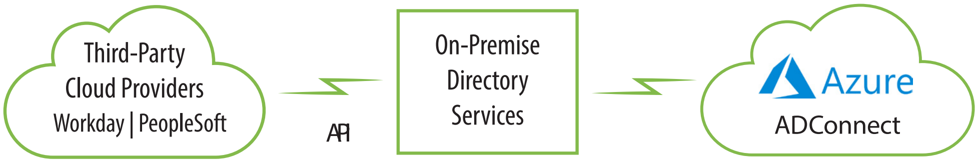
# Best Practice Methodologies

## Active Directory Assessment

Securance's methodology for assessing the security of directory services, such as Active Directory (AD), is comprehensive and supports testing the entire architecture, users, and assets to decrease the likelihood of abuse and escalation attacks.

## Our Process

### Gain an understanding of the AD architecture



### Review AD configuration

- Gain an understanding and assess the design of directory services and trust relationships
- Assess domain structure
- Assess domain policies (e.g., group policy object, audit, password)
- Assess user and computer attributes
- Compare AD configuration and security to industry standards and best practices

### Review InTune configuration

- Gain an understanding of Authority's IT environment
- Assess the structure of InTune and how it is used by Authority
- Review configurations within each existing policy, such as:
  - Compliance
  - Conditional access
  - Configuration

****
Devices
Policies
Configuration
Settings

# Best Practice Methodologies

## Active Directory Assessment (continued)

### Perform application programming interface (API) technical testing

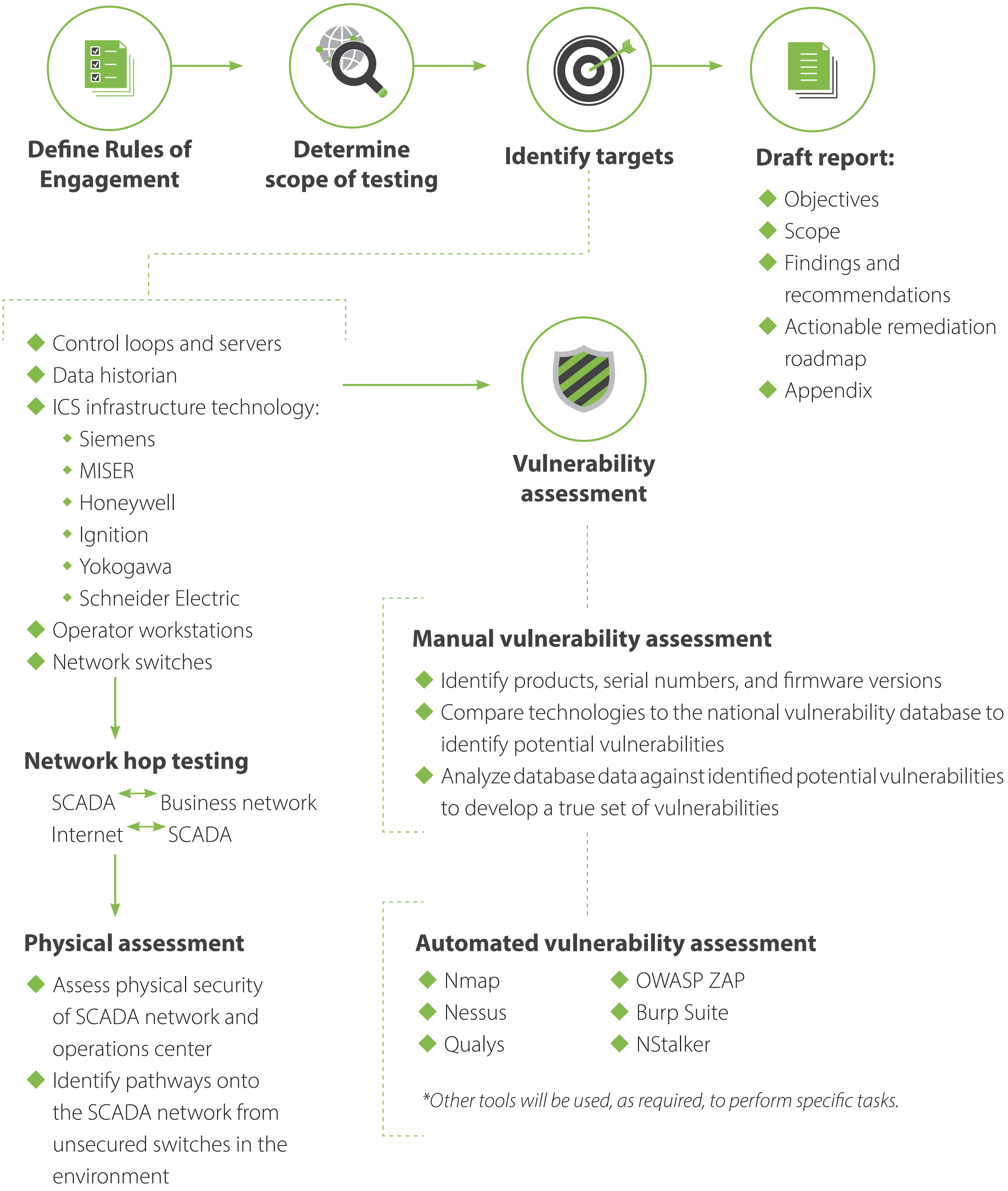
Perform manual and automated testing, including a review of API integration. Our primary tools will be OWASP ZAP and Burp Suite Pro.

Test each API for vulnerabilities in the following attack categories:

- Authentication
- Authorization
- Client-side threats
- Cryptography | encryption
- Strength
- Deployment management
- Error handling
- Identity management
- Input validation
- Injection vulnerability
- Logic and business flow
- Session management

# Best Practice Methodologies

## Industrial Control Systems | SCADA Assessment



**Define Rules of Engagement**

**Determine scope of testing**

**Identify targets**

**Draft report:**

- Objectives
- Scope
- Findings and recommendations
- Actionable remediation roadmap
- Appendix

- Control loops and servers
- Data historian
- ICS infrastructure technology:
  - Siemens
  - MISER
  - Honeywell
  - Ignition
  - Yokogawa
  - Schneider Electric
- Operator workstations
- Network switches

**Vulnerability assessment**

### Network hop testing

SCADA ↔ Business network
Internet ↔ SCADA

### Physical assessment

- Assess physical security of SCADA network and operations center
- Identify pathways onto the SCADA network from unsecured switches in the environment

### Manual vulnerability assessment

- Identify products, serial numbers, and firmware versions
- Compare technologies to the national vulnerability database to identify potential vulnerabilities
- Analyze database data against identified potential vulnerabilities to develop a true set of vulnerabilities

### Automated vulnerability assessment

- Nmap
- Nessus
- Qualys
- OWASP ZAP
- Burp Suite
- NStalker

**Other tools will be used, as required, to perform specific tasks.*

# Best Practice Methodologies

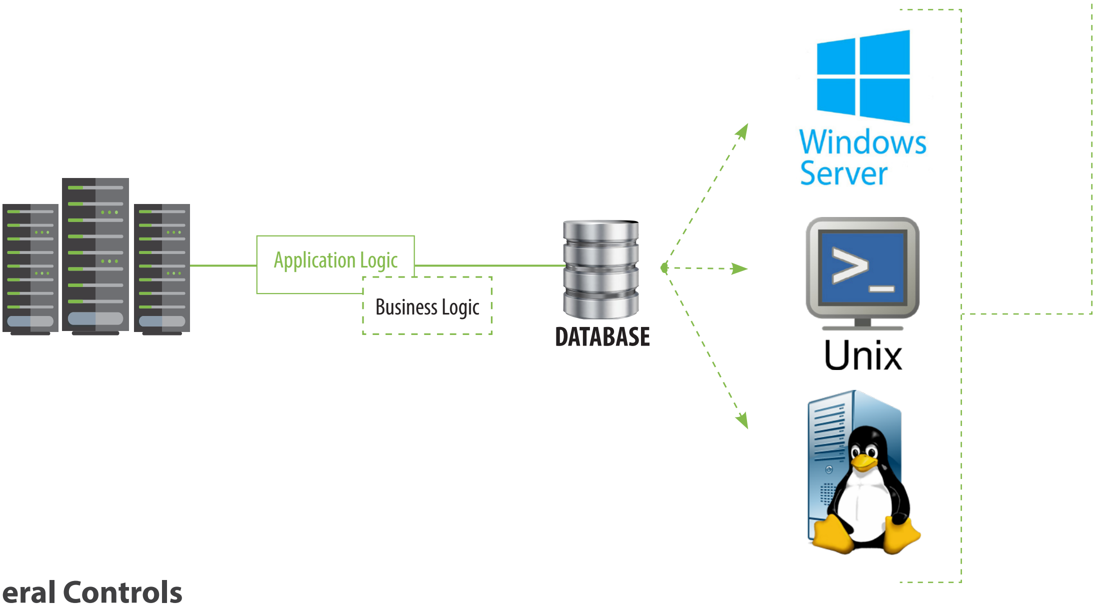
## Server | Operating System Review

Securance's methodology for assessing server security includes reviews of operating system (OS) configurations and governing general computing controls.

### ● Operating System Layer

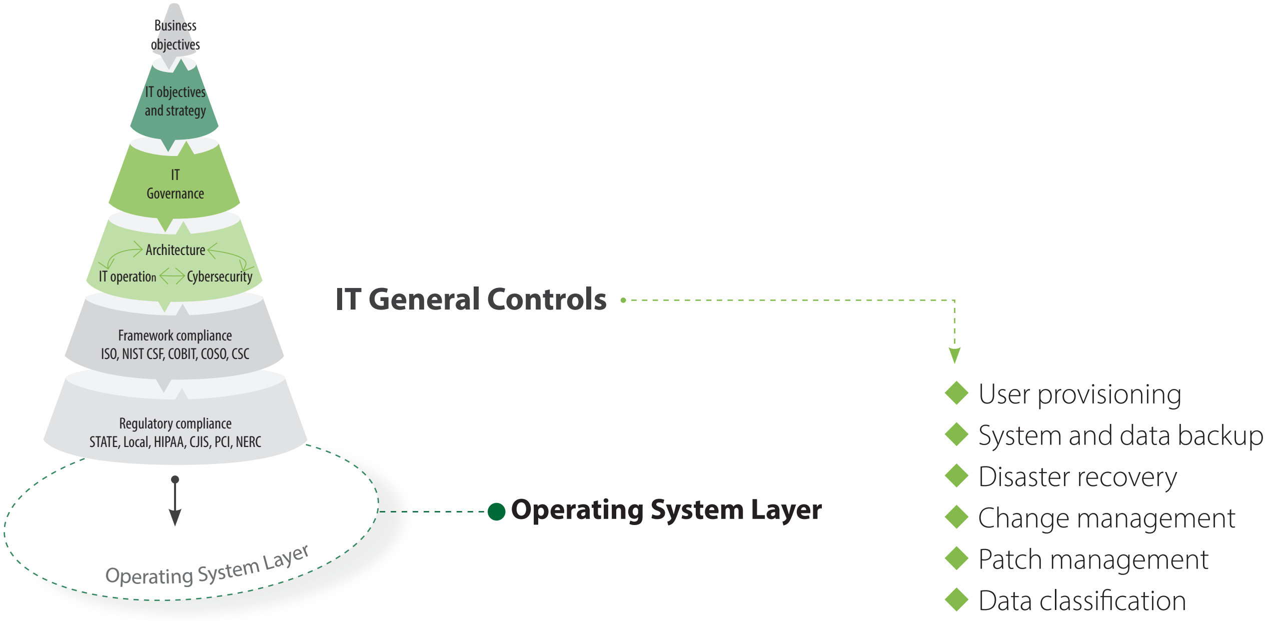
We will evaluate each server OS for:

- OS-level vulnerabilities
- Configuration assessed against CIS and/or DISG Standards
- Configuration assessed against best practices and the Authority's standards



### IT General Controls

We will assess the IT general controls supporting the server environment and compare them to NIST and CIS.



- User provisioning
- System and data backup
- Disaster recovery
- Change management
- Patch management
- Data classification

# Best Practice Methodologies

## Router | Switch Configuration Review

The Securance methodology for evaluating the security of network devices, such as routers and switches, focuses on ensuring these components are correctly configured and are creating and maintaining a secure network devoid of infrastructural gaps.

## Our Process

### Pre-Assessment

Interview device administrator(s) to gain a preliminary understanding of the devices in the network and their current configurations

### Analysis

#### Review

Perform a manual, line-by-line review of device configuration, including:

- Up-to-date firmware
- Strong access control
- Disuse of default passwords
- Change management procedures in place
- Unused ports are disabled
- Misuse of insecure protocols
- Routers eliminate generic classes of undesired traffic before they reach the firewall
- External router bins unknown protocols not provisioned in DMZs
- Routers are intelligently and securely configured and leveraged effectively
- External router does not forward private IPs; internal core router does not forward connections originating from an Internet IP address

#### Gap Analysis

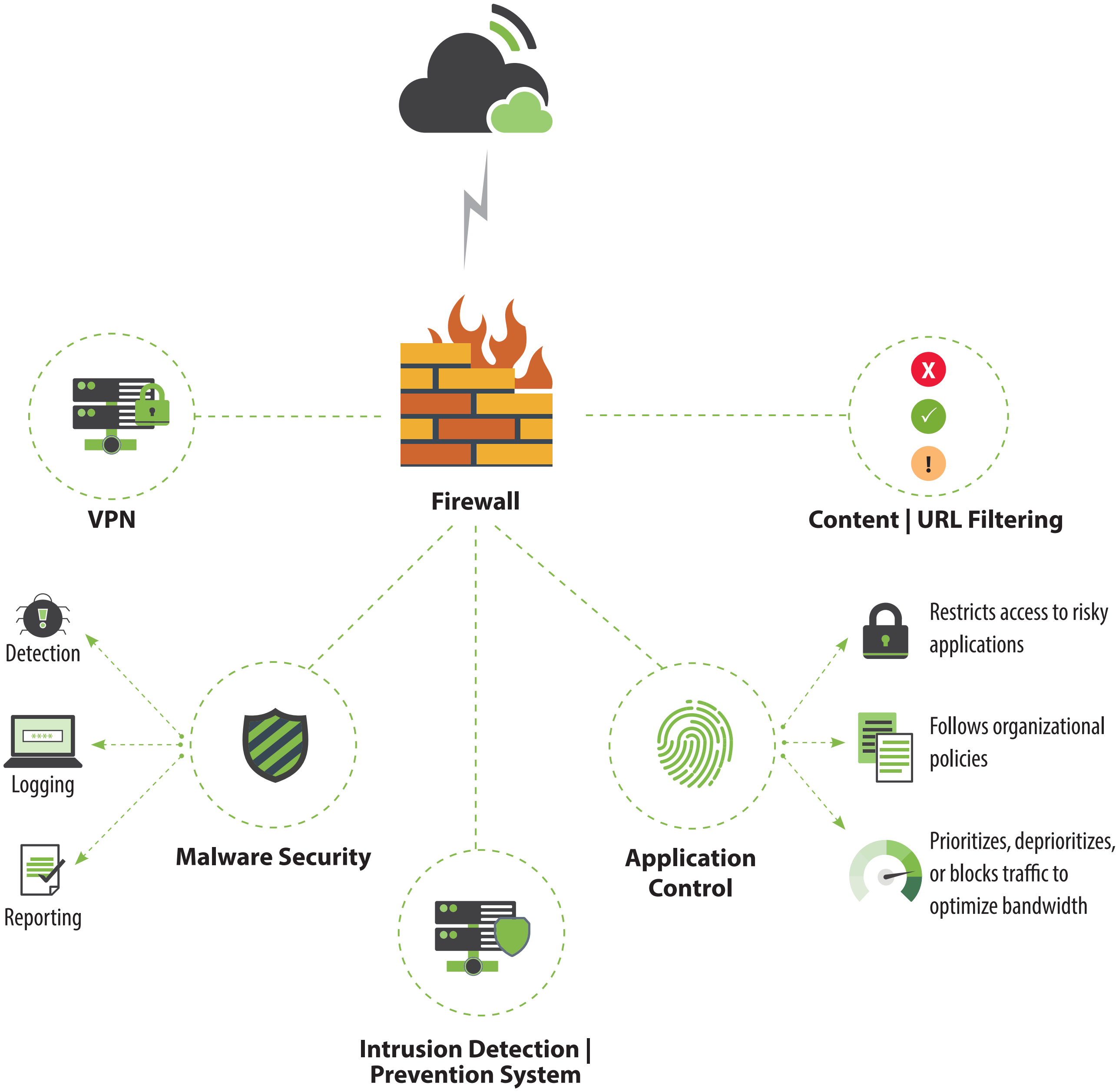
Compare device configuration and policies to the Center for Internet Security (CIS) benchmarks and identify gaps

## Best Practice Methodologies

### Next-Generation Firewall Assessment

Next generation firewalls (NGFW) are complex devices that provide all-in-one network protection via multiple security applications and technologies in one solution. They are managed by sophisticated rules that require regular review and updates to function effectively.

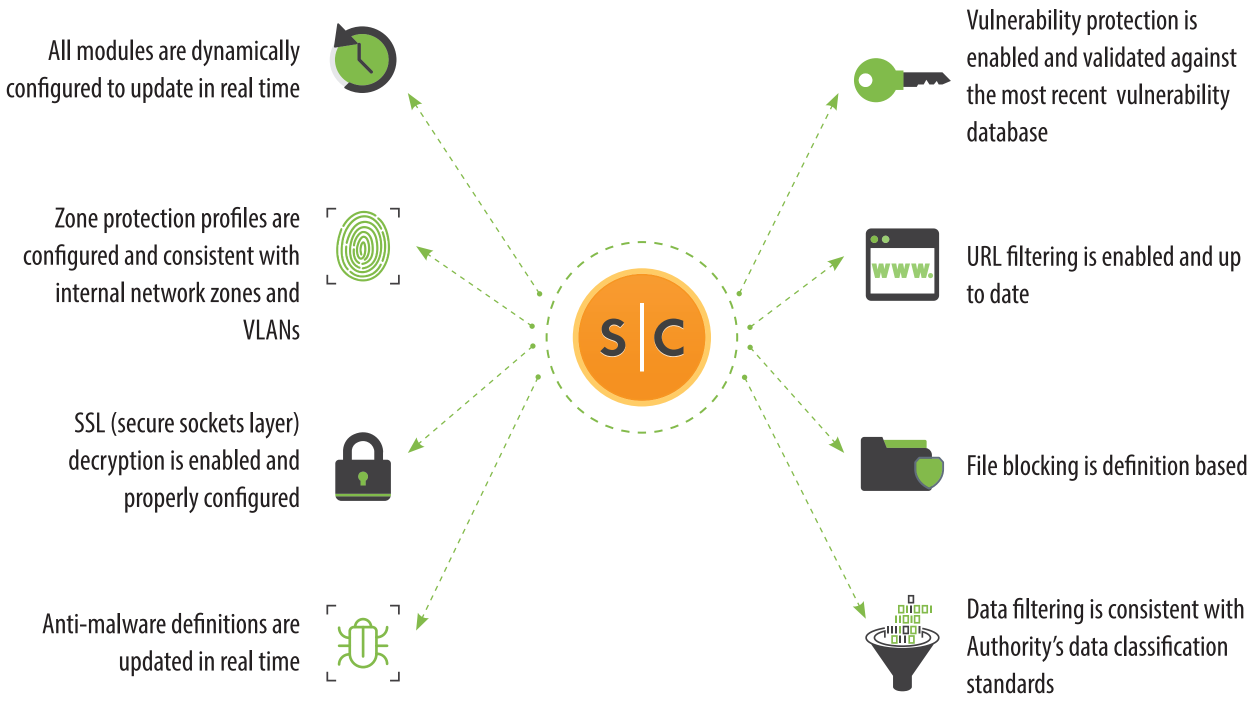
Securance's approach to performing NGFW configuration reviews covers misconfigurations, vulnerabilities, and other weaknesses that could leave an organization susceptible to attack. Our comprehensive assessment includes evaluations of the modules below.


VPN
Firewall
X
✓
!
Content | URL Filtering
Detection
****
Logging
Reporting
Malware Security
Restricts access to risky applications
Follows organizational policies
Prioritizes, deprioritizes, or blocks traffic to optimize bandwidth
Application Control
Intrusion Detection | Prevention System

# Best Practice Methodologies

## Next-Generation Firewall Assessment (continued)

We will ensure:



All modules are dynamically configured to update in real time

Zone protection profiles are configured and consistent with internal network zones and VLANs

SSL (secure sockets layer) decryption is enabled and properly configured

Anti-malware definitions are updated in real time

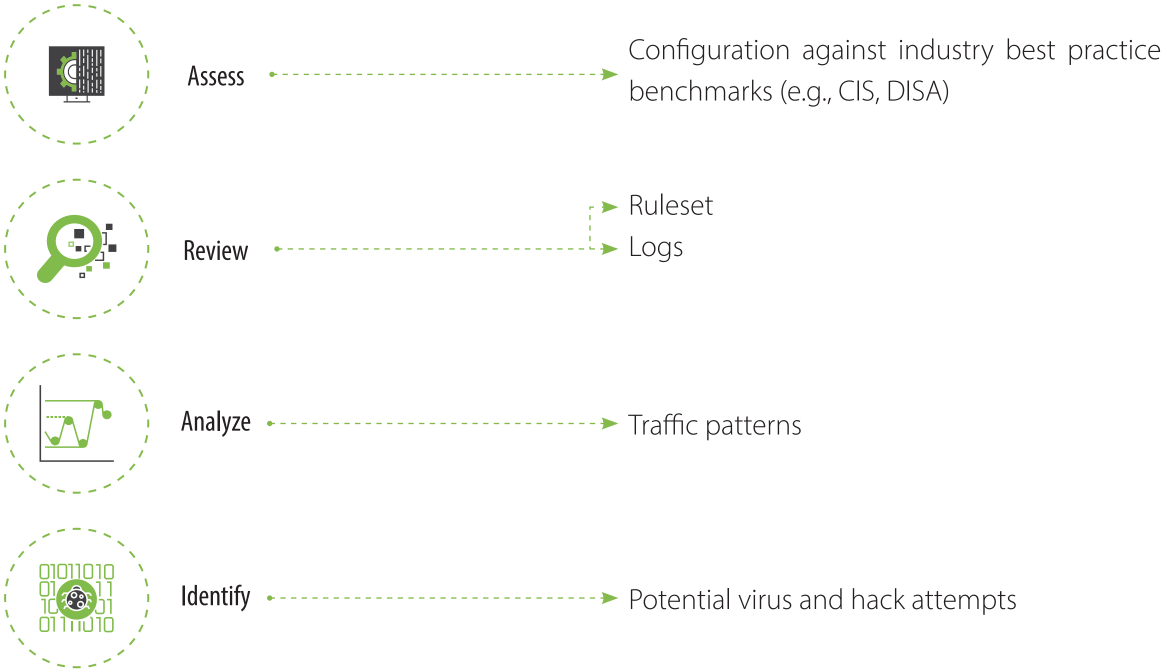
Vulnerability protection is enabled and validated against the most recent vulnerability database

URL filtering is enabled and up to date

File blocking is definition based

Data filtering is consistent with Authority's data classification standards

We will evaluate the configuration of the NGFW, ensuring it aligns with Authority's network environment and security goals, including:



Assess → Configuration against industry best practice benchmarks (e.g., CIS, DISA)

Review → Ruleset, Logs

Analyze → Traffic patterns

Identify → Potential virus and hack attempts

# HARDWARE AND SOFTWARE REQUIREMENTS

## Hardware and Software Requirements

Our consultants will use Securance-provided laptops to conduct all work throughout the performance of Authority's engagement. Box.com, a cloud content management and file sharing service, will be used to transfer data between Authority and the Securance teams. Outside of access to the systems being tested, no additional hardware or software will be required from Authority.

There are no limitations on the services being provided and no equipment being proposed.

Securance will provide a link to Box.com for the secure sharing of documentation.

# TIMEFRAME FOR DELIVERABLES

The chart below schedules each step in our cybersecurity risk and vulnerability assessment process, designating major tasks, weekly status reports, projected costs and hours, and task owner. This timeframe will be refined during the planning phases of the engagement between Securance and Authority.

| **ECWA Cybersecurity Risk & Vulnerability Assessment** | Week 1 | Week 2<br>▼ | Resource | SC Personnel Estimated Hours | Authority Personnel Estimated Hours |
|---|---|---|---|---|---|
| Kick-off Meeting | ■ | | Paul Ashe<br>Authority PM | 4 | 1 |
| Current State Assessment of IT Security | | ■ | SC Consultants | 24 | 0 |
| Evaluation of Planned Improvements | | ■ | SC Consultants | 8 | 0 |
| Review of IT Policies and Procedures | | ■ | SC Consultants | ▨ | ▨ |
| Evaluate current policies to ensure they include essential components | | ■ | SC Consultants | 10 | 0 |
| Perform comparative analysis against best practices | | ■ | SC Consultants | 4 | 0 |
| Document observations and gaps | | ■ | SC Consultants | 2 | 0 |
| APT Testing via IoC Analysis | | ■ | SC Consultants | ▨ | ▨ |
| Profile the network | | ■ | SC Consultants | 3 | 0 |
| Determine normal state behavior | | ■ | SC Consultants | 5 | 0 |
| Identify critical systems at risk | | ■ | SC Consultants | 5 | 0 |
| Gather system logs and historical data, and use forensic tools | | ■ | SC Consultants | 6 | 0 |
| Perform forensic analysis | | ■ | SC Consultants | 6 | 0 |
| Determine if there is any benign code | | ■ | SC Consultants | 5 | 0 |
| Determine initial point(s) of compromise | | ■ | SC Consultants | 2 | 0 |
| IDS \| IPS Configuration Assessment | | ■ | SC Consultants | ▨ | ▨ |
| Perform line-by-line review of the IPS \| ATD configuration | | ■ | SC Consultants | 8 | 0 |
| Evaluate detection capabilities and actions taken when a malicious event is detected | | ■ | SC Consultants | 2 | 0 |
| Review processes for prioritizing events, sending alerts, tracking \| documenting incidents, and data aggregation | | ■ | SC Consultants | 2 | 0 |

▼ PROJECT STATUS MEETINGS ◆ WORK PRODUCT REVIEWS

## TimeFrame for Deliverables (continued)

| **ECWA Cybersecurity Risk & Vulnerability Assessment** | Week 2 ▼ | Resource | SC Personnel Estimated Hours | Authority Personnel Estimated Hours |
|---|---|---|---|---|
| WIFI Vulnerability Assessment and Pen Test | | SC Consultants | ▨ | ▨ |
| Identify controllers and SSIDs | | SC Consultants | 4 | 0 |
| Interview wireless network administrator (NA) | | SC Consultants<br>Authority NA | 1 | 1 |
| Perform wireless network scanning | | SC Consultants | 6 | 0 |
| Obtain \| assess wireless or AP configuration | | SC Consultants | 5 | 0 |
| Perform manual penetration activities | | SC Consultants | 8 | 0 |
| Analyze results \| review with wireless administrator (WA) | ◆1 | SC Consultants<br>Authority WA | 2 | 1 |
| External Network VA and Pen Test | | SC Consultants | ▨ | ▨ |
| Perform information gathering of Public Info | | SC Consultants | 2 | 0 |
| Perform vulnerability scanning | | SC Consultants | 3 | 0 |
| Analyze results to remove false positives | | SC Consultants | 2 | 0 |
| Review results of scan with Authority PM | ◆2 | Paul Ashe<br>Authority PM | 1 | 1 |
| Identify hosts to attempt to exploit and confirm with client | | SC Consultants | 1 | 0 |
| Perform exploit testing | | SC Consultants | 4 | 0 |
| Extend testing to escalate privileges and move laterally in environment | | SC Consultants | 2 | 0 |
| Review results with client | ◆3 | Paul Ashe<br>Authority PM | 1 | 1 |

▼ PROJECT STATUS MEETINGS ◆ WORK PRODUCT REVIEWS

## TimeFrame for Deliverables (continued)

| **ECWA Cybersecurity Risk & Vulnerability Assessment** | Week 3 ▼ | Resource | SC Personnel Estimated Hours | Authority Personnel Estimated Hours |
|---|---|---|---|---|
| VoIP Security Assessment | | SC Consultants | ▨ | ▨ |
| Gain an understanding of the VoIP architecture | | SC Consultants | 2 | 0 |
| Identify security controls protecting the environment | | SC Consultants | 2 | 0 |
| Assess each server in the environment for vulnerabilities | | SC Consultants | 4 | 0 |
| Assess the configuration of the underlying OS | | SC Consultants | 4 | 0 |
| Assess the configuration of the VoIP solution | | SC Consultants | 4 | 0 |
| Assess the permissions to voicemail | | SC Consultants | 2 | 0 |
| Active Directory Assessment | | SC Consultants | ▨ | ▨ |
| Extract data for analysis | | SC Consultants | 8 | 0 |
| Review settings | | SC Consultants | 18 | 0 |
| Compare configuration \| security to industry standards and best practices | | SC Consultants | 6 | 0 |
| Email Security Assessment | | SC Consultants | ▨ | ▨ |
| Gain an understanding of the on-premise Email solution architecture | | SC Consultants | 4 | 0 |
| Identify security controls protecting the environment | | SC Consultants | 4 | 0 |
| Assess each server in the environment for vulnerabilities | | SC Consultants | 4 | 0 |
| Assess the configuration of the underlying OS | | SC Consultants | 8 | 0 |
| Assess the configurations of the Email (e.g., Exchange and CAS) servers | | SC Consultants | 6 | 0 |
| Assess Administrator access to mailboxes | | SC Consultants | 6 | 0 |

▼ PROJECT STATUS MEETINGS ◆ WORK PRODUCT REVIEWS

## TimeFrame for Deliverables (continued)

| **ECWA Cybersecurity Risk & Vulnerability Assessment** | Week 4<br>▼ | Resource | SC Personnel Estimated Hours | Authority Personnel Estimated Hours |
|---|---|---|---|---|
| File Server Security Assessment | | SC Consultants | ▨ | ▨ |
| Assess the configuration of the underlying OS | | SC Consultants | 8 | 0 |
| Gain understanding of directory structure | | SC Consultants | 4 | 0 |
| Assess critical directory permissions | | SC Consultants | 12 | 0 |
| Assess critical file permissions | | SC Consultants | 8 | 0 |
| SCADA Network Vulnerability Assessment | | SC Consultants | ▨ | ▨ |
| Evaluate and confirm ICS \| SCADA network is segmented from other networks | | SC Consultants | 1 | 0 |
| Interview ICS \| SCADA administrator | | SC Consultants<br>SCADA Admin | 1 | 1 |
| Obtain ICS \| SCADA network device information | | SC Consultants | 3 | 0 |
| Perform vulnerability scanning at guarded pace or manual vulnerability testing | | SC Consultants | 7 | 0 |
| Analyze results to remove false positives | | SC Consultants | 3 | 0 |
| Review results of scan with SCADA Admin | ◆4 | SC Consultants<br>SCADA Admin | 1 | 1 |
| Operating System Configuration Assessment | | SC Consultants | ▨ | ▨ |
| Assess Authority's build and configuration standards | | SC Consultants | 1 | 0 |
| Interview DBA | | SC Consultants<br>Authority DBA | 1 | 1 |
| Perform vulnerability scan of the OS | | SC Consultants | 1 | 0 |
| Perform configuration scan and analysis of OS | | SC Consultants | 4 | 0 |
| Analyze results of scanning | | SC Consultants | 4 | 0 |
| Review results with DBA | ◆5 | SC Consultants<br>Authority DBA | 1 | 1 |

▼ PROJECT STATUS MEETINGS ◆ WORK PRODUCT REVIEWS

## TimeFrame for Deliverables (continued)

| **ECWA Cybersecurity Risk & Vulnerability Assessment** | Week 4<br>▼ | Week 5<br>▼ | Resource | SC Personnel Estimated Hours | Authority Personnel Estimated Hours |
|---|---|---|---|---|---|
| Firewall Configuration Assessment | ■ | | SC Consultants | ▨ | ▨ |
| Interview firewall administrator (FA) | ■ | | SC Consultants<br>Authority FA | 2 | 1 |
| Analyze firewall configuration | ■ | | SC Consultants | 22 | 0 |
| Assess results of configuration analysis | ■ | | SC Consultants | 8 | 0 |
| Router \| Switch Configuration Assessment | | ■ | SC Consultants | ▨ | ▨ |
| Interview device administrator (DA) | | ■ | SC Consultants<br>Authority DA | 1 | 1 |
| Obtain device model and firmware version | | ■ | SC Consultants | 1 | 0 |
| Analyze device configuration file | | ■ | SC Consultants | 16 | 0 |
| Assess results of analysis | | ■ | SC Consultants | 6 | 0 |
| VPN Security Assessment | | ■ | SC Consultants | ▨ | ▨ |
| Interview VPN administrator, review logs, assess IT governance | | ■ | SC Consultants<br>VPN Admin | 2 | 1 |
| Perform technical scan of VPN appliance | | ■ | SC Consultants | 3 | 0 |
| Assess configuration of VPN | | ■ | SC Consultants | 3 | 0 |
| Perform ITGC assessment of remote access | | ■ | SC Consultants | 5 | 0 |
| Analyze results | | ■ | SC Consultants | 3 | 0 |
| Review with VPN administrator | | ■ ◆6 | SC Consultants<br>VPN Admin | 2 | 0 |

▼ PROJECT STATUS MEETINGS ◆ WORK PRODUCT REVIEWS

## TimeFrame for Deliverables (continued)

| **ECWA Cybersecurity Risk & Vulnerability Assessment** | Week 5 | Week 6<br>▼ | Resource | SC Personnel Estimated Hours | Authority Personnel Estimated Hours |
|---|---|---|---|---|---|
| Value Adds | ■ | | SC Consultants | | |
| Knowledge Transfer | ■ | | SC Consultants<br>Authority Staff | 16 | 16 |
| SCADA Network Hop \| Segmentation Testing | ■ | | SC Consultants | 16 | 0 |
| Vulnerability Scanner Selection Support | ■ | | SC Consultants | 12 | 0 |
| Cybersecurity Staffing Analysis \| Benchmark | ■ | | SC Consultants | 24 | 0 |
| Reporting | | ■ | SC Consultants | | |
| Vulnerability Mitigation Management Report | | ■ | SC Consultants | 32 | 0 |
| Roadmap Report | | ■ | SC Consultants | 20 | 0 |
| | | | **Total** | 502 | 30 |

▼ PROJECT STATUS MEETINGS ◆ WORK PRODUCT REVIEWS

# PROJECTED SOLUTIONS AND COSTS

We have provided itemized pricing for the major aspects of this project in the table below.

| Project Scope Item | Line Item Fee |
|---|---|
| Current State Assessment of IT Security | $2,976 |
| Evaluation of Planned Improvements | $992 |
| Review of IT Policies and Procedures | $1,984 |
| APT Testing via IoC Analysis | $3,968 |
| IDS/IPS Configuration Assessment | $1,488 |
| WIFI Vulnerability Assessment and Pen Test | $3,224 |
| External Network VA and Pen | $1,984 |
| Internal Network VA and Pen | $3,968 |
| VoIP Security Assessment | $2,232 |
| Active Directory Assessment | $3,968 |
| Email Security Assessment | $3,968 |
| File Server Security Assessment | $3,968 |
| SCADA Network Vulnerability Assessment | $1,984 |
| Operating System Configuration Assessment | $1,488 |
| Firewall Configuration Assessment | $3,968 |
| Router/Switch Configuration Assessment | $2,976 |
| VPN Security Assessment | $2,232 |

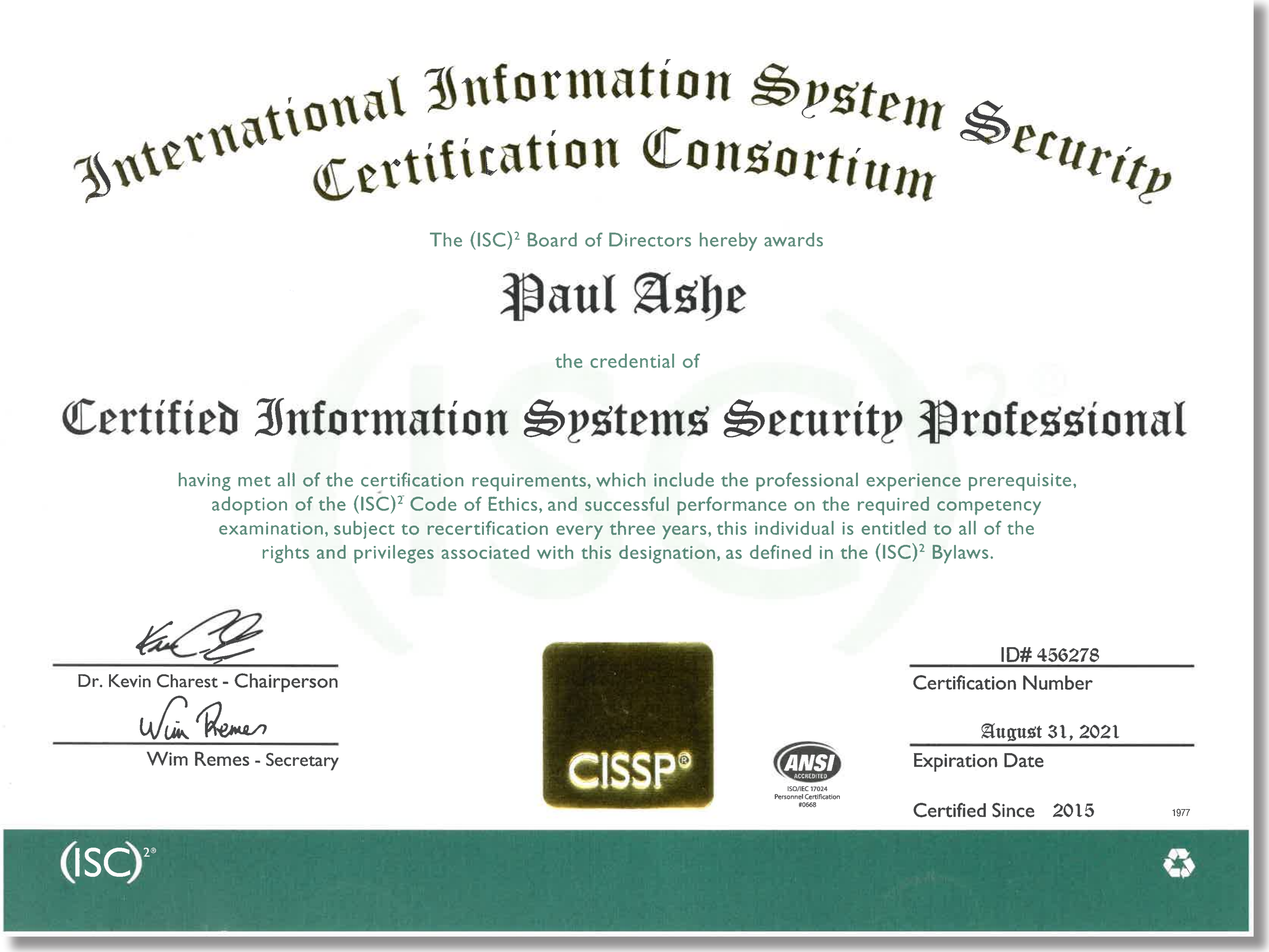
*This section is continued on the following page.*

| Project Scope Item | Line Item Fee |
|---|---|
| Knowledge Transfer — **Value Add** | $1,984 |
| SCADA Network Hop/Segmentation Testing — **Value Add** | $1,984 |
| Vulnerability Scanner Selection Support — **Value Add** | $1,488 |
| Cybersecurity Staffing Analysis/Benchmark — **Value Add** | $2,976 |
| Vulnerability Mitigation Management Report | $3,968 |
| Roadmap Report | $2,480 |
| Travel | Included |
| Independent Project Review* | Included |
| Sub-Total | $62,248 |
| Knowledge Transfer — Value Add | ($1,984) |
| SCADA Network Hop/Segmentation Testing — Value Add | ($1,984) |
| Vulnerability Scanner Selection Support — Value Add | ($1,488) |
| Cybersecurity Staffing Analysis/Benchmark — Value Add | ($2,976) |
| Total | $53,816 |

**Each assessment completed by Securance is reviewed by a consultant independent of the project, in order to ensure that the engagement thoroughly addresses all scope items, all observations are factual and appropriately documented, recommendations are feasible and customized to Client, and all assessment components adhere to the firm's quality control standards.*

# APPENDIX

# RELEVANT CERTIFICATIONS



International Information System Security Certification Consortium

The (ISC)² Board of Directors hereby awards

Paul Ashe

the credential of

Certified Information Systems Security Professional

having met all of the certification requirements, which include the professional experience prerequisite, adoption of the (ISC)² Code of Ethics, and successful performance on the required competency examination, subject to recertification every three years, this individual is entitled to all of the rights and privileges associated with this designation, as defined in the (ISC)² Bylaws.

Dr. Kevin Charest - Chairperson

Wim Remes

Wim Remes - Secretary

CISSP®

ANSI ACCREDITED
ISO/IEC 17024
Personnel Certification
#0668

ID# 456278
Certification Number

August 31, 2021
Expiration Date

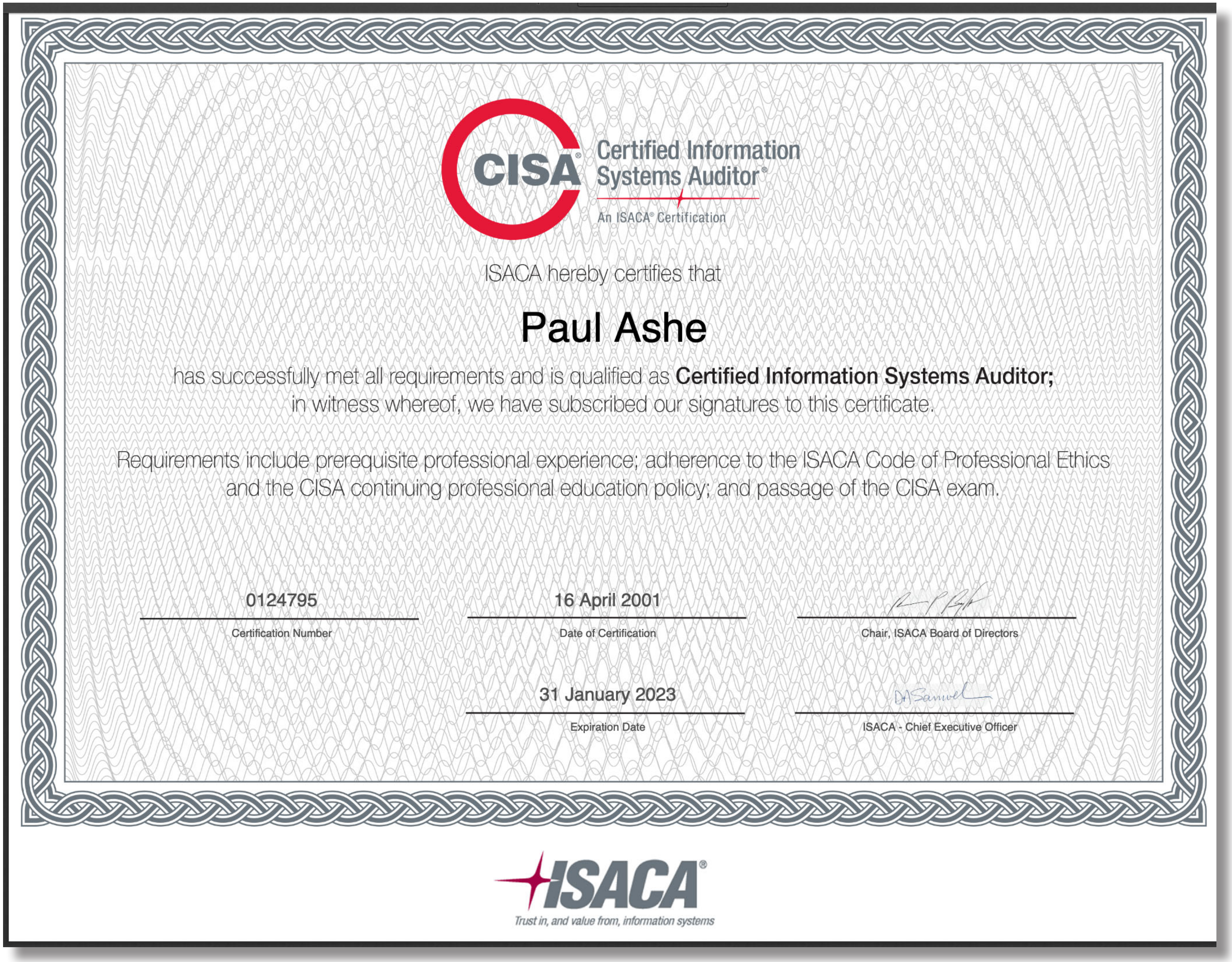
Certified Since 2015

1977

(ISC)²®

# Appendix

## Relevant Certifications — Paul Ashe (continued)



CISA® Certified Information Systems Auditor®

An ISACA® Certification

ISACA hereby certifies that

**Paul Ashe**

has successfully met all requirements and is qualified as **Certified Information Systems Auditor;**
in witness whereof, we have subscribed our signatures to this certificate.

Requirements include prerequisite professional experience; adherence to the ISACA Code of Professional Ethics and the CISA continuing professional education policy; and passage of the CISA exam.

0124795
Certification Number

16 April 2001
Date of Certification

Chair, ISACA Board of Directors

31 January 2023
Expiration Date

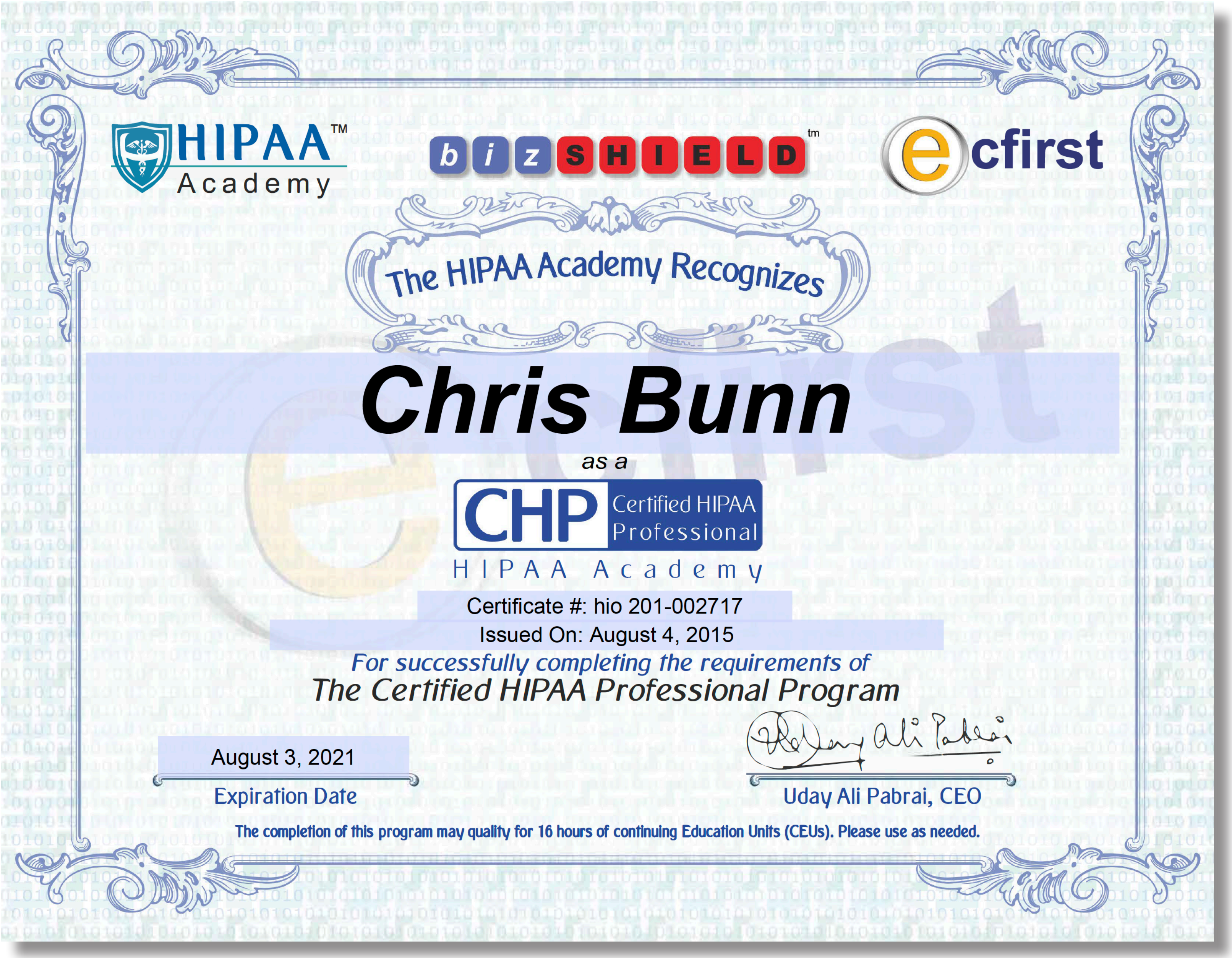
DASamuel
ISACA - Chief Executive Officer

ISACA®

Trust in, and value from, information systems

# Appendix

## Relevant Certifications — Chris Bunn (continued)



HIPAA™ Academy

bizSHIELD™

ecfirst

The HIPAA Academy Recognizes

**Chris Bunn**

as a

CHP Certified HIPAA Professional

HIPAA Academy

Certificate #: hio 201-002717

Issued On: August 4, 2015

*For successfully completing the requirements of*

*The Certified HIPAA Professional Program*

August 3, 2021

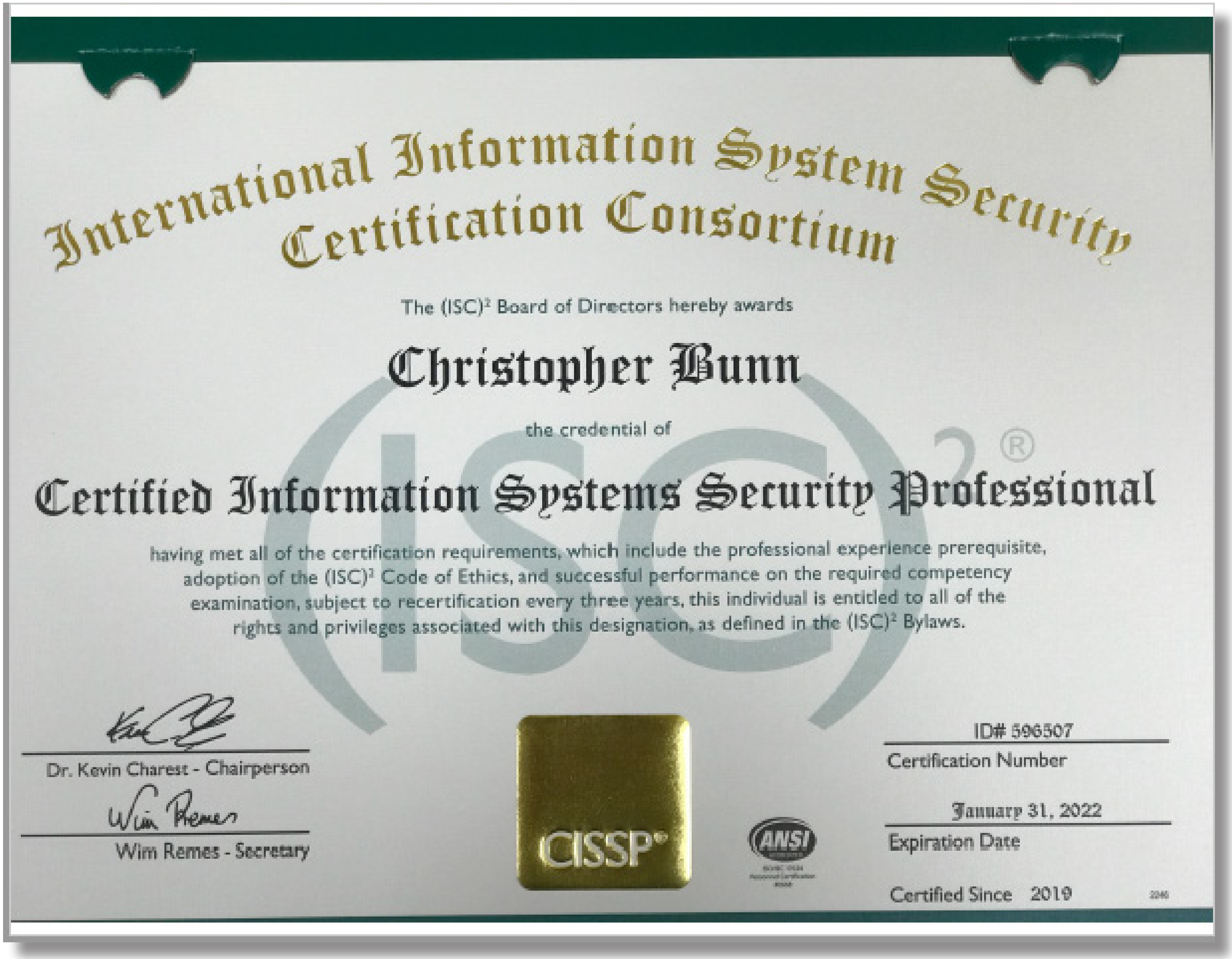
Expiration Date

Uday Ali Pabrai, CEO

The completion of this program may quality for 16 hours of continuing Education Units (CEUs). Please use as needed.

# Appendix

## Relevant Certifications —Chris Bunn



International Information System Security Certification Consortium

The $(ISC)^2$ Board of Directors hereby awards

Christopher Bunn

the credential of

Certified Information Systems Security Professional

having met all of the certification requirements, which include the professional experience prerequisite, adoption of the $(ISC)^2$ Code of Ethics, and successful performance on the required competency examination, subject to recertification every three years, this individual is entitled to all of the rights and privileges associated with this designation, as defined in the $(ISC)^2$ Bylaws.

Dr. Kevin Charest - Chairperson

Wim Remes

Wim Remes - Secretary

CISSP®

ANSI

ID# 596507

Certification Number

January 31, 2022

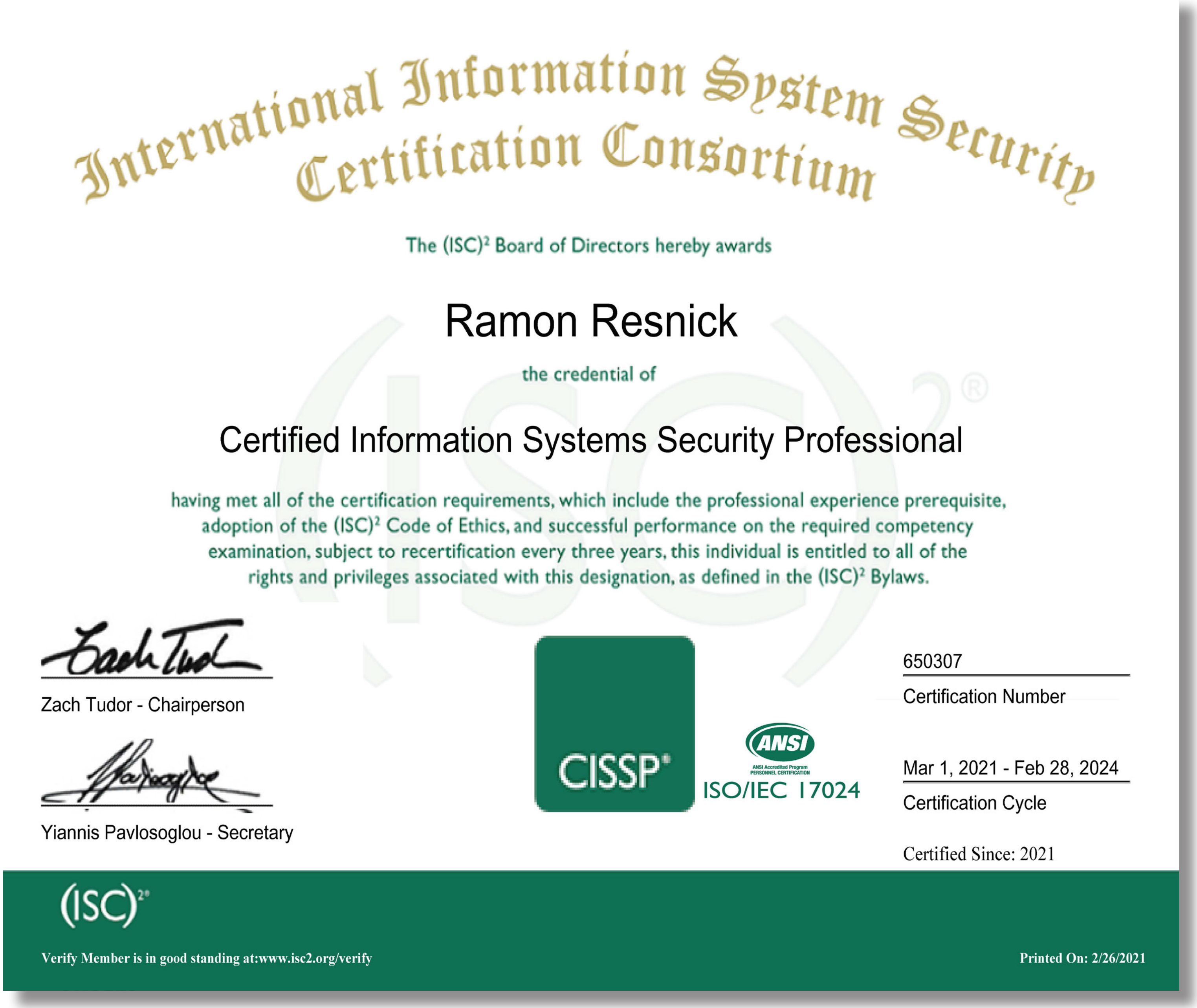
Expiration Date

Certified Since 2019

2246

# Appendix

## Relevant Certifications — Ray Resnick



International Information System Security Certification Consortium

The (ISC)² Board of Directors hereby awards

Ramon Resnick

the credential of

Certified Information Systems Security Professional

having met all of the certification requirements, which include the professional experience prerequisite, adoption of the (ISC)² Code of Ethics, and successful performance on the required competency examination, subject to recertification every three years, this individual is entitled to all of the rights and privileges associated with this designation, as defined in the (ISC)² Bylaws.

Zach Tudor - Chairperson

Yiannis Pavlosoglou - Secretary

CISSP®

ANSI

ANSI Accredited Program PERSONNEL CERTIFICATION

ISO/IEC 17024

650307

Certification Number

Mar 1, 2021 - Feb 28, 2024

Certification Cycle

Certified Since: 2021

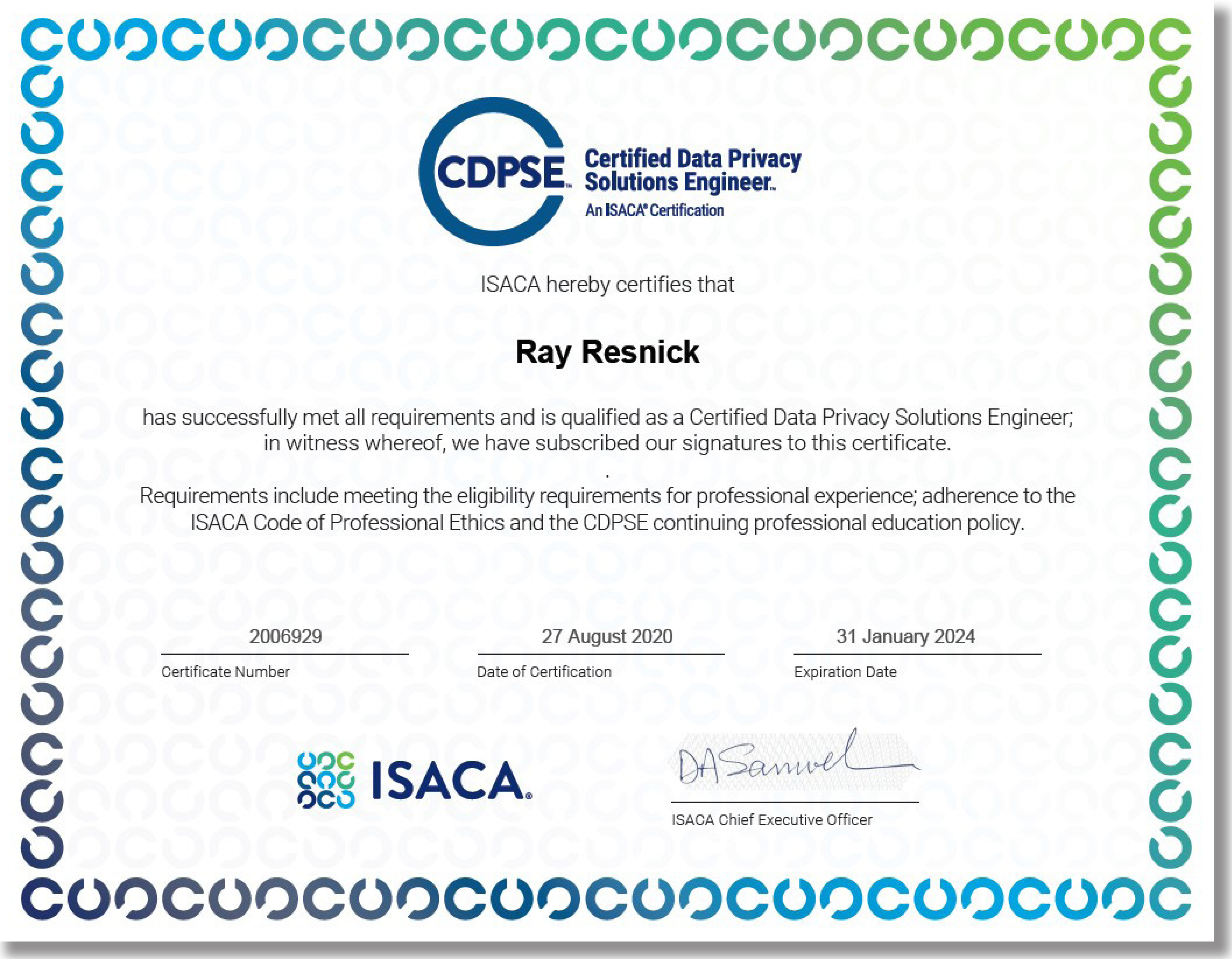
(ISC)²®

Verify Member is in good standing at:www.isc2.org/verify

Printed On: 2/26/2021

# Appendix

## Relevant Certifications — Ray Resnick (continued)



CDPSE™ Certified Data Privacy Solutions Engineer™

An ISACA® Certification

ISACA hereby certifies that

**Ray Resnick**

has successfully met all requirements and is qualified as a Certified Data Privacy Solutions Engineer; in witness whereof, we have subscribed our signatures to this certificate.

.

Requirements include meeting the eligibility requirements for professional experience; adherence to the ISACA Code of Professional Ethics and the CDPSE continuing professional education policy.

| Certificate Number | Date of Certification | Expiration Date |
|---|---|---|
| 2006929 | 27 August 2020 | 31 January 2024 |

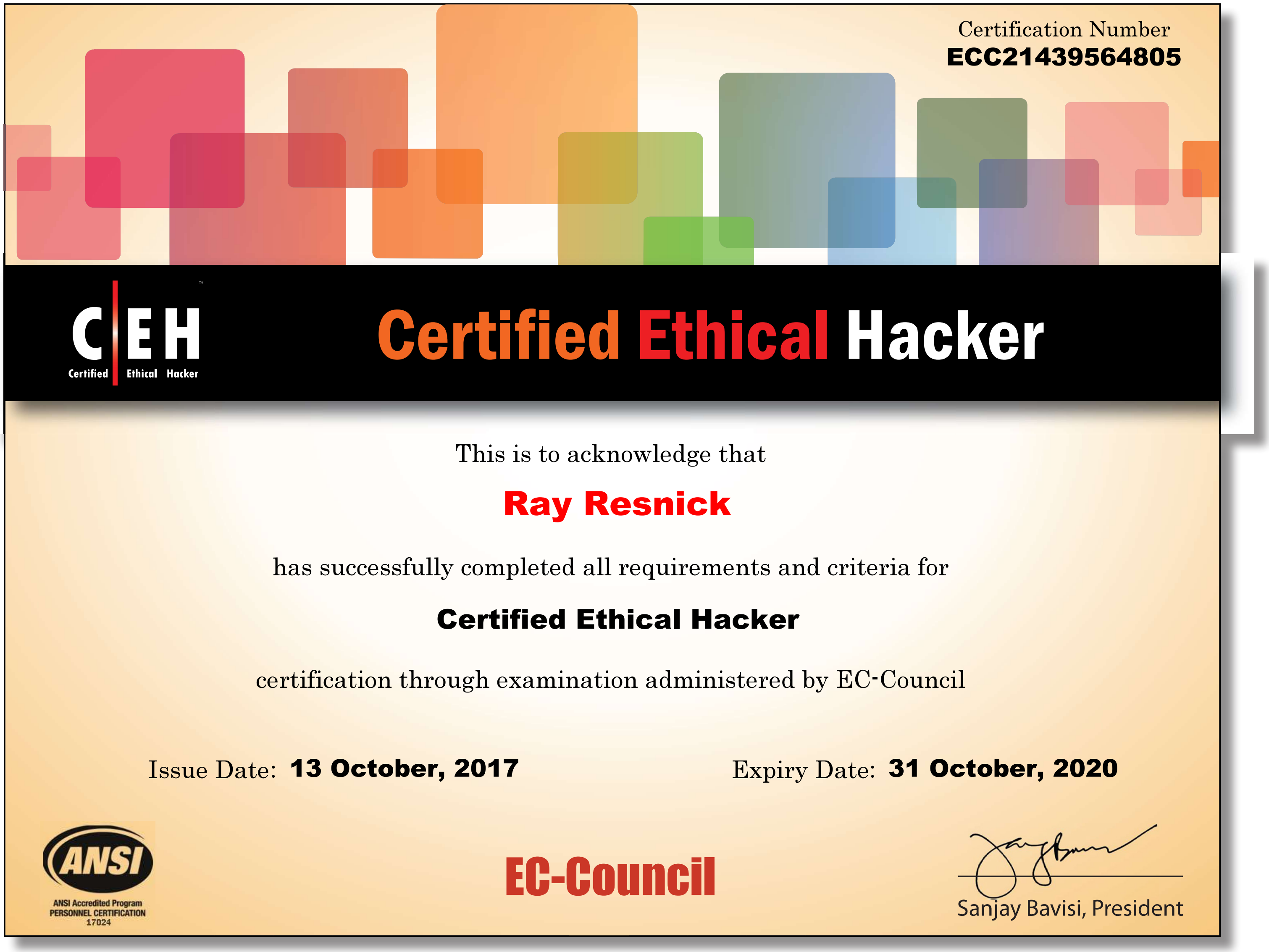
ISACA®

DA Samuel

ISACA Chief Executive Officer

## Appendix

### Relevant Certifications — Ray Resnick (continued)



Certification Number
**ECC21439564805**

C|EH
Certified Ethical Hacker

# Certified Ethical Hacker

This is to acknowledge that

**Ray Resnick**

has successfully completed all requirements and criteria for

**Certified Ethical Hacker**

certification through examination administered by EC-Council

Issue Date: **13 October, 2017**

Expiry Date: **31 October, 2020**

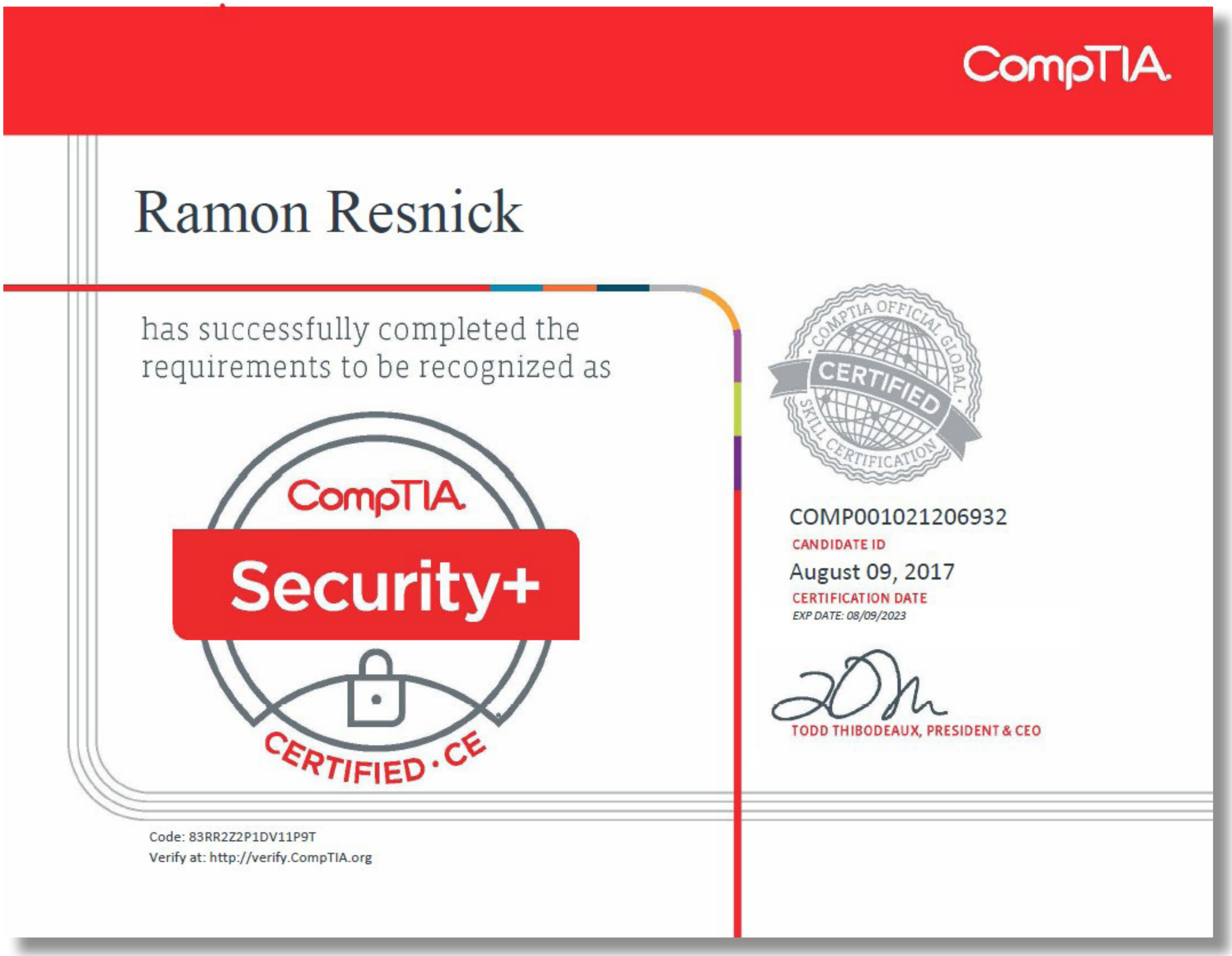
ANSI
ANSI Accredited Program
PERSONNEL CERTIFICATION
17024

EC-Council

Sanjay Bavisi, President

# Appendix

## Relevant Certifications — Ray Resnick (continued)



CompTIA

Ramon Resnick

has successfully completed the requirements to be recognized as

CompTIA Security+ CERTIFIED · CE

COMP001021206932

CANDIDATE ID

August 09, 2017

CERTIFICATION DATE

EXP DATE: 08/09/2023

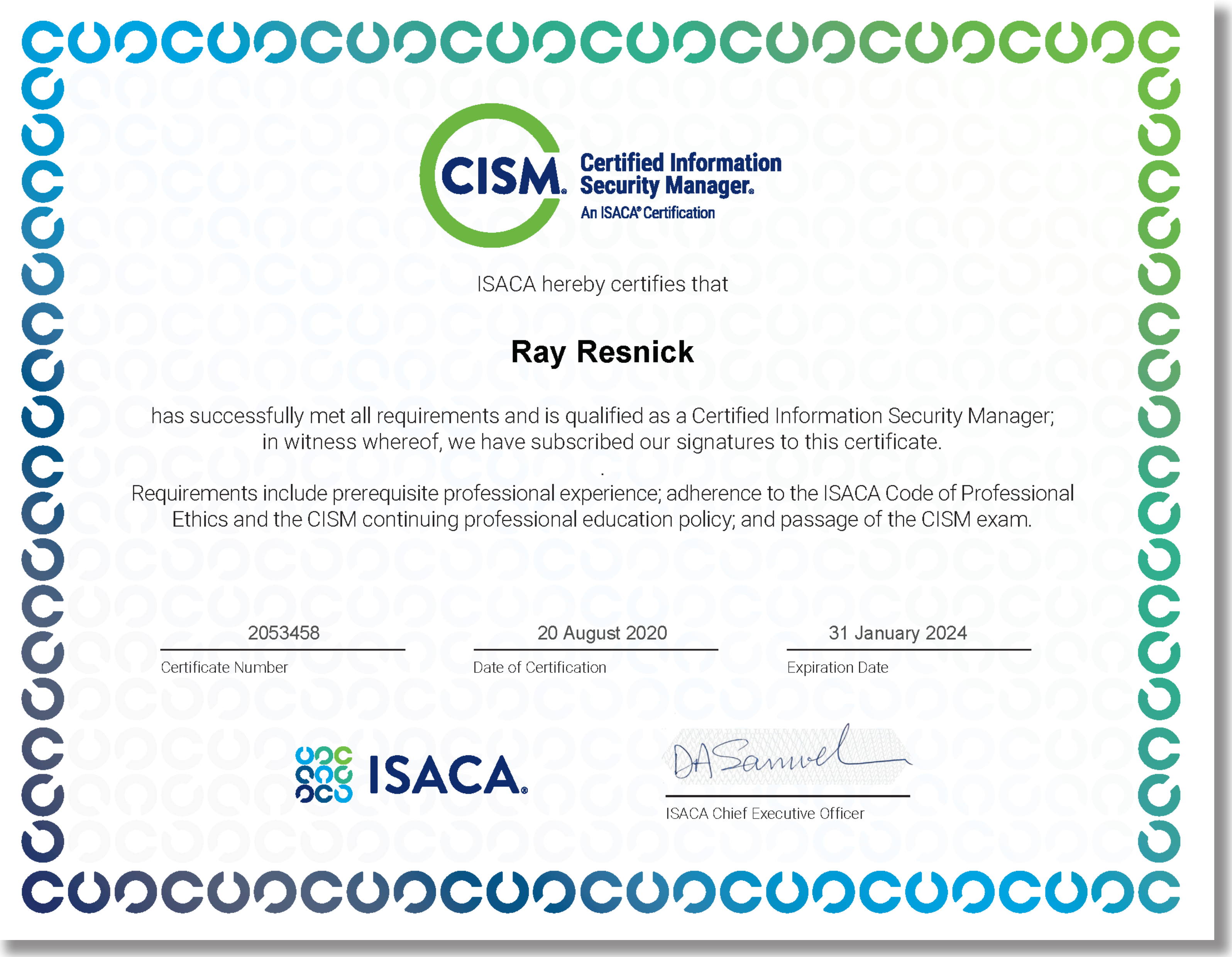
TODD THIBODEAUX, PRESIDENT & CEO

Code: 83RR2Z2P1DV11P9T

Verify at: http://verify.CompTIA.org

# Appendix

## Relevant Certifications — Ray Resnick (continued)



CISM. Certified Information Security Manager.

An ISACA® Certification

ISACA hereby certifies that

**Ray Resnick**

has successfully met all requirements and is qualified as a Certified Information Security Manager; in witness whereof, we have subscribed our signatures to this certificate.

.

Requirements include prerequisite professional experience; adherence to the ISACA Code of Professional Ethics and the CISM continuing professional education policy; and passage of the CISM exam.

| | | |
|---|---|---|
| 2053458 | 20 August 2020 | 31 January 2024 |
| Certificate Number | Date of Certification | Expiration Date |

ISACA.

DA Samuel

ISACA Chief Executive Officer

S|C SECURANCE CONSULTING

*the advantage of insight*

13904 Monroes Business Park • Tampa, FL 33635
**www.securanceconsulting.com**

Softchoice request for proposal response

# Erie County Water Authority

## Cybersecurity Risk & Vulnerability Assessment RFP No. 202100116

June 11, 2021 at 4:00 PM

Pam Jheetey
Account Executive

314 West Superior Street, Suite 400
Chicago, IL 60654

Telephone: (416) 583-8084
Email: pam.jheetey@softchoice.com

# Table of contents

TABLE OF CONTENTS 2

COVER LETTER 4

EXECUTIVE SUMMARY 5

PART 1 6

ITEM 1 - NAME OF INDIVIDUAL OR ORGANIZATION 6

ITEM 2 - NAME AND TITLE OF CONTACT PERSON 6

ITEM 3 - BUSINESS ADDRESS 6

ITEM 4 - TELEPHONE NO. 6

ITEM 5 - EMAIL ADDRESS 6

ITEM 6 - FAX NO. 6

PART 2 6

ITEM 1 - CONSULTANT BUSINESS FORM 6

ITEM 2 - CONSULTANT TEAM 8

PART 3 11

ITEM 1 - PROPOSED SCOPE OF SERVICE 11

ITEM 2 - HARDWARE AND SOFTWARE REQUIREMENTS 15

ITEM 3 - TIMEFRAME FOR DELIVERABLES 16

ITEM 4 - PRICE STRUCTURE 16

ADDITIONAL INFORMATION 18

CYBERSECURITY MATURITY ASSESSMENT 18

INFORMATION SECURITY POLICIES 18

RISK ASSESSMENT 18

1. EVALUATE RISK MANAGEMENT FRAMEWORK 18

2. PERFORM THE RISK ASSESSMENT 19

3. IDENTIFY & ASSESS RISK TREATMENT OPTIONS 19

4. EVALUATE RESIDUAL RISK 20

PENETRATION & VULNERABILITY TESTING 20

GENERAL TERMS AND CONDITIONS ........ 21

ATTACHMENTS ........ 22

CERTIFICATE OF INSURANCE ........ 22

SOFTCHOICE MASTER SERVICES AGREEMENT ........ 23

# Cover Letter

June 11, 2021

Erie County Water Authority,
295 Main Street, Room 350
Buffalo, New York 14203

**Attn:** Terrence D. McCracken, Secretary to the Authority

**RE:** Proposal for Risk & Vulnerability Assessment

Softchoice would like to thank you for the opportunity to respond to the Erie County Water Authority Request for Proposals for Cybersecurity Risk & Vulnerability Assessment.

As an officer of the company, I am authorized to sign and contractually bind Softchoice to the pricing provided in our response. During this evaluation period, I would encourage you to contact your Account Executive below with any questions you may have regarding the Softchoice Response.

Pam Jheetey
Telephone: (416) 583-8084
Email: pam.jheetey@softchoice.com

Softchoice has carefully reviewed this Request for Proposal and has prepared this response to outline our approach to meet the objectives and address them within the project scope.

As always, your time and willingness to consider Softchoice are very much appreciated.

Sincerely,

By:

Jordanna Silver
Manager, Sales Operations – Bid Response
Telephone: 416-588-9002
legal@softchoice.com

# Executive Summary

The Erie County Water Authority (“the Authority”) operates a federally designated critical infrastructure system and desires to conduct a cybersecurity risk and vulnerability assessment of physical and virtual assets and infrastructure. In order to secure information and assets for the Authority, it is imperative to develop a strategy that encompasses all security requirements for the organization that adheres to standards developed by the National Institute for Standards and Technology (NIST) for federally designated critical infrastructures.

Cybersecurity failure poses a major threat to the world, 2020 was rife with vulnerable targets. In 2020, SonicWall Capture Labs Threat Researchers recorded 5.6 billion malware attacks, of which 2.8 billion malware hits were in the US. When it comes to top 10 US States in terms of 2020 malware volume, NY comes at number 2. When it comes to 2020 ransomware volume, United States had more than 203 Million ransomware hits & NY comes in top 10 in ransomware hit volume. Last but not the least, industry specific data shows government entities were the most vulnerable in 2020 with 1,275 attempted malware attacks each on an average of 17 per hour. It is certain that cybercrimes storm will continue to rage into 2021, it’s already apparent that the confluence of factors at work over the past year has pushed cybercrime to a new level, requiring increased security and vigilance as we move ahead. Hence, all the above aspects must have been a driving factor for the Authority behind issuing the RFP for Risk and Vulnerability Assessment.

The Authority is seeking the support of a professional firm to assist in evaluating existing IT Cybersecurity Risks and Vulnerabilities and designing an adequate remediation plan to mitigate risks to an acceptable level while ensuring compliance with NIST standards and the NIST Cybersecurity Framework (CSF) that include:

1. Identify assets and assigning asset values for the Authority.
2. Identify and assess the IT Cybersecurity risks for ECWA and align the Cybersecurity program to the NIST Cybersecurity Framework (CSF) and standards for federally designated critical infrastructure.
3. Perform a control maturity assessment against industry best practices.

While the Authority provides to its customers the water they can trust, Softchoice, in partnership with security expert KMicro, would provide the Authority the security strategy they can trust. KMicro has expertise in comprehensive security services including Data Protection, Cloud Security, Managed Security Services (SOC Operations, Threat Detection, Incident Response) & Professional Services. Softchoice and KMicro have together worked on similar projects before. With our expertise we will together weed out the vulnerabilities in your IT Environment and propose a solution that fits the Authority the best.

Our proposal aims to provide the Authority with an evaluation that will focus on the Cyber Security Framework developed by the National Institute of Standards and Technology (NIST) *(see Additional Information section)*. We have prepared a well-suited response addressing all the elements of the RFP.

At Softchoice, we are not only work focused but also aware of our community responsibilities. We have various employee groups Softchoice cares, Shades of Orange, leading women committee are working together to raise community awareness related to prevalent disparities around us. Our Sustainable Softchoice Initiative is bent on raising awareness related to environmental issues.

We are passionate about uncovering obstacles, solving problems, and creating success for our customers. Our technology solutions help you win today and be prepared for tomorrow. We have been working with State, local, and federal organizations by not merely providing them the solution they ask for but customizing it to their needs, be it hardware, software, cloud and datacenter, collaboration and digital workplace, network, or security. We are the trusted advisor for all our partners.

We appreciate your time and willingness to consider Softchoice as your partner in success.

# PART 1

## Item 1 - Name of Individual or Organization

Response: Softchoice Corporation

## Item 2 - Name and Title of Contact Person

Response: Pam Jheetey, Account Executive

## Item 3 - Business Address

Response: 314 West Superior Street, Suite 400, Chicago IL 60654

## Item 4 - Telephone No.

Response: (416) 583-8084

## Item 5 - Email Address

Response: pam.jheetey@softchoice.com

## Item 6 - Fax No.

Response: N/A

# PART 2

## Item 1 - Consultant Business Form

1. *Identify the Consultant's business or corporate structure:*

(a) *If a Corporation, including the following:*

- *Date and State of Incorporation*
  Response: Softchoice Corporation

- *List Name and Title of Executive Officers*
  Response:
  - Vince De Palma, President & CEO
  - Andrew Caprara, Chief Operating Officer
  - Bryan Rocco, Chief Financial Officer
  - Jeff Reis, Senior Vice President, Information Technology
  - Karen Scott, Senior Vice President, People & Growth
  - Kevin Hendrick, Senior Vice President, Sales

    - Maria Odoardi, Senior Vice President, Business Transformation
    - Sean Denomey, Senior Vice President, Services

- *Principal Place of Business*
  Response: Headquarters in Chicago, IL with local offices across North America.

- *List all Related Principal or Subsidiaries Corporations*
  Response: Softchoice LP (Canadian business)

- *Closed or Publicly Traded*
  Response: Publicly traded

- *EIN*
  Response: 13-3827773

2. *Identity the number of years your entity has been in business.*

Response: Softchoice Corporation has been in business for 16 years, since 1995.

3. *Identity whether your business/corporate structure has changed in the past five years and if yes, describe the change.*

Response: From 2013 to 2021, Softchoice was a private company fully owned by Birch Hill Equity Partners. Since June 2021, Softchoice is a publicly traded company.

4. *Identity the type and coverage amount of all insurance policies.*

Response: Please refer to the Certificate of Insurance in the Attachments section of this document.

5. *Identified the name, address, and contract information for three (3) companies that the Consultant has performed similar services to those being sought by the Authority.*

Response: Softchoice, in partnership with KMicro, has worked successfully with the entities listed below:

- New Belgium Brewing Company
- H.W Lochner
- Distinguished Vineyards & Winery Partners
- College Health Services
- Indiana Farmers Mutual Insurance
- Oneonta Starr Orchards
- Carriage Services

Out of respect for our clients' hectic schedules, Softchoice prefers to take an active role in facilitating reference discussions between existing and prospective clients. At the appropriate point in your procurement process please advise Softchoice that you would like to start checking references and we will gladly facilitate calls or meetings with the relevant reference site(s) and contact(s).

**Reference #1**

| | |
|---|---|
| **Name** | New Belgium Brewing Company |
| **Address** | 500 Linden St, Fort Collins, Colorado 80524 |
| **Contact information** | Jake Jakel, IT Operations Manager<br>Jjakel@newbelgium.com |

**Reference #2**

| | |
|---|---|
| **Name** | Carriage Services |
| **Address** | 3040 Post Oak Blvd Ste 300, HOUSTON, Texas 77056 |
| **Contact information** | Chris Strom, Infrastructure Manager<br>chris.strom@carriageservices.com<br>832-314-8909 |

**Reference #3**

| | |
|---|---|
| **Name** | Oneonta Trading Company |
| **Address** | P.O. BOX 549, Wenatchee, Washington 98807 |
| **Contact information** | Ian Kirkpatrick, IT Manager<br>iank@oneonta.com<br>(509) 888-4410 |

6. *If you are a certified, minority and/or women owned business, submit a copy of the certification.*

Response: Not applicable.

## Item 2 - Consultant Team

*Identify the individuals whose professional services will be utilized to undertake a comprehensive IT Cybersecurity Risk and Vulnerability Assessment, including thoroughly reviewing the current state of the Authority's information technology security, developing a vulnerability mitigation plan, and developing a prioritized road map of activities to enhance the Authority's future Cybersecurity position. Please provide the following information for each identified individual:*

*(a) Relevant qualifications and experience, including educational degrees and any applicable licenses or certifications (e.g., CISSP, CISM, CGEIT, CRISC), and*
*(b) State and county of residence, and*
*(c) Scope of responsibility, and*
*(d) Length of time working for Consultant.*

Response:

| | |
|---|---|
| **Name** | John Haifa |
| **Designation** | Cybersecurity Practice Lead - KMicro |
| **Residence** | Waterloo, Ontario - Canada |

| | |
|---|---|
| **Qualifications** | • Master’s Degree - Networking and Systems Administration<br>• Certified Information Security Manager (CISM)<br>• ITIL Service Manager (ITSM)<br>• ITIL Foundation Certificate (ITILF)<br>• CMMC-AB Registered Practitioner (RP)<br>• Sun Certified System Administrator for the Solaris OS (SCSA) (Solaris 9, 10)<br>• Sun Solaris Advanced Networking (SCNA)<br>• Sun Solaris Certified Security Administrator (SCSECA)<br>• Microsoft Certified IT Professional (MCITP)<br>• Microsoft Certified Systems Engineer (MCSE 2000/ 2003)<br>• Microsoft Certified IT Professional (MCITP)<br>• Microsoft Certified Technology Specialist (MCTS)<br>• Microsoft Certified Trainer (MCT)<br>• Certified Novell Administrator (CNA)<br>• Certified Unix System Administrator for UNIX ware 7 (CUSA)<br>• Certified Ethical Hacker (CEH)<br>• Certified Computer Forensics Investigator (CHFI)<br>• Network Security (CEP) eccouncil<br>• Wireless Network Architect (CEP) eccouncil<br>• Linux Security (CEP) eccouncil<br>• e-Business Security (CEP) eccouncil<br>• Security +<br>• Network + |
| **Experience/Role** | John has over 15 years of experience in Cybersecurity, Information Service Management, and Security Governance and will be the lead Consultant for the project. Being certified as a Cybersecurity Professional, System Administration, as well as IT Service Management, he has a deep understanding of standards-based controls.<br>John has worked with a number of organizations across multiple industry verticals to ensure process, people and technologies meet cybersecurity best practices. As a trusted practitioner, he has helped the Authority define and deliver cybersecurity strategies, architectures, and projects. Applying a focused based approach, John manages fully customizable managed security solutions, including assessments, advanced security event monitoring solutions, threat analytics, risk management, and incident response. Engagements include development of cybersecurity programs, policies, review of external guidelines, regulatory expectations to determine suitability of controls in the areas of information security governance, secure design, and cybersecurity. |

| | |
|---|---|
| **Name** | Victor Westbrook |
| **Designation** | Senior Cybersecurity Analyst (Penetration & Vulnerability Testing) |
| **Residence** | San Antonio, Texas |
| **Qualifications** | Clearance:<br>• Adjudicated Top Secret<br>Certifications:<br>• Certified Information System Security Professional (CISSP)<br>• Certified DarkWeb Investigator (CDWI)<br>• Certified Ethical Hacker (C\|EH)<br>• Red Team Security Certified Red Team Operator (CRTO)<br>• Offensive-Security Certified Expert (OSCE)<br>• Offensive-Security Certified Professional (OSCP)<br>• Offensive-Security Wireless Professional (OSWP)<br>• GIAC Certified Exploit Researcher and Advanced Penetration Tester (GXPN) |

| | |
|---|---|
| | • GIAC Certified Penetration Testing (GPEN)<br>• GIAC Certified Web Application Penetration Tester (GWAPT)<br>• GIAC Mobile Device Security Analyst (GMOB)<br>• GIAC Certified Incident Handler (GCIH)<br>• GIAC Certified Forensics Analyst (GCFA)<br>• GIAC Certified Auditing Wireless Networks (GAWN)<br>• GIAC Certified Security Essentials (GSEC)<br>• GIAC Certified Intrusion Analyst (GCIA)<br>• eLearnSecurity Junior Penetration Tester (eJPT)<br>• eLearnSecurity Web Application Penetration Tester (eWPT)<br>• eLearnSecurity Certified Professional Penetration Tester (eCPPT Gold)<br>• eLearnSecurity Certified Professional Penetration Tester v2 (eCPPTv2)<br>• Rapid7 Application Assault Certified Professional (AACP)<br>• Rapid7 Network Assault Certified Professional (NACP)<br>• National Security Agency InfoSec Assessment Methodology (NSA-IAM)<br>• National Security Agency InfoSec Evaluation Methodology (NSA-IEM)<br>• Comptia Network+<br>• Comptia Security+<br>• Comptia Linux+<br>• Comptia Project+<br>• Linux Professional Institute Certified (LPI-1)<br>• SUSE Certified Linux Administrator (SCLA) |
| **Experience/Role** | Victor has over 10 years of experience in Penetration and Vulnerability Testing.<br>Victor will be performing the technical penetration testing and vulnerability scanning activities as part of this proposal |

# PART 3

## Item 1 - Proposed Scope of Service

*Working in consultation with the Authority's IT staff, the Consultant will be required to develop comprehensive IT Cybersecurity Risk and Vulnerability Assessment.*

*Describe the scope of service, which the Consultant would recommend to the Authority, to undertake a comprehensive IT Cybersecurity Risk and Vulnerability Assessment. The scope should include the following elements, along with such elements will be performed on-site or off-site:*

*(a) Review of current state of the Authority's information technology security,*

Response:

**1. Review Existing Information Security Documentation**

Softchoice will review existing security Policies, Standards, Guidelines, Risk Reports, Incident Report, Audit Reports, and other relevant documentation in place with the Authority to evaluate their effectiveness. Softchoice will scrutinize and collect evidence & details relevant to the documentation under examination. This detailed review will provide a clear overview of the present state of Cybersecurity activities focusing on its adequacy against Information Security Management Policy best practices in line with the NIST CSF and standards.

**2. Current State Assessment**

Assessment of the level of compliance of the Authority against information assurance maturity levels based on the controls defined by the NIST Cybersecurity Framework and standards developed by NIST for federally designated critical infrastructures. A "Current Profile" will be created in line with the NIST Framework for Improving Critical Infrastructure Cybersecurity by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved towards supporting subsequent steps by providing baseline information.

The objective of this assessment is to identify any Cybersecurity Risks, deficiencies and/or deviations in the Authority's current security processes or activities.

The Current State Assessment is a critical in assuring that all subsequent activities are properly defined to determine the required actions towards further development of the Cybersecurity Management Program that is effective and efficient in their operation.

The Assessment Plan includes the following:

- Establish needed artifacts.
- Define assessment team roles and responsibilities.
- Identify the Authority participants and roles.
- Scheduling of interviews with the Authority participants.
- Schedule testing, tours, and other on-site/virtual requirements.
- Highlight any assessment constraints and schedule dependencies.
- **Assess Current Conditions** – Softchoice will perform a thorough evaluation of the current state of controls and gain an understanding of the current cybersecurity state of the Authority against standards developed by NIST for federally designated critical infrastructures.
- **Analyze Gaps** – NIST Standards and Cybersecurity best practices will be compared to the Authority's current controls and changes will be identified to build a relevant, actionable, and sustainable cybersecurity program that demonstrates Cybersecurity Maturity against the NIST CSF.

The assessments will be dynamic documents that are maintained by the Authority in order to monitor the level of compliance against NIST controls and Cybersecurity Frameworks.

*(b) Development of a vulnerability mitigation plan,*

Response:

For every risk recorded in the 'Risk Register' as part of the technical vulnerability scans or the Risk Assessment, Softchoice will identify Risk Treatment Options that mitigate the risks and satisfy the relevant control activity. The potential controls will be aligned with the level of maturity intended by the Authority as well as standards developed by the National Institute for Standards and Technology (NIST) for federally designated critical infrastructures. Softchoice will assess the risk treatment options/potential controls and will consider several aspects of the potential countermeasure such as:

- Accountability (can be held responsible)
- Ease of use/Required effort
- Auditability (can it be tested?)
- Minimum manual intervention
- Trusted source (source is known)
- Secure
- Consistently applied
- Protects Confidentiality, Integrity, and Availability of the Authority services
- Cost-effective (implementation and maintenance cost)
- Reliable
- Creates no additional issues during operation

Residual Risk is the risk remaining when appropriate controls are properly applied to lessen or remove the vulnerability. Softchoice will estimate and evaluate the residual risk based on the defined Risk Treatment Plan and document it in a formal register to enable future monitoring and management review of residual risks.

As part of the project, Softchoice will research, recommend, and present additional technologies to improve security capabilities where deemed necessary. This will be presented in a compare/contrast model with the recommended technologies and/or evaluation/upgrade of existing technologies.

*(c) Development of a prioritized road map of activities to enhance the Authority's future Cybersecurity position,*

Response:

An important and useful component is a Plan of Action and Milestones (POA&M or POAM) that will be developed for the Authority as part of this project proposal. To achieve compliance with NIST Standards, a POA&M is an extremely useful tool in helping the Authority to plan for a multitude of security projects, including compliance with standards developed by NIST for federally designated critical infrastructures.

The POA&M will:

- Provide the Authority with a structured approach for how to approach findings during the assessment
- Outline activities necessary to mitigate security issues.
- Helps identify the security issue and the underlying gap in the Authority systems or processes.
- Assigns resources needed to mitigate issues.
- Holds the Authority organization accountable with projected completion of milestone activities.
- Calls out how vulnerabilities were identified during the assessment.
- Denotes risk level, labels status, and captures the estimated cost to remediate.

(d) *Best practice methodologies to ensure a standardized risk mitigation approach that will offer the highest risk reduction potential, complementing the "Framework for Improving Critical Infrastructure Cybersecurity", developed by the National Institute for Standards and Technology (NIST),*

Response:

The Risk Assessment process will determine a risk scoring that will give a clearer picture of the risks that require more attention. Risk is determined by combining the likelihood and security categorization impact of threats for a specific vulnerability. This will then be used to prioritize risks and the Authority's approach to risk mitigation with be defined within a formal Risk Treatment Plan.

(e) *Assessment that includes but not limited to:*

- *Test for susceptibility to Advanced Persistent Threats (APTs) such as viruses, malware, Trojan horses, botnets, and other targeted attack exploits.*
- *Evaluate the Authority's current threat posture including antivirus and Intrusion Detection and Prevention (IDP) capabilities.*
- *Evaluate the Authorities planned changes and improvements to the threat surface and assist identifying and addressing security concerns.*
- *Review the Authority's current Supervisory Control and Data Acquisition (SCADA) water systems for security vulnerabilities.*
- *Review wireless network system components for security vulnerabilities, validating system-specific operating systems and firmware versions for known exploits and recommend upgrades, updates, and mitigations.*
- *Review current system-specific operating systems and firmware versions for known exploits and recommend upgrades, updates, and mitigations. This includes firewalls, switches and routers, Microsoft Active Directory, email and file servers, web servers, wireless routers, WAN, VPN, VoIP, and CCTV systems.*
- *Assess VoIP network system components for security vulnerabilities, validating system-specific operating system and firmware versions and reviewing for known exploits.*
- *Review existing IT policies and procedures and make recommendations for changes and/or additional policy and procedure development.*
- *Execute and review internal network vulnerability scans and external vulnerability and penetration scans and make recommendations to reduce the threat attack surface.*
- *Recommend or assist in selection of vulnerability scan software for purchase/license for continued use by the Authority after the assessment is complete*

Response:

All the above assessments will be completed as part of this proposal. This will include vulnerability scanning of internal systems and penetration testing of external systems as follows:

| Particulars | Internal (Vulnerability Scans only) | External |
|---|---|---|
| **Desktops/Laptops** | 350 nodes (up to 2000 internal IP addresses) | 0 |
| **Servers** | 100 Nodes | 4 Nodes |
| **Email Servers** | 2 | 0 |
| **Routers/Switchers** | 175 routers & switches | 0 |
| **Firewalls** | 4 | 0 |
| **IDS/IPS** | 1 system | 0 |
| **Subnets** | - | (2) 26-bit subnets |
| **Web applications** | - | 4 |
| **Static Web pages** | - | Less than 100 |

| | | |
|---|---|---|
| **Unique Dynamic pages** | - | Less than 100 |
| **Unique Input fields** | - | Approx. 100 |
| **API Testing** | - | Yes |
| **Mobile App Testing** | - | Android |

## External Network Penetration Test

Softchoice will follow an in-house developed methodology based on the Penetration Testing Execution Standard (PTES). At a high-level, our methodology is executed over the following phases:

- Opensource Intelligence Information Gathering (OSINT)
- Discovery and Enumeration
- Vulnerability Scanning and Analysis
- Vulnerability Exploitation
- Post Exploitation Activities
- Report Development
- Post Engagement Consulting

### Phase 1: Opensource Intelligence Information Gathering (OSINT)

Phase 1 begins with gathering information via Opensource Intelligence via online information resources. These resources consist of multiple search engines, online metadata gathering utilities, domain registrants, whois registrations and more. This phase is designed for discovery, and to discern the presence of vulnerabilities and potential areas of exploitation, all while remaining 100% stealthy.

### Phase 2: Discovery and Enumeration

Phase 2 involves sending packets to the target network to discover live systems and any open ports, and services that are exposed to the External network. This gives the tester a view of possible applications and high-level vulnerabilities and exposures that may affect those hosts. This phase also involves the enumeration of banners, the application version strings of each exposed service, that may lead to clues on vulnerabilities affecting the host.

### Phase 3: Vulnerability Scanning and Analysis

Phase 3 involves the automated and manual testing of the target hosts and services that were found during phase 2. This phase involves multiple open source and commercial tools to automatically analyze the presence of known vulnerabilities within the information system and the exposed service(s). Manual analysis is conducted on the target host that helps to flush out any false positives that are discovered during the automated scanning efforts. Manual analysis is also conducted to find vulnerabilities that may have been missed by automation or issues that can only be discerned through human intelligence.

### Phase 4: Vulnerability Exploitation

Phase 4 involves the exploitation of the discovered vulnerabilities in phase 3. During this phase denial of service conditions and vulnerabilities are NOT exploited but are documented in phase 6. Careful analysis and exploitation is performed using manual exploitation techniques and very little automation. Vulnerable network services, host-based services and web applications are targeted and exploited during this phase in order to achieve initial access to the target(s).

### Phase 5: Post Exploitation Activities

Phase 5 involves the tactics, techniques and procedures to further gain access into the environment.  This may include activities such as privilege escalation, lateral movements, additional enumeration, scanning and exploitation as outlined in phases 2-4, additionally key objectives may include obtaining domain or enterprise admin privileges and compromising an organization's critical assets.

**Phase 6: Report Development**

Phase 6 is where the engagement deliverables are developed, and additional testing may occur to ensure that proper evidence have been captured in order to prove risks and exposures of the network environment.  Engagement deliverables are commonly in the form of report documents, PowerPoint presentations, and / or letters of attestation or opinion.

**Phase 7: Post Engagement Consulting**

Phase 7 involves the consultant(s) performing a walkthrough of the engagement deliverables and answering any question about the engagement and next steps.  Additionally, feedback from the Authority is noted, and adjustments made to the final deliverable(s).  Agreements in terms of retesting efforts are coordinates during this phase.

### Asset Review and Assessment

Annually, Softchoice will conduct Asset Reviews compiled by gathering reports on the client's environment directly from the vendor. Through our reporting and client briefing, we provide a full overview of their status, the state of the devices in terms of their lifecycle and provide recommendations to simplify contract and or purchasing management and aid future planning.  The information is delivered one-to-one by a subject matter expert. These are Funded by Softchoice.

Licensing Assessments are available, with the price determined by the relative scope and complexity of the requirements of same.

Our Licensing Assessments constitute a software asset management offering that gives you the insight you need to avoid overspending, optimize your software usage, and manage the licensing lifecycle. It combines the insights of an Asset Review with Install and/or Entitlement information to provide a gap analysis

**Capabilities:**

- Visibility into the current state of usage and renewals.
- Expertise needed to navigate licensing agreements.
- A methodology to right size your needs and budgets.
- An audited inventory of your assets, even if they were not purchased from Softchoice.
- Vendor contracts are reviewed to understand your ownership position and entitlements.
- Gap analysis and recommendations are delivered by licensing experts through a workshop.
- Insight into and potential compliance risk.
- Optimization of your current vendor entitlements, eliminating waste or overspending.
- Confidence in your ability to evaluate the impact of new licensing programs and future platform shifts.

## Item 2 - Hardware and Software Requirements

(a) *Describe the required hardware and/or software necessary to implement Consultant's plan, if any.*
(b) *Describe the limitations of the service and/or equipment, if any.*
(c) *Identify whether the required hardware and/or software will be provided by Consultant or the Authority.*

Response: Not applicable, no hardware or software requirements to implement the plan.

## Item 3 - Timeframe for Deliverables

*Provide a timeframe for completing the following deliverables:*

1. *Project Management Deliverables:*
   (a) *Work Breakdown Schedule (WBS) including tasks,*
   (b) *Schedule and dependencies, and*
   (c) *Weekly Status Reports including risks and progress reports.*
2. *Report: A written report documenting:*
   (a) *Executive summary detailing the Authority's Cybersecurity position, including a comparative scorecard of findings,*
   (b) *Results of vulnerability testing performed,*
   (c) *Identified cybersecurity vulnerabilities, gaps, and mitigation plans,*
   (d) *A prioritized road map of activities, developed in conjunction with Authority's IT staff to enhance the Authority's future cybersecurity position.*
3. *Projected solutions and costs:*
   (a) *Provide an estimated range, based upon previous experience, of the total services costs to implement the proposed solutions,*
   (b) *Include a Rate Sheet that specifies and itemizes the cost for each proposed component, including all licensing, support, maintenance, and hosting fees, and*
   (c) *For subscription-based services, provide annual pricing.*

Response:

The entire duration of the project will be (8) weeks. Project Plan will be provided during the first week and project status updates will be sent on a weekly basis. The project will involve scheduling of workshops with the Authority project team members and scheduling of Vulnerability and Penetration Testing.

Deliverables will include:

| Item | Deliverable Description |
|---|---|
| 1 | Information Security Policy, Process, Standards reviews with recommendations |
| 2 | NIST Cyber Security Framework Assessment – Spreadsheet (includes maturity scorecard) |
| 3 | Risk Management Framework - Document |
| 4 | Plan of Action and Milestones - Spreadsheet |
| 5 | Risk Assessment – (Spreadsheet) |
| 6 | Risk Treatment Plan - (Spreadsheet) |
| 7 | Vulnerability Scan Reports – Internal Network |
| 8 | Penetration Test Report – External Systems |

## Item 4 - Price Structure

1. *Provided a detailed description of the Consultant price structure or pricing option for the services to be provided by the Consultant.*
2. *If the Consultant has a standardize agreement used for such services, include a copy with the Proposal.*

Response:

| Task | Qty | Rate | Amount |
|---|---|---|---|
| Cybersecurity Framework/Current State Assessment | 1 | $27,500 | $27,500 |
| Risk Assessment | 1 | $22,625 | $22,6251 |
| Penetration Testing & Vulnerability Scanning | 1 | $26,310 | $26,310 |
| Project Management | 1 | $3,210 | $3,210 |
| **Total*** | | | **$79,645** |

We have included our standard as a separate attachment.

# Additional Information

Our proposal aims to provide the Authority with an evaluation that will focus on the Cyber Security Framework developed by the National Institute of Standards and Technology (NIST).

## Cybersecurity Maturity Assessment

The Cybersecurity Maturity Assessment will be geared towards adhering to the NIST Cybersecurity Framework. Softchoice will evaluate the fundamental parts of the Authority Cybersecurity program, develop better "security situational awareness," and create a solid foundation for information security program development.

- **Assess Current Conditions**
  - Perform a thorough evaluation of the current state of controls and gain an understanding of the organizational risk appetite and business objectives.
  - Describe the Authority's current cybersecurity posture
  - Describe the Authority's target state for cybersecurity
- **Analyze Gaps**
  - Industry Cybersecurity Framework (NIST) best practices will be compared to the Authority current controls and changes will identified to build a relevant, actionable, and sustainable Cybersecurity program.
  - Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
  - Communicate among internal and external stakeholders about cybersecurity risk.

## Information Security Policies

Developing varying policies, processes, and standards is an integral part in the development of a Governance security strategy for the Authority. These policies will deal with all three parameters that are required for enabling information security including people, technology, and processes. The Information Security policies will be evaluated based on the various domains as defined by NIST and ISO27001.

## Risk Assessment

Softchoice will assist the Authority in devising a Risk Management approach based on the NIST Framework for Improving Critical Infrastructure Cybersecurity that is both effective and efficient. This will include appropriately selecting countermeasures for the Authority that are documented it in a Risk Treatment Plan (RTP). The objective is to build a consistent and cost-benefit course of action that can be efficiently and effectively applied to the risks identified. The treatment action should mitigate the risks in a cost-effective manner and ensure that the Authority is applying security controls that are fully aligned with NIST standards for or federally designated critical infrastructures. In summary, our overall methodology consists of the following:

### 1. Evaluate Risk Management Framework

The aim of the Risk Assessment is to identify the risks faced by the Authority and to implement the most appropriate and cost-effective countermeasures or controls to reduce major risks to an acceptable level. Softchoice will work with the Authority to develop a Risk Management Framework that specifies the set of activities to be performed in establishing an effective and efficient Risk Management process. The Framework will cover:

- Holistic Risk Management sequential activities, including:
    - Confidentiality, Integrity and Availability Assessment Criteria
    - Likelihood Measures
    - Risk Tolerance
- Security Categorization/Impact
- Threat Identification and Analysis
- Vulnerability Identification and Analysis
- Likelihood Determination

## 2. Perform the Risk Assessment

The Risk Assessment will cover Management & Functional security controls and; or; Preventive, Detective and Corrective type of controls. NIST Cybersecurity standards will be considered as the main input to develop the Authority Risk Treatment Plan. Softchoice will document the compliance status of the controls as evaluated and validated during the current state assessment in-line with the NIST Cybersecurity Framework.

## 3. Identify & Assess Risk Treatment Options

For every risk recorded in the 'Risk Register' and for every 'Partially or Not Implemented' control compliance status identified during the current cybersecurity state assessment and risk assessment phases, Softchoice will identify Risk Treatment Options that mitigate the risks and satisfy the relevant control activity. The potential controls will be aligned with the level of maturity intended by the Authority as well as standards developed by the National Institute for Standards and Technology (NIST) for federally designated critical infrastructures. Softchoice will assess the risk treatment options/potential controls and will consider several aspects of the potential countermeasure such as:

- Accountability (can be held responsible)
- Ease of use/Required effort
- Auditability (can it be tested?)
- Minimum manual intervention
- Trusted source (source is known)
- Secure
- Consistently applied
- Protects Confidentiality, Integrity, and Availability of the Authority services
- Cost-effective (implementation and maintenance cost)
- Reliable
- Creates no additional issues during operation

## 4. Evaluate Residual Risk

Residual Risk is the risk remaining when appropriate controls are properly applied to lessen or remove the vulnerability. Softchoice will estimate and evaluate the residual risk based on the defined Risk Treatment Plan and document it in a formal register to enable future monitoring and management review of residual risks.

As part of the project, Softchoice will research, recommend, and present additional technologies to improve security capabilities where deemed necessary. This will be presented in a compare/contrast model with the recommended technologies and/or evaluation/upgrade of existing technologies.

## Penetration & Vulnerability Testing

Softchoice will conduct a Network Penetration Testing assessment of the external network, aka the Internet presence to help identify existing vulnerabilities and their associated risks. Softchoice will discover and identify hosts belonging to the Authority's external network, identify vulnerabilities and exploit vulnerabilities identified during the ethical hacking process. After a system is compromised, the vulnerabilities and any applicable exploits will be documented in a detailed, repeatable process.

Softchoice will also conduct an Internal Network Vulnerability assessment of the Authority's internal network and identify existing vulnerabilities and their associated risks. Softchoice will discover and identify hosts belonging to the Authority's internal network, identify vulnerabilities, and generate reports accordingly.

# General Terms and Conditions

Softchoice provides information technology professional services (“**Services**”) and resells products and related services from third party vendors (collectively, “**Products**”, which include maintenance, support and warranty services).

Our response to your request is provided with the expectation that the final terms and conditions applicable to the provision of Services and/or resale of Products will be negotiated by the parties in good faith upon your acceptance of our proposal. Our standard terms include the following:

i. We will warrant that the Services provided will be performed in a good and workmanlike manner in accordance with generally accepted standards and practices and will re-perform any Services that do not meet this warranty, within a mutually agreed-upon time period.

ii. Products are subject to end user license agreements, subscription agreements, or such other terms of use required by third party vendors. Third party vendors often provide warranties or indemnities directly to the end customer under these agreements or terms of use. As a reseller, Softchoice does not directly provide any warranties or indemnities for products.

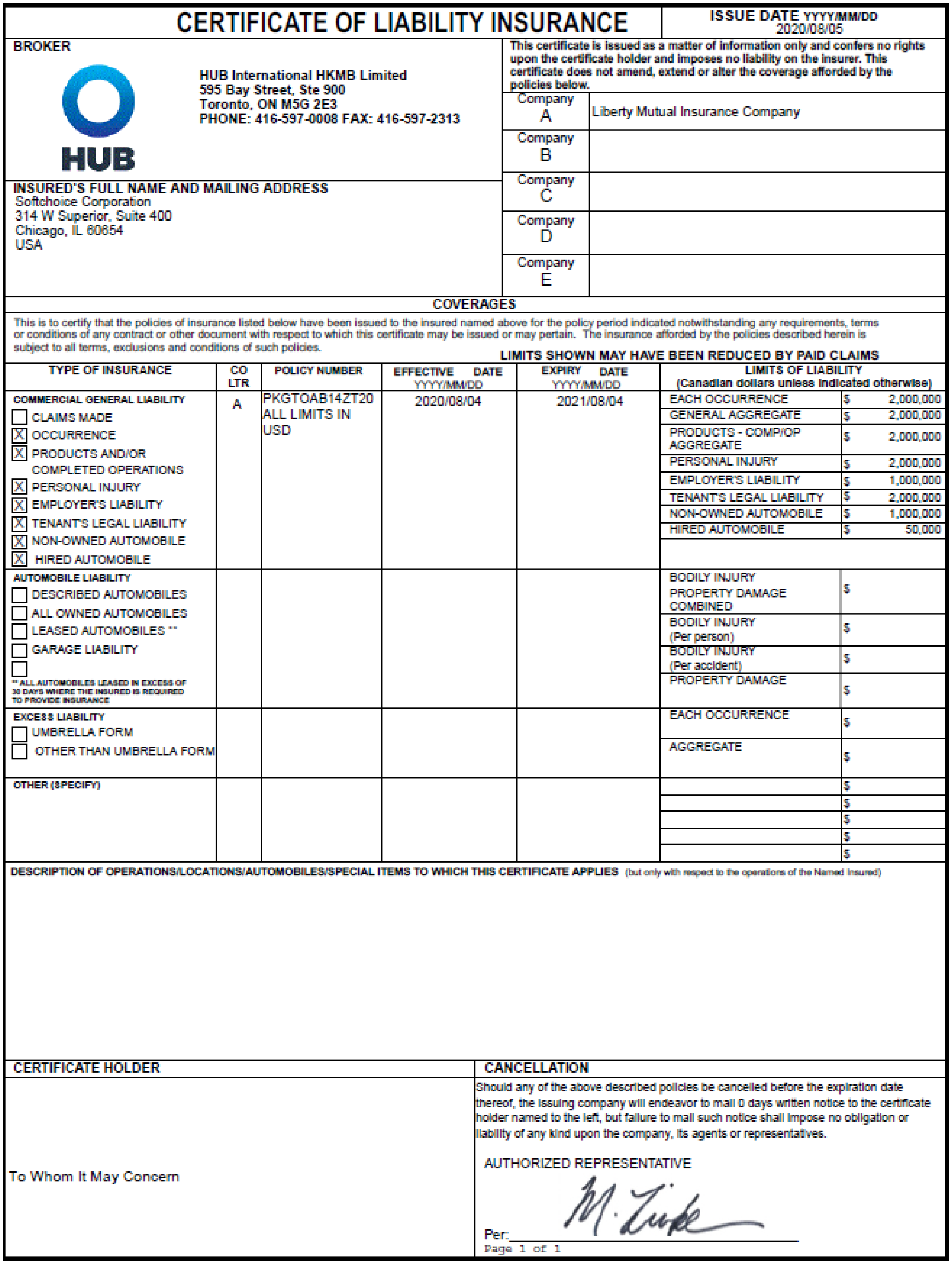
iii. Our liability will be limited to the dollar amount paid for the Product or Service. Neither party would be liable for any indirect, special or consequential damages, lost or corrupted data, or for any lost earnings or profits.

Our response contains confidential information of Softchoice. Neither party shall be liable for any loss, damage, cost or expense suffered or incurred by the other party in respect of this proposal.

Thank you for your consideration of our response, we look forward to working with you.

# Attachments

## Certificate of Insurance



| | |
|---|---|
| **CERTIFICATE OF LIABILITY INSURANCE** | **ISSUE DATE** YYYY/MM/DD<br>2020/08/05 |

**BROKER**

HUB International HKMB Limited
595 Bay Street, Ste 900
Toronto, ON M5G 2E3
PHONE: 416-597-0008 FAX: 416-597-2313

This certificate is issued as a matter of information only and confers no rights upon the certificate holder and imposes no liability on the insurer. This certificate does not amend, extend or alter the coverage afforded by the policies below.

| | |
|---|---|
| Company A | Liberty Mutual Insurance Company |
| Company B | |
| Company C | |
| Company D | |
| Company E | |

**INSURED'S FULL NAME AND MAILING ADDRESS**

Softchoice Corporation
314 W Superior, Suite 400
Chicago, IL 60654
USA

**COVERAGES**

This is to certify that the policies of insurance listed below have been issued to the insured named above for the policy period indicated notwithstanding any requirements, terms or conditions of any contract or other document with respect to which this certificate may be issued or may pertain. The insurance afforded by the policies described herein is subject to all terms, exclusions and conditions of such policies.

**LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS**

| TYPE OF INSURANCE | CO LTR | POLICY NUMBER | EFFECTIVE DATE YYYY/MM/DD | EXPIRY DATE YYYY/MM/DD | LIMITS OF LIABILITY (Canadian dollars unless indicated otherwise) | |
|---|---|---|---|---|---|---|
| COMMERCIAL GENERAL LIABILITY | A | PKGTOAB14ZT20<br>ALL LIMITS IN<br>USD | 2020/08/04 | 2021/08/04 | EACH OCCURRENCE | $ 2,000,000 |
| ☐ CLAIMS MADE | | | | | GENERAL AGGREGATE | $ 2,000,000 |
| ☒ OCCURRENCE | | | | | PRODUCTS - COMP/OP AGGREGATE | $ 2,000,000 |
| ☒ PRODUCTS AND/OR COMPLETED OPERATIONS | | | | | PERSONAL INJURY | $ 2,000,000 |
| ☒ PERSONAL INJURY | | | | | EMPLOYER'S LIABILITY | $ 1,000,000 |
| ☒ EMPLOYER'S LIABILITY | | | | | TENANT'S LEGAL LIABILITY | $ 2,000,000 |
| ☒ TENANT'S LEGAL LIABILITY | | | | | NON-OWNED AUTOMOBILE | $ 1,000,000 |
| ☒ NON-OWNED AUTOMOBILE | | | | | HIRED AUTOMOBILE | $ 50,000 |
| ☒ HIRED AUTOMOBILE | | | | | | |
| AUTOMOBILE LIABILITY<br>☐ DESCRIBED AUTOMOBILES | | | | | BODILY INJURY PROPERTY DAMAGE COMBINED | $ |
| ☐ ALL OWNED AUTOMOBILES | | | | | BODILY INJURY (Per person) | $ |
| ☐ LEASED AUTOMOBILES ** | | | | | BODILY INJURY (Per accident) | $ |
| ☐ GARAGE LIABILITY<br>☐<br>** ALL AUTOMOBILES LEASED IN EXCESS OF 30 DAYS WHERE THE INSURED IS REQUIRED TO PROVIDE INSURANCE | | | | | PROPERTY DAMAGE | $ |
| EXCESS LIABILITY<br>☐ UMBRELLA FORM | | | | | EACH OCCURRENCE | $ |
| ☐ OTHER THAN UMBRELLA FORM | | | | | AGGREGATE | $ |
| OTHER (SPECIFY) | | | | | | $ |
| | | | | | | $ |
| | | | | | | $ |
| | | | | | | $ |
| | | | | | | $ |

**DESCRIPTION OF OPERATIONS/LOCATIONS/AUTOMOBILES/SPECIAL ITEMS TO WHICH THIS CERTIFICATE APPLIES** (but only with respect to the operations of the Named Insured)

**CERTIFICATE HOLDER**

To Whom It May Concern

**CANCELLATION**

Should any of the above described policies be cancelled before the expiration date thereof, the issuing company will endeavor to mail 0 days written notice to the certificate holder named to the left, but failure to mail such notice shall impose no obligation or liability of any kind upon the company, its agents or representatives.

AUTHORIZED REPRESENTATIVE

Per:

Page 1 of 1

KCD48DWR

## Softchoice Master Services Agreement

*(Included as a separate document)*

STEALTH
ISS GROUP

June 11, 2021

Terrence D. McCracken
Secretary to the Authority
Erie County Water Authority
295 Main Street, Room 350
Buffalo, New York 14203

Dear Mr. McCracken,

The CEO of Stealth-ISS Group® Inc. ("Stealth Group" hereafter), Robert Davies, an authorized company official, is delighted for this opportunity to work with you.

We would like to take a moment to thank you for allowing us to collaborate with you on understanding your concerns and reducing your cybersecurity risk profile. Our mission is to become your trusted partner, a true collaborator, and not "just another vendor." We look forward to long-lasting business and a mutually beneficial relationship with you.

Your decision to test your cybersecurity risk is prudent. Continued, high-profile cyber-attacks and an evolving regulatory landscape mean that public benefit entities need to proactively implement capabilities to detect and respond to security incidents. Adversaries are increasingly targeting critical infrastructure to disrupt the lives of consumers and "earn" a huge payout – in May 2021, Colonial Pipeline paid cyber-criminals over $4 million[1] after a cyber-attack shut down the fuel pipeline network. Organizations such as yours maintain systems critical to the livelihoods of the citizens of Erie County and it is essential to protect them from bad actors. It is becoming unmistakably clear that robust cybersecurity measures are an indispensable investment to combat the risks of ransomware, phishing attacks, and other threats facing your critical infrastructure.

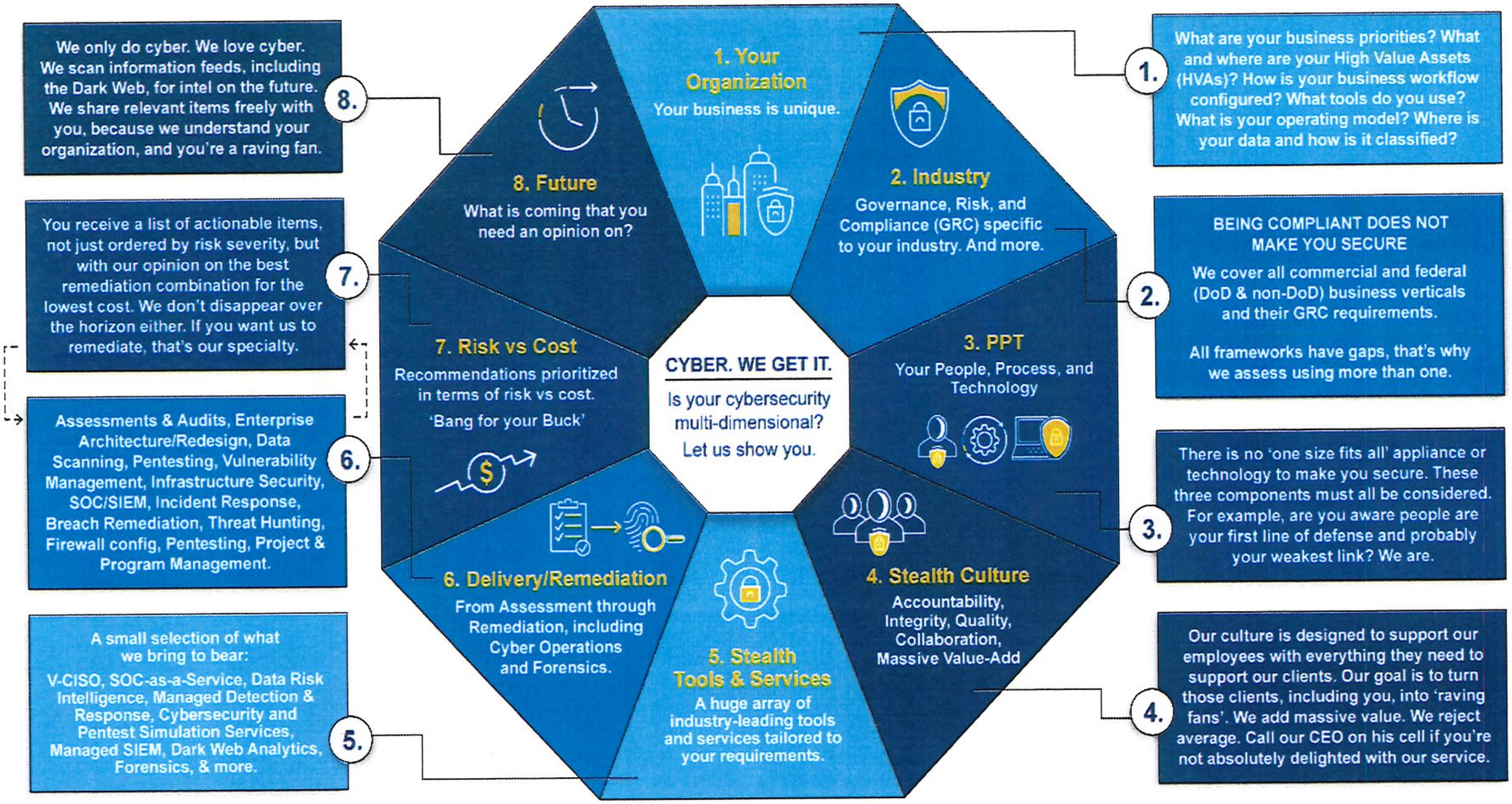
The Erie County Water Authority (the "Authority") will be served well by Stealth Group, a company whose sole focus is cybersecurity and helping organizations understand their current cyber risk profile and prepare for, or react to, high-risk threats. Established in 2002, Stealth Group is a total service cybersecurity and compliance consulting company that uses its deep domain knowledge to assess and remediate cybersecurity problems of vital importance to the Nation and internationally. Stealth Group is a Federally recognized Service-Disabled Veteran-Owned Small Business (SDVOSB) and Economically Disadvantaged Woman-Owned Small Business (EDWOSB) providing the full portfolio of Cybersecurity Consulting, Regulatory Compliance, Risk Management, and IT security engineering services. Cyber Defense Awards recognized our president and founder, Dasha Deckwerth, as one of the top 100 Chief Information Security Officers of 2020.

[1] Bloomberg, "Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom." May 13, 2021. https://bloom.bg/3hnngHz

Stealth Group does not offer a "one-size-fits-all" approach to cybersecurity, which is why we have won many awards and continue to grow, both commercially and in the state and local government and educational spaces. When you hire Stealth Group, you benefit from a cybersecurity company whose focus is on quality outcomes for you, by way of completely tailored solutions for you, through full collaboration with you, and underpinned by a company culture built on accountability, quality, and integrity.

Unlike many cybersecurity companies, Stealth Group specializes in tailored cybersecurity solutions specific to our clients' requirements. We are a specialist Managed Security Service Provider (MSSP), not a Managed Service Provider (MSP) that dabbles in security. Our wide variety of services and breadth and depth of our technical knowledge enable us to deliver a solution for every combination of cybersecurity pain points. To be able to deliver fully tailored solutions we see cybersecurity in eight dimensions, where other cybersecurity companies only tend to consider two or three:

1. Organizational Context – You and your business are unique and have a unique set of pain points, configuration, operation, and strategy. One size does not fit all.
2. Industry Vertical – Consideration of Governance, Risk, and Compliance (GRC) guides or mandates specific to your industry. We also consider ISO27K, Information Security Forum (ISF), and other frameworks for gaps that are relevant to your organization in your industry. Being compliant doesn't mean you are secure. Each vertical also has its own preferred technologies and way of doing things.
3. People, Process, Technology – We don't just do technology; all three components must be considered together. For example, people are your first line of defense and are often your weakest link. Technology alone will not meet your requirements.
4. Stealth Group Culture – Our culture supports our clients through accountability, integrity, quality, and collaboration. Our culture has only one goal – create raving fans of Stealth Group.
5. Stealth Group Tools and Services – We offer a huge array of industry-leading tools and best practice services, tailored and combined to serve your unique requirements. We review thousands of tools and services; we only choose those that are best of breed and that also deliver massive value.
6. Delivery and Remediation – From Assessment through Remediation, we cover the entire spectrum of cyber, including Penetration Testing, Vulnerability Scanning, Cyber Operations, Incident Response, Forensic Analysis, and Dark Web.
7. Risk vs. Cost – Recommendations are prioritized for you in terms of risk severity and the best remediation combination for the lowest cost.
8. The Future – GRC/Policy changes, Dark Web trends, Blockchain, Internet of Things (IoT), Microsegmentation, Artificial Intelligence (AI), Quantum Computing, Zero Trust – What is coming that you need to anticipate?



1. Your Organization
Your business is unique.

2. Industry
Governance, Risk, and Compliance (GRC) specific to your industry. And more.

3. PPT
Your People, Process, and Technology

4. Stealth Culture
Accountability, Integrity, Quality, Collaboration, Massive Value-Add

5. Stealth Tools & Services
A huge array of industry-leading tools and services tailored to your requirements.

6. Delivery/Remediation
From Assessment through Remediation, including Cyber Operations and Forensics.

7. Risk vs Cost
Recommendations prioritized in terms of risk vs cost.
'Bang for your Buck'

8. Future
What is coming that you need an opinion on?

CYBER. WE GET IT.
Is your cybersecurity multi-dimensional?
Let us show you.

1. What are your business priorities? What and where are your High Value Assets (HVAs)? How is your business workflow configured? What tools do you use? What is your operating model? Where is your data and how is it classified?

2. BEING COMPLIANT DOES NOT MAKE YOU SECURE

We cover all commercial and federal (DoD & non-DoD) business verticals and their GRC requirements.

All frameworks have gaps, that's why we assess using more than one.

3. There is no 'one size fits all' appliance or technology to make you secure. These three components must all be considered. For example, are you aware people are your first line of defense and probably your weakest link? We are.

4. Our culture is designed to support our employees with everything they need to support our clients. Our goal is to turn those clients, including you, into 'raving fans'. We add massive value. We reject average. Call our CEO on his cell if you're not absolutely delighted with our service.

5. A small selection of what we bring to bear:
V-CISO, SOC-as-a-Service, Data Risk Intelligence, Managed Detection & Response, Cybersecurity and Pentest Simulation Services, Managed SIEM, Dark Web Analytics, Forensics, & more.

6. Assessments & Audits, Enterprise Architecture/Redesign, Data Scanning, Pentesting, Vulnerability Management, Infrastructure Security, SOC/SIEM, Incident Response, Breach Remediation, Threat Hunting, Firewall config, Pentesting, Project & Program Management.

7. You receive a list of actionable items, not just ordered by risk severity, but with our opinion on the best remediation combination for the lowest cost. We don't disappear over the horizon either. If you want us to remediate, that's our specialty.

8. We only do cyber. We love cyber. We scan information feeds, including the Dark Web, for intel on the future. We share relevant items freely with you, because we understand your organization, and you're a raving fan.

Exhibit 1: Eight Dimensions of Cybersecurity

We bring a depth of understanding of the policies relating to the management and securing of organizations, conform to standards, requirements, and procedures set by the National Institute of Standards and Technology (NIST), North America Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), Information Security Forum (ISF), International Organization for Standardization (ISO) 27001, and other industry practices.

You will receive huge value from our cybersecurity services – not only does Stealth Group provide technical and executive reports of risks and remediation proposals, but we also identify any shortcomings against the above frameworks and standards, including the NIST Cybersecurity Framework (NIST CSF). For added value, we prioritize the risks in order of most effective sequence of remediation, while considering cost and impact to business operations.

With over 19 years of demonstrated success in providing innovative cybersecurity solutions, Stealth Group has a wide range of past performance examples in terms of scope, size, scale, and complexity. Previous clients have included the Town of North Kingstown, Rhode Island; Baha Mar Resort & Casino; the U.S. Department of Transportation; the Olympic Broadcasting Service during the 2018 Winter Olympics; and numerous other North Atlantic Treaty Organization (NATO) and commercial Fortune 100 clients.

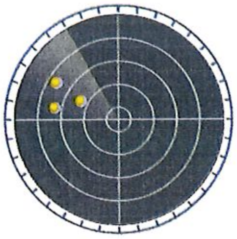
Thank you again for allowing us this opportunity to earn your business; it is our absolute pleasure to work with you. We hope that through our approach and expertise, flexibility, and clear addition of massive value that you will be our next 'raving fan.'

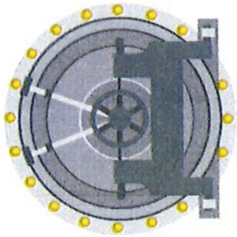
Sincerely,

I.A.

DASHA DECKWERTH
- PRESIDENT STEALTH-ISS GROUP W.L

Robert Davies, CEO
robert.davies@stealth-iss.com





We bring a depth of understanding of the policies relating to the management and securing of organizations, conform to standards, requirements, and procedures set by the National Institute of Standards and Technology (NIST), North America Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), Information Security Forum (ISF), International Organization for Standardization (ISO) 27001, and other industry practices.

You will receive huge value from our cybersecurity services – not only does Stealth Group provide technical and executive reports of risks and remediation proposals, but we also identify any shortcomings against the above frameworks and standards, including the NIST Cybersecurity Framework (NIST CSF). For added value, we prioritize the risks in order of most effective sequence of remediation, while considering cost and impact to business operations.

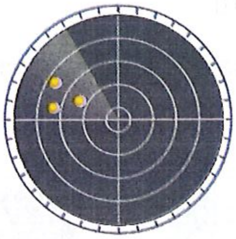
With over 19 years of demonstrated success in providing innovative cybersecurity solutions, Stealth Group has a wide range of past performance examples in terms of scope, size, scale, and complexity. Previous clients have included the Town of North Kingstown, Rhode Island; Baha Mar Resort & Casino; the U.S. Department of Transportation; the Olympic Broadcasting Service during the 2018 Winter Olympics; and numerous other North Atlantic Treaty Organization (NATO) and commercial Fortune 100 clients.

Thank you again for allowing us this opportunity to earn your business; it is our absolute pleasure to work with you. We hope that through our approach and expertise, flexibility, and clear addition of massive value that you will be our next 'raving fan.'

Sincerely,

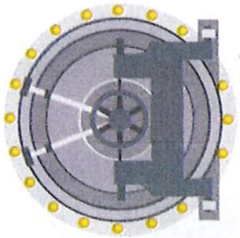
Robert Davies

Robert Davies, CEO
robert.davies@stealth-iss.com



GET SHARP.

GET SERIOUS.



GET SAFE.

STEALTH
ISS GROUP®

# Erie County Water Authority

# Cybersecurity Risk and Vulnerability Assessment

## Response to Request for Proposal Project Number 202100116

**Response Due Date**: June 11, 2021, 4:00pm EDT

**Submitted By:**

Robert Davies, CEO
Stealth-ISS Group® Inc.
4601 North Fairfax Drive, Suite 1200
Arlington, Virginia 22203
proposals@stealth-iss.com

**Submitted To:**

Terrance D. McCracken
Secretary to the Authority
Erie County Water Authority
295 Main Street, Room 350
Buffalo, New York 14203
tmmccracken@ecwa.org

This response shall be valid for a period of one hundred-twenty (120) calendar days from the stated due date.

Per the New York Freedom of Information Law, this submission shall be considered non-confidential and available to the public, excepting any portions identified and marked "CONFIDENTIAL." Each specific portion or portions of this submission which are confidential have been so marked.

# TABLE OF CONTENTS

Table of Contents ........ 6

Table of Exhibits ........ 7

Glossary of Abbreviations ........ 7

Part 1 ........ 10

Part 2 ........ 11

Consultant Business Form ........ 11

1. Identify the Consultant's corporate structure. ........ 11

2. Identify the number of years your entity has been in business. ........ 11

3. Identify whether your business/corporate structure has changed in the past five years and if yes, describe the change. ........ 11

4. Identify the type and coverage amount of all insurance policies. ........ 11

5. Identify the name, address, and contract information for three (3) companies that the Consultant has performed similar services to those being sought by the Authority. ........ 12

6. If you are a certified, minority and/or women-owned business, submit a copy of the certification. ........ 13

Item 2 – Consultant Team ........ 13

Part 3 ........ 15

Item 1 – Proposed Scope of Service ........ 15

Current State Review ........ 15

Vulnerability Mitigation Plan ........ 16

Road Map to Future State ........ 16

Best Practice Methodologies ........ 17

Assessment ........ 17

Reporting ........ 23

System Security Plan (SSP) ........ 23

Gap Analysis and Plan of Action and Milestones (POA&M) ........ 24

Target Operating Model ........ 24

Item 2 – Hardware and Software Requirements ........ 25

Item 3 – Timeframe for Deliverables ........ 25

Item 4 – Price Structure ........ 25

Pricing Methodology ........ 26
Project Price ........ 26
Itemized Travel and Out-of-Pocket Expenses ........ 27
Project Assumptions and Dependencies ........ 27
Appendix A: WOSB Program Letter ........ 29
Appendix B: Resumes ........ 30

# TABLE OF EXHIBITS

Exhibit 1: Eight Dimensions of Cybersecurity ........ 3
Exhibit 2: Sample Social Engineering Report – Phishing Campaign ........ 22
Exhibit 3: Sample Password Complexity Chart – Phishing Campaign ........ 22
Exhibit 4: Estimated Project Timeline ........ 25
Exhibit 5: Project Pricing Breakdown ........ 27

# GLOSSARY OF ABBREVIATIONS

| Acronym | Definition | Acronym | Definition |
|---|---|---|---|
| AB | Accreditation Board | IP | Internet Protocol |
| AD | Active Directory | IPS | Intrusion Prevention System |
| AI | Artificial Intelligence | IRP | Incident Response Plan |
| APT | Advanced Persistent Threat | ISACA | Information Systems Audit and Control Association |
| ATO | Authority to Operate | ISC2 | International Information System Security Certification Consortium |
| BA | Bachelor of Arts | ISF | Information Security Forum |
| BAS | Breach and Attack Simulation | ISO | International Organization for Standardization |
| BPA | Blanket Purchase Agreement | ISSA | Information Systems Security Association |
| CCCM | Certified Commercial Contracts Manager | ISSAP | Information Systems Security Architecture Professional |
| CCO | Certified Confidentiality Officer/Business Espionage | ISSMP | Information Systems Security Management Professional |
| CCPA | California Consumer Privacy Act | ITCP | Information Technology Contingency Plan |
| CCSA | Check Point Certified Security Administrator | ITIL | Information Technology Infrastructure Library |

| Acronym | Definition | Acronym | Definition |
|---|---|---|---|
| CCSE | Check Point Certified Security Expert | KPI | Key Performance Indicator |
| CCTV | Closed Circuit Television | MAS | Multiple Award Schedule |
| CEO | Chief Executive Officer | MBA | Master of Business Administration |
| CERT | Community Emergency Response Team | MS | Master of Science |
| CFCM | Certified Federal Contract Manager | MSP | Managed Service Provider |
| CGEIT | Certified in the Governance of Enterprise IT | MSSP | Managed Security Service Provider |
| CHFI | Computer Hacking Forensic Investigator | NATO | North Atlantic Treaty Organization |
| CIP | Critical Infrastructure Protection | NCMA | National Contract Management Association |
| CIS | Center for Internet Security | NERC | North American Electric Reliability Corporation |
| CISA | Certified Information Systems Auditor | NIST | National Institute of Standards and Technology |
| CISM | Certified Information Security Manager | NSA | National Security Agency |
| CISO | Chief Information Security Officer | NTE | Not to Exceed |
| CISSP | Certified Information Systems Security Professional | OBS | Olympic Broadcast Services |
| CMMC | Cybersecurity Maturity Model Certification | OMB | The Office of Management and Budget |
| COTS | Commercial Off the Shelf | OWASP | Open Web Application Security Project |
| CRISC | Certified in Risk and Information Systems Control | PA | Provisional Assessor |
| CSC | Critical Security Controls | PCI | Payment Card Industry |
| CSF | Cyber Security Framework | PCIP | Payment Card Industry Professional |
| DFARS | Defense Federal Acquisition Regulation Supplement | PMI | Project Management Institute |
| DISA | Defense Information Systems Agency | PMP | Project Management Professional |
| DLA | Defense Logistics Agency | POA&M | Plan of Action and Milestones |
| DNS | Domain Name System | QSA | Qualified Security Assessor |
| DSS | Data Security Standard | RMF | Risk Management Framework |
| EDWOSB | Economically Disadvantaged Woman-Owned Small Business | ROE | Rules of Engagement |
| FBI | Federal Bureau of Investigation | RSS | Rich Site Summary |
| FEMA | Federal Emergency Management Agency | SAP | Security Assessment Plan |
| FIPS | Federal Information Processing Standards | SAR | Security Architecture Review |

| Acronym | Definition | Acronym | Definition |
|---|---|---|---|
| FISMA | Federal Information Security Modernization Act | SCADA | Supervisory Control and Data Acquisition |
| FSSI | Federal Strategic Sourcing Initiative | SDVOSB | Service-Disabled Veteran-Owned Small Business |
| GDPR | General Data Protection Regulation | SLED | State, Local Government, and Education |
| GLBA | Gramm–Leach–Bliley Act | SOX | Sarbanes-Oxley Act |
| GPO | Group Policy Objects | SP | Special Publication |
| GRC | Governance, Risk, and Compliance | SRR | Security Readiness Review |
| GSA | General Services Administration | SSP | System Security Plan |
| GSS | General Support System | TOM | Target Operating Model |
| HACS | Highly Adaptive Cybersecurity Services | TTP | Tactics, Techniques, and Procedures |
| HCISSP | Health Care Security Professional | USACE | U.S. Army Corps of Engineers |
| HIPAA | Health Insurance Portability and Accountability Act | VOIP | Voice over IP |
| IAM | Identity and Access Management | VPN | Virtual Private Network |
| ICFP | Institute of Computer Forensic Professionals | WBS | Work Breakdown Structure |
| IDS | Intrusion Detection System | WEP | Wired Equivalent Privacy |
| IEEE | Institute of Electrical and Electronics Engineers | WLAN | Wireless Local Area Network |
| IEM | Information Security Evaluation Methodology | WOSB | Woman-Owned Small Business |
| INDOPACOM | United States Indo-Pacific Command | WPA | Wi-Fi Protected Access |
| IOC | Indicators of Compromise | | |

# PART 1

## Item 1 – Name of Organization

Stealth-ISS Group® Inc. ("Stealth Group" hereafter)

## Item 2 – Name and Title of Contact Person

Robert Davies, Chief Executive Officer

## Item 3 – Business Address

4601 North Fairfax Drive, Suite 1200
Arlington, Virginia 22203

## Item 4 – Telephone Number

866-500-0751

## Item 5 – Email Address

proposals@stealth-iss.com

## Item 6 – Fax No.

866-500-0751

# PART 2

## Consultant Business Form

1. **Identify the Consultant's corporate structure.**

   Stealth-ISS Group® Inc. is a "C" Corporation.

| | |
|---|---|
| Date and State of Incorporation | 10/2002, State of Florida |
| List Name and Title of Executive Officers | Dasha Deckwerth, President<br>Robert Davies, Secretary & Treasurer |
| Principal Place of Business | Headquarters<br>4601 North Fairfax Drive, Suite 1200<br>Arlington, Virginia 22203 |
| List all Related Principal or Subsidiaries Corporations | N/A |
| Closed or Publicly Traded | Closed |
| Federal Employer Tax Identification Number | 98-0392447 |

2. **Identify the number of years your entity has been in business.**

   19 years

3. **Identify whether your business/corporate structure has changed in the past five years and if yes, describe the change.**

   Yes – in 2018 we opened a branch office in Huntsville, Alabama. This branch was closed in 2021 due to COVID-19 but all staff were retained and continue to work remotely.

4. **Identify the type and coverage amount of all insurance policies.**

   Current insurance type and coverage amount:

   1. Commercial General Liability $2,000,000/$2,000,000
   2. Cyber and Data Risk $1,000,000/$1,000,000

   We believe this is a suitable amount of coverage for the work requested by the Authority, but can discuss it with the Authority upon award and scale as appropriate.

**5. Identify the name, address, and contract information for three (3) companies that the Consultant has performed similar services to those being sought by the Authority.**

The following recent and highly relevant contracts demonstrate Stealth Group's corporate experience and past performance that is similar in scope and magnitude to your requirements. Our references are evidence of expertise and corporate capabilities relative to all of your requirements, while also demonstrating our strategic vision through use of best practices, tools, processes, and innovation. Our work demonstrates conformance to contract requirements and to standards of great workmanship, record of forecasting and controlling costs, and adherence to contract schedules, including the administrative aspects of performance. Each reference shows a history of reasonable, collaborative, and cooperative behavior, and total commitment to customer satisfaction.

| Town of North Kingstown<br>Information Systems Security Risk Assessment Audit with<br>NIST Cybersecurity Framework Maturity Assessment | |
|---|---|
| Point of Contact Name | Michael Forlingieri |
| Address | 100 Fairway Drive<br>North Kingstown, Rhode Island 02852 |
| Email | mforlingieri@northkingstown.org |
| Period of Performance | 06/2020 – 12/2020 |
| Purchase Order | 20202166-00 |
| Contract Type | Firm, Fixed Price |

| Baha Mar Resort & Casino<br>NIST 800 Enterprise Assessment<br>Risk and Vulnerability Assessment<br>Continuing Services – Virtual Chief Information Security Officer | |
|---|---|
| Point of Contact Name | Jeff Burge |
| Address | One Baha Mar Boulevard<br>Nassau, The Bahamas |
| Email | jeff.burge@bahamar.com |
| Period of Performance | 01/2017 – Present |
| Contract Number | BHM90001 |
| Contract Type | Time and Materials |

| U.S. Department of Transportation<br>Security Control Assessment – NIST SP 800-53 | |
|---|---|
| Point of Contact Name | Terrance King |
| Address | 1200 New Jersey Ave SE<br>Washington, DC 20590 |
| Email | terrance.king@dot.gov |
| Period of Performance | 09/2019 – 12/2019 |

| | |
|---|---|
| Contract Number | 693JJ319F000513 |
| Contract Type | Firm, Fixed Price |

**6. If you are a certified, minority and/or women-owned business, submit a copy of the certification.**

We have included a letter from the U.S. Small Business Administration regarding our EDWOSB/WOSB certification as Appendix A.

## Item 2 – Consultant Team

We are fully confident that our team is second to none in our quest to meet and surpass the requirements, as we bring massive experience with the right skills and certifications. Our cybersecurity-certified professionals are experienced in the Commercial, Federal, and State, Local Government, and Education (SLED) security processes, regulatory compliance, vulnerability assessments, penetration testing, and risk mitigation.

| | Proposed Personnel | | | | |
|---|---|---|---|---|---|
| **Experience and Role** | **Misty R.** | **Dasha D.** | **Inno E.** | **Daniel C.** | **Robert D.** |
| Years of Experience | 12+ | 25+ | 20+ | 11+ | 25+ |
| Length of Time Working for Stealth Group | 1 year | 19 years | 1 year | < 1 year | 5 years |
| County / State of Residence | Rock County / Wisconsin | Pinellas County / Florida | Loudoun County / Virginia | Geauga County / Ohio | Clark County / Nevada |
| Scope of Responsibility | Project Manager | Senior Assessor/ Security | Senior Assessor/ Network | IT Technical Writer | Operating Model Consultant |
| **Certifications** | | | | | |
| Project Management Professional (PMP) | ✓ | ✓ | | | |
| Certified Information System Security Professional (CISSP) | | ✓ | ✓ | | |
| Certified Information Security Manager (CISM) | | | ✓ | | |
| Certified in the Governance of Enterprise IT (CGEIT) | | ✓ | | | |
| Certified in Risk and Information Systems Control (CRISC) | | ✓ | | | |
| Certified Information Systems Auditor (CISA) | | | ✓ | | |
| PRINCE2 | | | | | ✓ |

We have provided, in Appendix B, abbreviated resumes indicative of the quality of our staff members. If the listed candidate is unavailable at the time of the project start, staff similar or equal in experience, qualifications, and certifications will be selected for your review.

# PART 3

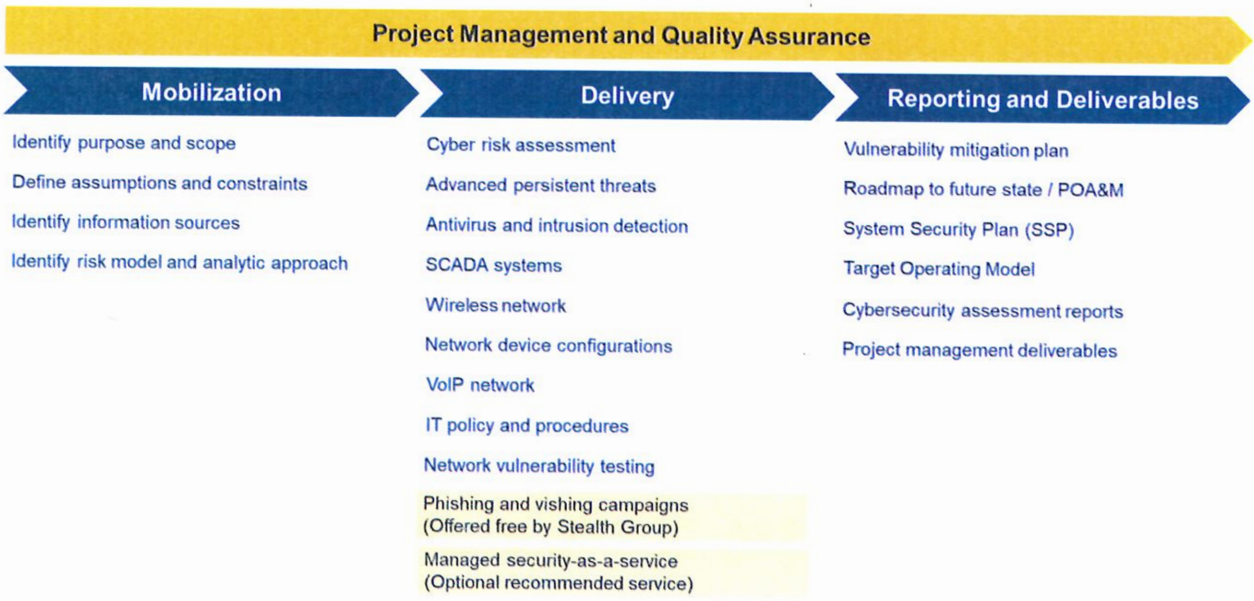
## Item 1 – Proposed Scope of Service

To support the Erie County Water Authority's mission of providing customers with a plentiful supply of safe, high quality, and affordable drinking water, Stealth Group will conduct a comprehensive IT Cybersecurity Risk and Vulnerability Assessment, the results of which will enable you to efficiently strengthen the security and reliability of your critical infrastructure systems.

The objective of this engagement is to:

a. Analyze your vulnerabilities, threats, and possible consequences from potential internal or external cyberattacks
b. Rank vulnerability and security issues by priority and the timeframe to address
c. Advise the Authority on matters relating to employee training and education, and preventative measures to be taken to secure Authority assets
d. Recommend additional staffing for the Authority's IT Department

We are able to meet your objectives by leveraging our experience as a total service cybersecurity and consulting company and using a phased approach:



Project Management and Quality Assurance

| Mobilization | Delivery | Reporting and Deliverables |
|---|---|---|
| Identify purpose and scope | Cyber risk assessment | Vulnerability mitigation plan |
| Define assumptions and constraints | Advanced persistent threats | Roadmap to future state / POA&M |
| Identify information sources | Antivirus and intrusion detection | System Security Plan (SSP) |
| Identify risk model and analytic approach | SCADA systems | Target Operating Model |
|  | Wireless network | Cybersecurity assessment reports |
|  | Network device configurations | Project management deliverables |
|  | VoIP network |  |
|  | IT policy and procedures |  |
|  | Network vulnerability testing |  |
|  | Phishing and vishing campaigns (Offered free by Stealth Group) |  |
|  | Managed security-as-a-service (Optional recommended service) |  |

### Current State Review

We will conduct a risk assessment that follows the NIST SP 800-30, *Guide for Conducting Risk Assessments*. This ensures that the Authority receives a methodical, comprehensive assessment of your risks. Using this will enable us to work with you and challenge your thinking around crucially important strategic questions such as:

- What Information Assets does your organization possess?
- How valuable are those assets in business terms? What is the impact on your business if any of those assets suffer harm in terms of their Confidentiality, Integrity, or Availability?
- What threats (accidental and environmental as well as adversarial) does your organization face? How capable are those threats and what are their motivations?
- Address all relevant areas for your business and industry and best business practices.

The purpose of taking this approach is that it provides not just the information you need to be informed about your security posture, but also a business context and justification for making improvements to individual security controls. It provides a means of determining which aspects of your security need addressing more urgently than others. Our hypothesis is that without having this structure in place you may be placing undue emphasis on certain aspects of security which may not give you the best return on your investment. Security is all about identifying and managing risk and applying finite budgets in the most effective and efficient manner – rather than having a very long list of action items that may or may not do anything to manage the overall risk to your business.

**Vulnerability Mitigation Plan**

After all assessments have been completed, Stealth Group provides you with a report including all documentation of recommended policy changes, remediation recommendations, and other relevant data required based on the outcome and in adherence to the applicable standards. A detailed chart which cross-references the standards is included. These results will inform and drive most of your decision-making and discussion that will follow and play a key role when creating the Plan of Actions and Milestones (POA&M).

Per answers to questions released during the solicitation period, the Authority does not currently utilize a Governance, Risk Management, and Compliance (GRC) tool. We can assist you with selecting a reporting tool, which allows for prioritized remediation, Key Performance Indicator (KPI) measurement of program maturity and CSF compliance, and as a shared portal for centralized use by your security teams and managers for proactive monitoring of risk, progress, delays, and exceptions.

**Road Map to Future State**

Performing a comprehensive risk assessment against relevant industry-recognized frameworks (e.g., NIST CSF, NERC-CIP, ISF, and data privacy requirements) will result in a list of threats, vulnerabilities, probabilities of occurrence, and controls in place to mitigate the identified risks. Once Stealth Group has completed the current state ("as is") assessments of the Authority's Information Systems security program, we will provide observations and recommendations for overall program improvement. The future state ("to be") architecture will be less vulnerable to unwarranted risks or hacks.

**Best Practice Methodologies**

Over time and experience, Stealth Group has developed a common-sense approach aligning cybersecurity risk to the three pillars of consulting – People, Process, and Technology. The key aspects of our methodology are:

- Understand, refine, and confirm client requirements
- People awareness review – phishing campaigns, etc.
- Supporting process, policy, and documentation review
- Technology assessment (vulnerability scans, penetration testing, tech architecture)
- Risk analysis following the NIST SP 800-30, *Guide for Conducting Risk Assessments*
- Report including list of risk-prioritized action items

To support this methodology, and depending on the client and their industry context, we use various frameworks and tools to provide some boundaries to the project. This assessment will be delivered via the "Framework for Improving Critical Infrastructure Cybersecurity":

- NIST Cybersecurity Framework – to assess against best business practices in the following areas:
    - Identify: Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy
    - Protect: Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, Protective Technology
    - Detect: Security Continuous Monitoring, Detection Processes
    - Respond: Response Planning, Communications, Analysis, Mitigation, Improvements
    - Recover: Recovery Planning, Improvements, Communication

**Assessment**

*Advanced Persistent Threats*
Stealth Group will evaluate your capability to detect, prevent, and respond to indicators of compromise (IOC) and APT techniques, tactics, and procedures (TTP) in the network and on hosts. This will include assessing the following:

- Detection and response processes and Standard Operating Procedures (SOPs)
- Logging and monitoring capabilities
- Tools, processes, and resources to detect unusual network traffic vs. the baseline, privileged user account activity, login anomalies, increases in database read volumes, suspicious registry of system file changes, unusual DNS requests, and web traffic showing non-human behavior.

### *Antivirus and Intrusion Detection and Prevention Capabilities*

Per NIST SP 800-83, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, malware, or malicious code, is the most common external threat to most hosts. Classic categories of malware include:

- Viruses
  - Compiled Viruses
  - Interpreted Viruses
- Worms
  - Network Service Worms
  - Mass Mailing Worms
- Trojan Horses
- Malicious Mobile Code

Many modern instances of malware are blended attacks of the classic categories and can be challenging to detect and remove. While the best virus protection is following a robust policy and maintain awareness, Stealth Group will also check the Authority's preparedness by assessing the following:

- Antivirus software
- Intrusion Prevention Systems
- Firewalls
- Content Filtering/Inspection
- Application Whitelisting
- BIOS Protection
- Sandboxing
- Browser Separation
- Segregation through Virtualization

### *Review SCADA Systems*

The following process is the best practice method we use for assessing a Supervisory Control and Data Acquisition (SCADA) system:

- Meet with you to identify the exact details of the SCADA systems in scope and agree upon a detailed Rules of Engagement (ROE).
- Perform reconnaissance to gather information on the target system.
- Scan the SCADA network for open ports and vulnerabilities, test for published exploits, perform static code analysis, hardware configuration review, and log review as appropriate based on system sensitivity.
- Check for vulnerabilities that are associated with the main cyber-attack methods targeting SCADA systems:
  - Trojan Malware - Attacks using Advanced Windows-executable malware for remote control methods

  - Spear Phishing - Email spear phishing with spoofed sender identity and malicious attachments
  - Remote Control - Remote operation of power company substation equipment and systems
  - Destructive Action - Attacks that destroy files on substation servers and devices
  - Denial of Service - Attacks to degrade your ability to provide service to affected customers
- Return the system to its original state, removing all traces of penetration testing activities.
- Deliver reports detailing all findings and recommended remediation steps.

*Wireless Network Assessment*
The Authority's wireless systems will be tested to include internal touchpoints from all Service Set Identifiers (SSIDs) – broadcast or hidden – as well as encryption levels. A walkthrough of your facilities will be conducted to evaluate IEEE 802.11 emissions and to determine if any rogue access points are in use.

Per NIST SP 800-153, *Guidelines for Securing Wireless Local Area Networks (WLANs)*, some items which will be checked will include:

- Verifying that standardized security configurations for common WLAN components have been implemented
- Determining how the security of the WLAN affects the security of other networks
- Examine policies regarding dual connections
- Test attack and vulnerability monitoring
- Check frequency of WLAN technical security assessments

*Device Configuration Review*
Stealth Group consultants will conduct a detailed review of your network security goals and requirements as well as evaluating any associated security technology policies. Our security assessors will partner with your network and systems architects to:

- Conduct an in-depth analysis of the network security architecture, including the network topology (including wireless networks), solution components, device features, and configurations.
- Review firewall, router, network switch, VOIP, email and file servers, and CCTV configurations.
- Evaluate security technology policies for remote access, network segmentation, server protection, authentication, and firewall design.
- Assess cascading security controls over networks, systems, and applications that overlap for vital redundancy.
- Assess your Active Directory (AD) configuration and Group Policy Object (GPO) settings to identify potential attack vectors. Key assessment areas include:
  - Infrastructure Configuration Visibility and Management

  - Domain Controllers
  - Group Policy and Privilege Controls
  - Recommendations and Remediation Plans
- Conduct an automated scan of the VPN, allowing us to identify exploitation points. Once completed, an automated and manual review of the configuration file of the VPN will be analyzed to identify additional risks and provide remediation actions.

Following the above analysis, Stealth Group will provide you with a detailed analysis of network security architecture vulnerabilities and operational risks. This will include an evaluation on how closely the current security architecture aligns with industry network security best practices.

As part of the delivery, you will receive a prioritized recommendation to mitigate the identified operational risks, including improvements to topology, protocols, policy, device configurations, and network and security management tools. By following a systematic and detailed approach to assessing network security, the service helps organizations reduce threats to the confidentiality, integrity, and availability of business processes and applications and helps to improve risk management and satisfy compliance needs.

### *VoIP Assessment*

Your VoIP network system components will be assessed for any known security vulnerabilities. The following process is the best practice method we use for assessing a Voice-over-IP (VoIP) system:

- Meet with you to identify the exact details of the VoIP systems in scope and agree upon a detailed Rules of Engagement (ROE).
- Perform reconnaissance to gather information on the target system.
- Scan the VoIP network for open ports and vulnerabilities, test for published exploits, hardware configuration review, and log review as appropriate based on system sensitivity.
- Check for vulnerabilities that are associated with common cyber-attack methods targeting VoIP systems:
  - Caller ID Spoofing – Attacks where legitimate users are impersonated to call other legitimate users on the voice network.
  - Eavesdropping – Attacks which intercept VoIP conversation data and reconstruct the audio.
  - Denial of Service – Attacks to degrade your ability to provide service to affected customers
- Return the system to its original state, removing all traces of penetration testing activities.
- Deliver reports detailing all findings and recommended remediation steps.

*IT Policy and Procedure Review*

Your current state of information security policies and procedures will be reviewed and benchmarked against the business needs, commonly accepted industry standards (e.g., NIST CSF, CIS CSC). We will use the following methodology for performing this assessment:

- **Readiness Review** – Review currently implemented information security policies, interview select managers, and provide feedback.
- **Gap Analysis** – Review and analyze policies, procedures, and documentation and benchmark against NIST standards. Provide an overview of any major concerns and outline steps to address any vulnerabilities or weaknesses.
- **Trajectory Plan** – Assist you in developing a strategy to update internal policies and procedures based on the findings of the policy review.

*Network Vulnerability Testing*

Network vulnerability testing identifies exploitable vulnerabilities and access to systems and data based on either an authenticated user or an unauthenticated (rogue) actor. This testing includes discovery of hosts within the provided IP address ranges and vulnerability assessment of live systems in scope. Test results are manually validated to remove false positives.

If sensitive data or major security holes are discovered during any phase of the vulnerability assessment, Stealth Group will raise a red flag to the Authority immediately, per the defined procedures. Stealth Group will keep detailed documentation as to exactly what data was accessed and how it was accessed to assist in remediation or compensating control activities.

Stealth Group cybersecurity specialists have extensive experience in implementing, operating, and customizing a multitude of commercial off-the-shelf (COTS) vulnerability scanning tools, such as Nessus, Qualys, OpenVAS, Network Mapper (Nmap), Syhunt, and BeyondTrust. Additionally, our custom scripting allows for unique scanning capabilities and identification of threats for custom built applications or zero-day vulnerabilities. Our processes and procedures quickly enable isolation of root cause vulnerability findings and continuous monitoring constructs compliant with annual reporting requirements.

Stealth Group will effectively perform an accurate and thorough analysis of risk, recording potential threats and vulnerabilities to the confidentiality, integrity, and availability of protected information and associated assets. Our experts perform vulnerability and threat analyses associated with known published and recently discovered vulnerabilities, research the Dark Web for intel to keep one step ahead of hackers, and subscribe to commercial and free feeds for the latest Indicators of Compromise (IoC). We monitor vulnerabilities and threats for early warning and preemptive management of operations as they are discovered in unofficial and informal reporting by trusted user groups, specialized security-related Rich Site Summary (RSS) feeds, as well as industry specific security and intel groups, national Computer Emergency Readiness Teams (CERTs), and local and federal enforcement (e.g., InfraGard).

### *Phishing Campaign*

At no additional cost to you, Stealth Group will conduct targeted social engineering tests aimed at your employees, providing you with valuable insight into employee awareness. We do not purely focus on technology; as we assess across the dimensions of people, processes, and technology, we find that the human factor brings the highest risk – people are your first line of defense and often your weakest link, so we are sure to treat this aspect as a priority.

The objective is to identify whether any unauthorized actor could obtain access to any assets or data using various social engineering techniques. We use open-source intelligence tools to gather potential user accounts to use in the social engineering attack. Using a sample of user accounts from the total population of Authority accounts, Stealth Group engages in various electronic access infiltration campaigns against your employees.

**Phishing**: The user accounts within the sample are sent an email message designed with a realistic pretext to solicit information from the user or entice the user into visiting our websites. The pretexts for scenarios are crafted based on extensive research of open-source intelligence - information that any external malicious actor could obtain. In this way, it closely mirrors the way an attacker would target your environment. This allows you to track user responses and adjust security procedures accordingly.

We track the percentage of employees who clicked on the planted link, which provides insight into the effectiveness of existing procedural controls. To validate the information, we may use the obtained information via remote access tool to determine the risk of the phishing susceptibility by attempting to escalate privileges and move laterally within the environment.

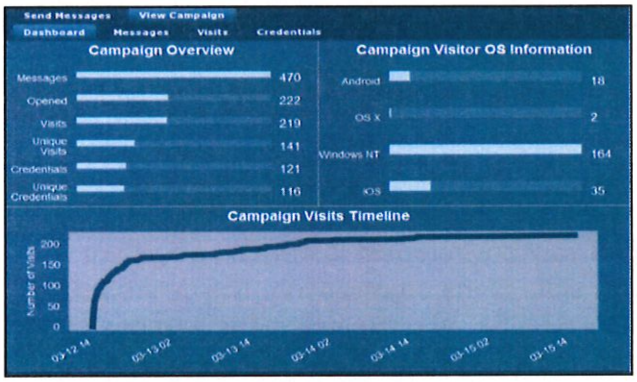


**Exhibit 2: Sample Social Engineering Report – Phishing Campaign**

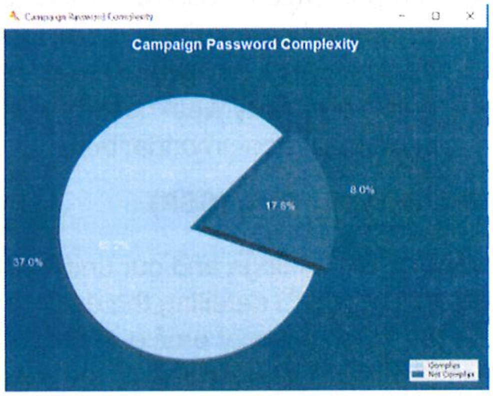


**Exhibit 3: Sample Password Complexity Chart – Phishing Campaign**

**Vishing**: Stealth Group will call a sampling of ten (10) Authority users using a pretext tailored to solicit sensitive information from the users. This could include attempting to obtain the following:

- Sensitive information regarding the users' systems (e.g., IP address)
- Information regarding your technologies or processes
- Account credentials

### *Managed Security as a Service Recommendation*

After the assessment is complete, you can test the continued effectiveness of your security controls by utilizing Stealth Group's optional Simulated Penetration Testing Service. With our SaaS-based breach and attack simulation (BAS) platform, organizations benefit from the best of all worlds:

- Industry-recognized threat modelling using the blocks of the MITRE ATT&CK™ framework.
- Simulations of the very latest techniques utilized by current cyber-threats, updated daily.
- Full attack-kill chain coverage, emulating the logical flow of events of a multi-vector Advanced Persistent Threat (APT).
- Simple wizard-based templates for customizing attack simulations to your needs.
- Automation of ATT&CK-based simulations, so you can run them daily, weekly, or whenever you need them.
- Remediation and mitigation guidelines mapped to ATT&CK for additional context.

### Reporting

Once the Cybersecurity Risk and Vulnerability Assessment is complete, Stealth Group will provide detailed reports to the Authority as a result of analysis and assessment including but not limited to the following:

- An executive summary with objectives, scope, background, summary of findings, and recommendations.
- A report which cross-references the NIST Cybersecurity Framework to describe your current cybersecurity posture, identify and prioritize opportunities for improvement within the context of a continuous and repeatable process.
- A list of security weaknesses in the form of findings, ranking of risk severity, and a list of prioritized recommendations.

### System Security Plan (SSP)

We will use the findings and our understanding of your environment to develop a System Security Plan (SSP) detailing the desired security state of the organization. The desired state will be based on a target profile aligned with the NIST CSF, at a minimum. The purpose of the SSP is to provide an overview of the security requirements of the enterprise 'system'. An SSP is not a single document. It is a collection of documents that tells the story of the security requirements of the system and describes the controls in place or planned, responsibilities, and expected behavior of all individuals who access the system including administrators. The SSP serves as a repository of documentation of the structured process of planning adequate, cost-effective security protection for the system. It reflects input from various managers with responsibilities concerning the system, including information owners, the system operators, and your system security manager.

### Gap Analysis and Plan of Action and Milestones (POA&M)

We will create a gap analysis using the SSP as the desired state and the results of our assessments as the current state. We will then help the Authority develop a prioritized action plan (POA&M) to address the gaps that includes the following:

- Weaknesses in deployed security controls and source of the identified weakness
- Severity of the identified security control weaknesses or deficiencies
- Scope or affected assets of the weakness in components within the environment
- Proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security control implementations

### Target Operating Model

Stealth Group will assist the Authority in determining a Target Operating Model (TOM). A TOM approaches IT and security from a people, process, and technology standpoint to ascertain the required structure of those three pillars to support your future security objectives.

Using your results from the assessment and gap analysis will enable us to work with you and challenge your thinking around crucially important strategic questions such as:

- People
  - What is the functional definition of each IT security team?
  - Are the right people with the right skills in place?
  - What is the current resourcing efficiency and which roles will need to be filled first was the Authority grows?
  - Is there an emphasis on cybersecurity as a culture and not just a checklist?
- Process
  - Are best practices and policies being followed?
  - Is there an established level of standardization for every tenant?
- Technology
  - Are there tools which are not being fully utilized or could be replaced?
  - Will the tools in place still be the best choice as the Authority grows?

With these strategic questions in mind, Stealth Group will assist you to determine the success criteria in achieving TOM and a Plan of Action & Milestones (POA&M).

The purpose of taking this approach is that it provides not just the information you need to be informed about your security posture, but also a business context and justification for making improvements to individual security controls. It provides a means of determining which aspects of your security need addressing more urgently than others. Our hypothesis is that without having this structure in place you may be placing undue emphasis on certain aspects of security which may not give you the best return on your investment. Security is all about identifying and managing risk and applying finite budgets in the most effective and efficient manner – rather than having a very long list of action items that may or may not do anything to manage the overall risk to your business.

## Item 2 – Hardware and Software Requirements

Stealth Group will provide and use our own tools or third-party software to conduct this assessment.

## Item 3 – Timeframe for Deliverables

**Period of Performance:** Fifteen (15) continuous business days for comprehensive IT Cybersecurity Risk and Vulnerability Assessment, with final report delivered within two (2) weeks following completion of testing.

Below is an estimated project timeline. The project timeline may change depending on the Authority's and Stealth Group's availability.

| **Task** | **Duration** |
|---|---|
| Kickoff meeting and project commencement | 2-3 hours |
| Project Management Deliverables<br>a. Work Breakdown Scheduled (WBS) including tasks<br>b. Schedule and dependencies<br>c. Weekly Status Reports including risks and progress reports | Within one week of kickoff meeting |
| Projected Solutions and Costs<br>a. Estimated range to implement solutions<br>b. All-inclusive rate sheet for each component<br>c. Annual pricing for subscription-based services | Within one week of kickoff meeting |
| Cyber Risk Assessment | 3 weeks |
| TOM (in parallel) | 1 week |
| Data analysis, prioritization, draft report<br>a. Executive Summary including comparative scorecard<br>b. Results of vulnerability testing performed<br>c. Identified cybersecurity vulnerabilities, gaps, and mitigation plans<br>d. Prioritized roadmap of activities to enhance the Authority's cybersecurity position | 1 week |
| Executive report delivery/meeting | ½ day |
| **Total Duration (Not to Exceed)** | **6 weeks** |

Exhibit 4: Estimated Project Timeline

## Item 4 – Price Structure

Stealth Group has been providing performance-based Cybersecurity and Information Assurance services to commercial clients since 2002. Our Federal GSA Schedule 70 Contract includes all cyber Highly Adaptive Cybersecurity Services (HACS) Special Item Numbers (SINs). We offer an experienced management team and cyber assessment and engineering subject matter experts. This price submission includes all elements of cost and other information as appropriate. It includes a complete and detailed price breakdown.

**Pricing Methodology**

Stealth Group's pricing approach is heavily weighted in cost realism. This is a result of our ability to control internal costs, indirect rate pools, and through our past experience, salary research, and active, national recruiting.

To calculate pricing for this project, we first identified which direct labor categories would be best suited for the project. As a GSA Schedule 70 Contractor, we used our existing pricelist and offered the Authority discounts on those rates between 15 and 25 percent, with respect to the scope of work. We have provided to you the Fixed Price for the Engagement, broken down by type of test, based on our previous experience with similarly sized organizations.

**Project Price**

This assessment will be a fixed price engagement. Stealth Group does exercise a large degree of flexibility with effort against requirements; however, change orders due to major client-driven scope revisions do happen and will be priced on a time and materials basis. A complete price breakdown is as follows:

| Labor Category | GSA Hourly Rate | Discount Rate % | Discounted Hourly Rate | Total Hours | Final Discount Price |
|---|---|---|---|---|---|
| **Risk and Vulnerability Assessment with Penetration Testing** | | | | | |
| Project Manager | $143.75 | 20% | $115.00 | 10 | $ 1,150.00 |
| Senior Assessor / Security | $205.36 | 15% | $174.56 | 120 | 20,946.72 |
| Senior Assessor / Network | $179.69 | 20% | $143.75 | 120 | $ 17,250.24 |
| **Risk and Vulnerability Assessment with Penetration Testing Subtotal** | | | | | **$ 39,346.96** |
| **Findings Review and Report** | | | | | |
| Project Manager | $143.75 | 20% | $115.00 | 10 | $ 1,150.00 |
| Senior Assessor / Security | $205.36 | 15% | $174.56 | 40 | $ 6,109.46 |
| IT Technical Writer | $150.94 | 25% | $113.21 | 40 | $ 4,528.20 |
| **Findings Review and Report Subtotal** | | | | | **$ 11,787.66** |
| **Target Operating Model** | | | | | |
| Operating Model Consultant | $246.43 | 20% | $197.14 | 40 | $ 7,885.76 |
| IT Technical Writer | $150.94 | 25% | $113.21 | 8 | $ 905.64 |
| **Target Operating Model Subtotal** | | | | | **$ 8,791.40** |
| **Project Subtotal** | | | | | **$ 59,926.02** |

| Travel and Other Direct Costs – 1 Week On-Site* | | |
|---|---|---|
| Estimated Cost – Flight & Transportation | $ | 900.00 |
| Estimated Cost – Accommodation | $ | 800.00 |
| Estimated Cost – Per diem/meals | $ | 400.00 |
| Travel Costs Not to Exceed Total | $ | 4,000.00 |
| **TOTAL PROJECT PRICE** | **$** | **62,026.02** |

* Travel assumes one (1) person for five (5) days Monday – Friday (travel Sunday – Saturday)

Exhibit 5: Project Pricing Breakdown

### Itemized Travel and Out-of-Pocket Expenses

Using the GSA Travel Rates for Buffalo, New York, we have calculated the estimated direct costs for an on-site engagement. The travel expenses outlined above are reimbursable with a not to exceed (NTE) amount.

### Project Assumptions and Dependencies

*Assumptions*

In order to produce this proposal and deliver the work as proposed we have made the following assumptions. If any of these assumptions turns out to be incorrect then this may impact the overall project timeline and cost and may be subject to contract change control. We have assumed that:

- You have up to date and accurate information and diagrams related to the existing IT infrastructure and that these can be provided to us at the start of the project.
- We will be able to undertake work on this project from our Stealth Group offices in North America where appropriate and provided that we satisfy any information security requirements you may have for safeguarding confidential data whilst not on your premises.
- We will be using tools or third-party software (e.g., vulnerability scanners, network discovery) that needs to be deployed in your IT environment in non-intrusive mode (we will request VPN access to your network or ask your IT administrator and key personnel to execute non-intrusive scripts on selected machines).

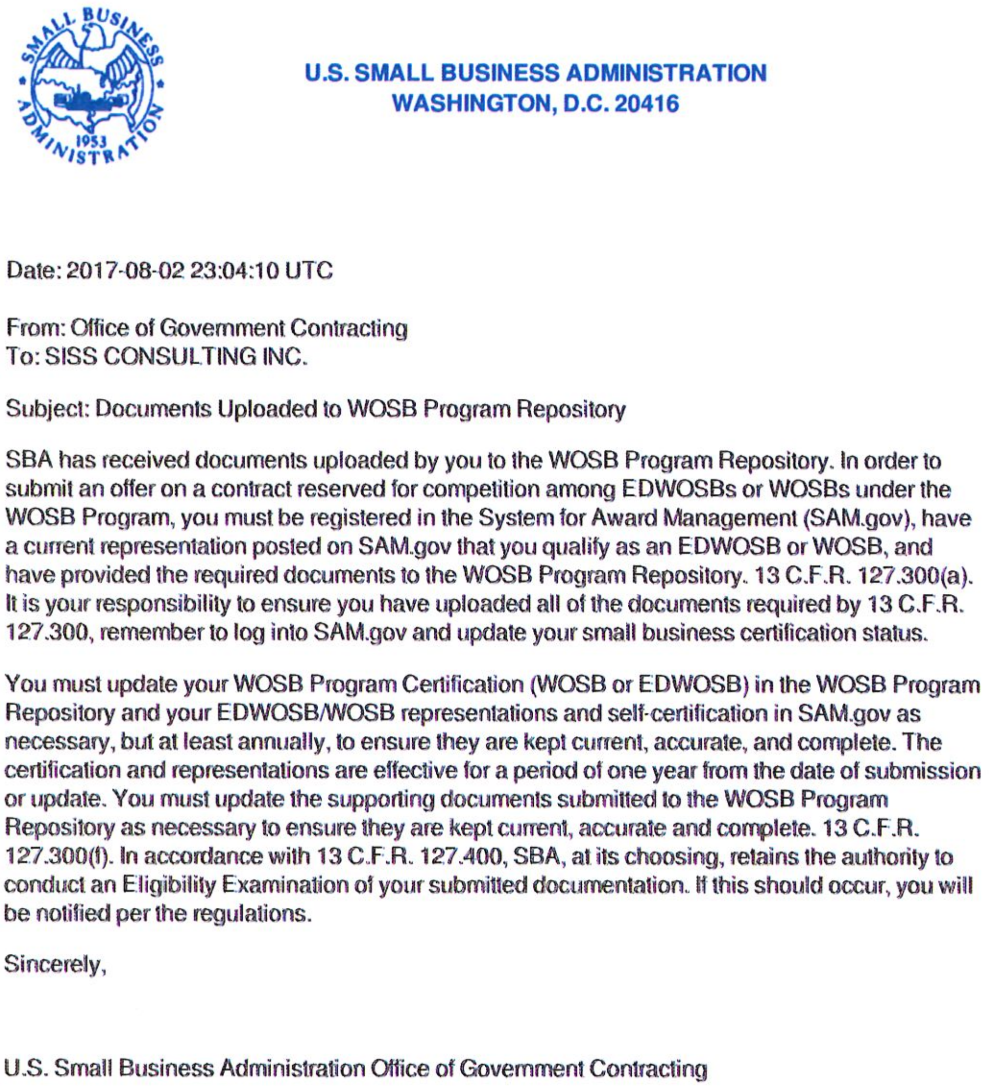
*Dependencies*

In order to deliver this work according to our proposal then we will need you to:

- Identify and appoint a senior executive to act as Project Sponsor. This person will chair the kickoff and provide strategic input and context into the project, and direct the Authority's staff to collaborate as much as possible during this project
- Identify and appoint a Project Manager within the Authority's organization for this project and someone who can act as our primary point of contact for the project. We will need this person to:
    - Manage communications with other internal stakeholders.

- Facilitate any discussions required with third parties (e.g., IT Service providers).
- Be available for regular engagement updates and reviews as required.
- Please note – delays caused by not having a local project manager may incur delay of project delivery and potentially extra cost

# APPENDIX A: WOSB PROGRAM LETTER



**U.S. SMALL BUSINESS ADMINISTRATION**
**WASHINGTON, D.C. 20416**

Date: 2017-08-02 23:04:10 UTC

From: Office of Government Contracting
To: SISS CONSULTING INC.

Subject: Documents Uploaded to WOSB Program Repository

SBA has received documents uploaded by you to the WOSB Program Repository. In order to submit an offer on a contract reserved for competition among EDWOSBs or WOSBs under the WOSB Program, you must be registered in the System for Award Management (SAM.gov), have a current representation posted on SAM.gov that you qualify as an EDWOSB or WOSB, and have provided the required documents to the WOSB Program Repository. 13 C.F.R. 127.300(a). It is your responsibility to ensure you have uploaded all of the documents required by 13 C.F.R. 127.300, remember to log into SAM.gov and update your small business certification status.

You must update your WOSB Program Certification (WOSB or EDWOSB) in the WOSB Program Repository and your EDWOSB/WOSB representations and self-certification in SAM.gov as necessary, but at least annually, to ensure they are kept current, accurate, and complete. The certification and representations are effective for a period of one year from the date of submission or update. You must update the supporting documents submitted to the WOSB Program Repository as necessary to ensure they are kept current, accurate and complete. 13 C.F.R. 127.300(f). In accordance with 13 C.F.R. 127.400, SBA, at its choosing, retains the authority to conduct an Eligibility Examination of your submitted documentation. If this should occur, you will be notified per the regulations.

Sincerely,

U.S. Small Business Administration Office of Government Contracting

# APPENDIX B: RESUMES

We have provided abbreviated resumes below. If the proposed staff member is unavailable at the time of the project start, staff with equal or better experience, qualifications, and certifications will be selected for the Authority's review.

| Misty R. | Project Manager |
|---|---|
| **Experience:** 12+ years in contracts & compliance<br>6+ years in program & project management | **Education:** B.S. Business Management, Southwest Technical College, 1993<br>B.S. Project Management, Rockford University |
| **Certifications:**<br>• Project Management Professional (PMP)<br>• National Contract Management Association (NCMA)<br>o Certified Commercial Contracts Manager (CCCM)<br>o Certified Federal Government Contracts Manager (CFCM) | **Professional Memberships:**<br>• Coalition for Government Procurement<br>o Small Business Committee<br>o General Products Committee<br>o E-Commerce Committee<br>• GSA Industrial Products & Services Supplier Research Panel<br><br>**Clearance:** DoD Top Secret (inactive) |

## General Qualifications to Meet Requirements

Service Delivery: Responsible for the overall direction, coordination, implementation, execution, control and completion of specific projects ensuring consistency with company strategy, commitments and goals. Manage multiple priorities within expected timelines while effectively meeting client expectations for quality.

- Knowledge of both theoretical and practical aspects of project management
- Knowledge of project management techniques and tools
- Direct work experience in project management capacity
- Proven experience in people management, strategic planning, risk management, change management
- Proficient in project management software

## Relevant Experience and Positions Held

| | |
|---|---|
| **Stealth-ISS Group, Inc. – VICE PRESIDENT OF FEDERAL BUSINESS AND SERVICE DELIVERY** | **06/2020 – Present** |
| | |
| **STEALTH-ISS GROUP PROJECT MANAGER EXPERIENCE** | |
| **City of Virginia Beach – SCADA System Penetration & Vulnerability Testing** | **06/2021 – Present** |
| **DC BLOX – Cybersecurity Risk Assessment** | **06/2021 – Present** |
| **iBASEt – CMMC Pre-Assessment** | **04/2021 – Present** |

| | |
|---|---|
| **Akima – CMMC Pre-Assessment** | **04/2021 - Present** |
| **Absolute Dental – Cybersecurity and Risk Assessment** | **03/2021 – Present** |
| **PLX Inc. – CMMC Pre-Assessment and Remediation** | **01/2021 – Present** |
| **Barge Design Solutions Consulting Group, Inc. – CMMC Pre-Assessment** | **11/2020 – 01/2021** |
| **Maryland State Board of Elections – Penetration Testing** | **09/2020 – 10/2020** |
| **Applied Thin-Film Products (ATP) – CMMC Pre-Assessment** | **07/2020 – 10/2020** |
| **Town of North Kingstown, Rhode Island – Vulnerability Assessment** | **06/2020 – 12/2020** |
| **Epoch Concepts LLC – CMMC Pre-Assessment** | **05/2020 – 07/2020** |
| **ADDITIONAL EXPERIENCE** | |
| **Continental Mapping Consultants – DIRECTOR OF FEDERAL BUSINESS** | **02/2020 – 06/2020** |
| Responsible for federal business development & proposal team, post award contracts & compliance and the federal service delivery team for JANIS, USACE FEMA BlueRoof, GSA IT 70, and various protected clients. Security Clearance obtained – currently inactive | |
| **SupplyCore – DIRECTOR OF OPERATIONS** | **4/2017 – 2/2020** |
| Responsible for federal business development & proposal team, post award contracts & compliance and the federal service delivery team for DLA-MRO - 9 Global Contracts, GSA MAS which include 51V, 23, 84, INDOPACOM, MRO BPA & FSSI BPA), Israel Weapon Systems contract. | |

| Dasha D. | Senior Assessor/Security |
|---|---|
| **Experience:** 25+ years of IT and IT Security, U.S. Navy Veteran | **Education:** MS (Summa Cum Laude) IT Project Management/IT Security, MBA Advanced Business Management, BA International Relations & Foreign Affairs |
| **Certifications:**<br>• Certified Information System Security Professional (CISSP)<br>• Certified in Risk and Information Systems Control (CRISC)<br>• Certified in the Governance of Enterprise IT (CGEIT)<br>• Project Management Professional (PMP)<br>• Disaster Recovery & Business Continuity, Cyber Security, Lean Six Sigma, ITIL<br>• National Security Agency – NSA IAM/ IEM (Information Assessment/Evaluation Methodologies)<br>• Certified Chief Information Security Officer (C\|CISO)<br>• Payment Card Industry Qualified Security Assessor (PCI QSA)<br>• Payment Card Industry Professional (PCIP)<br>• Health Care Security Professional (HCISSP)<br>• FEMA/CERT – Incident Command Systems<br>• National Incident Management System, Risk Assessments<br>• Certified Confidentiality Officer/Business Espionage (CCO)<br>• Trained by CMMC-AB as a CMMC Provisional Assessor | **Professional Memberships:**<br>• Institute of Electrical and Electronics Engineers (IEEE)<br>• International Information System Security Certification Consortium (ISC)$^2$<br>• Information Systems Audit and Control Association (ISACA)<br>• FBI – InfraGard<br>• PMI (Project Management Institute)<br>• WikiStrat – Sr. Analyst (Cybersecurity)<br>• Civil Air Patrol – 2nd Lieutenant<br>• FBI – CyberDefense Response Team<br>**Achievements:**<br>U.S. Navy 2006-2008 – Achievement Medal for successful management of Aviation Department with $45M budget (deployment operations, logistics, inventory) |

## General Qualifications to Meet Requirements

Accomplished cybersecurity professional with over 25 years' experience in the IT sector. Has successfully completed assessments and gap analysis in both the Federal and Commercial sectors, and closely involved with risk identification and mitigation procedures. Thorough knowledge of NIST CSF, PCI DSS, ISO 27K, and HIPAA. Regularly develops Policies and Procedures for clients. Closely involved with risk identification and mitigation procedures.

## Relevant Experience and Positions Held

| Stealth-ISS Group Inc., CO-FOUNDER AND PRESIDENT | 10/2002 – Present |
|---|---|

- Serves Fortune 1000 clients worldwide
- Manages consultants and maintains pool of 30 Cybersecurity Subject Matter Experts

| | |
|---|---|
| • Business development<br>• Execution of various consulting engagements and projects | |
| **Stealth-ISS Group, Inc. - Barge Design Solutions Consulting Group, Inc.** | **11/2020 – 01/2021** |
| • Conducted a detailed gap analysis to help meet CMMC Level 3<br>• Delivered a list of remediation recommendations and updates to POA&M | |
| **Stealth-ISS Group, Inc. – Applied Thin Film Products (ATP)** | **07/2020 – 10/2020** |
| • Conducted a CMMC Gap Analysis<br>• Created a system security plan in accordance with CMMC guidelines<br>• Supported CMMC gap remediation | |
| **Stealth-ISS Group, Inc. – Town of North Kingstown** | **06/2020 – 12/2020** |
| • Performed full Information Systems Security Risk Assessment Audit<br>• Conducted a gap analysis based on NIST CSF maturity goal of Level 3<br>• Developed prioritized remediation recommendations | |
| **Stealth-ISS Group, Inc. – Epoch Concepts, LLC** | **05/2020 – 07/2020** |
| • Conducted a gap analysis based on NIST SP 800-1710 and the draft version of CMMC<br>• Developed prioritized remediation recommendations | |
| **Stealth-ISS Group, Inc. – U.S. Department of Transportation** | **09/2019 – 12/2019** |
| • Supported Security Assessment & Authorization for FIPS-199 system<br>• Validated NIST SP 800-53 security controls<br>• Developed Security Assessment Plan (SAP) and Plan of Actions & Milestones (POA&M) | |
| **Stealth-ISS Group, Inc., Atos SE - PyeongChang 2018 Olympic Games, 2016 Rio Olympics Games, Security Design, SR. SECURITY CONSULTANT – SPECIAL PROJECTS (CONTRACT)** | **01/2017 – 03/2018** |
| • Project 1: Set up and design of new Security Operations Center for PyeongChang 2018 Olympic Games for Olympic Broadcast Services (OBS) and Olympic Channel including selection of team members, technology, staff and client training, standard operation procedures creation, table-top exercises including 24/7 monitoring operations.<br>• Project 2: Acted as Single Point of Contact and Manager for all Security Escalations and Security Incidents during the 2016 Rio Olympics Games for Olympic Broadcast Services and Olympic Channel.<br>• Project 3: In charge of $12Million security design and implementation for global client and their 50+ commercial and government agencies starting with gap analysis, recommendations, and execution. Managed team of 27 and acted as PCI DSS QSA. Design for Security Operations Plan meeting PCI requirements | |

| Inno E. | Senior Assessor/Network |
|---|---|
| **Experience:** 20+ years of experience with risk management, computer forensics, incident response, data breach investigation, threat hunting, malware analysis, penetration testing, and security operations solutions | **Education:**<br>• M.S., Computer Science, The George Washington University, Washington, DC, May 1995<br>• B.S., Computer Science, Morgan State University, Baltimore, MD, May 1993<br>• B.S., Mathematics, Morgan State University, Baltimore, MD, May 1993<br>o Graduated cum laude<br>o Elected to Beta Kappa Chi Honor Society |
| **Certifications:**<br>• Certified Information Systems Security Professional (CISSP) – # 36690<br>• Certified Information Security Manager (CISM) – # 0405349<br>• Certified Information Systems Auditor (CISA) – # 0647986<br>• Information Systems Security Architecture Professional (ISSAP) – # 36690<br>• Information Systems Security Management Professional (ISSMP) – # 36690<br>• Computer Hacking Forensic Investigator (CHFI) – # ECC922471<br>• Check Point Certified Security Expert (CCSE)<br>• Check Point Certified Security Administrator (CCSA) | **Security Clearance:**<br>• Active DoD Top Secret Clearance<br>**Professional Memberships:**<br>• FBI InfraGard<br>• Institute of Computer Forensic Professionals (ICFP)<br>• International Information Systems Security Certifications Consortium (ISC)$^2$<br>• Information Systems Security Association (ISSA)<br>• Information Auditing and Control Association (ISACA) |

### General Qualifications to Meet Requirements

20+ years of hands-on experience in delivering world-class results and solving real-world cyber security, digital forensics, and incident response challenges. Lead cyber security, incident response, and digital forensics investigations for private and public-sector clients and law firms. Perform complex Risk Management Framework (RMF) Assessment & Authorization (A&A) – formerly Certification and Accreditation (C&A) activities

### Relevant Experience and Positions Held

| | |
|---|---|
| **Stealth-ISS Group Inc. – PENETRATION TESTER (CONSULTANT)** | **08/2020 – Present** |
| **Maryland State Board of Elections** | **09/2020 – 10/2020** |

- Perform hands-on vulnerability assessments and penetration testing against network infrastructure technologies, including firewalls, IDS/IPS, routers, network servers, VPN gateways, database servers, web-based applications, mainframe, VoIP devices, wireless networks, and mobile devices.
- Identify vulnerabilities and execute appropriate exploits to compromise target systems, including server penetration, buffer overflows, privilege escalation, password cracking, and social engineering.
- Execute OWASP Top 10 vulnerabilities (such as: Injection, Cross Site Scripting, Broken Authentication and Session Management, Security Misconfiguration, etc.) against web applications.

## ADDITIONAL EXPERIENCE

| **NetSecurity Corporation – PRINCIPAL SECURITY/FORENSICS CONSULTANT** | **10/2003 – Present** |
|---|---|

*Penetration Testing:*

- Perform hands-on vulnerability assessments and penetration testing against network infrastructure technologies, including firewalls, IDS/IPS, routers, network servers, VPN gateways, database servers, web-based applications, mainframe, VoIP devices, wireless networks, and mobile devices.
- Identify vulnerabilities and execute appropriate exploits to compromise target systems, including server penetration, buffer overflows, privilege escalation, password cracking, and social engineering.
- Conduct WEP, WPA and WPA-2, man-in-the-middle, access point impersonation, and back-end database exploitation attacks.
- Execute OWASP Top 10 vulnerabilities (such as: Injection, Cross Site Scripting, Broken Authentication and Session Management, Security Misconfiguration, etc.) against web applications.
- Leverage IDS/IPS evasion attacks against target systems.
- Test the vulnerability of emerging mobile devices.
- Work with clients to implement remediation mechanisms to protect valuable assets proactively.
- Execute advanced (spear) phishing attacks as part of social engineering tests against users to simulate susceptibility to advanced cyber threats.

*Regulatory Compliance:*

- Assist customers to comply with ISO 27001, PCI, HIPAA, FISMA, FedRAMP, DFARS, GLBA, SOX, OMB, NIST, and DoD Directives.
- Lead Risk Management Framework (RMF) and Assessment and Authorization (A&A) efforts for various agencies such as Internal Revenue Service (IRS), Department of Treasury, Department of Labor, Defense Health Agency, Department of Veterans Affairs, and U.S. Air Force.

- Provide regulatory compliance support, including FISMA, DFARS, FedRAMP, PCI, SOX, GLBA, and HIPAA.
- Perform risk assessments, business impact assessments, business continuity planning, and disaster recovery plans for Federal and commercial clients.
- Perform and lead risk assessments.
- Perform Security A&A activities in accordance with NIST SP 800-37 and NIST SP 800-171.
- Serve various leadership roles, including documentation lead, team lead, quality control lead, and team manager for several Major Applications (MA) and General Support Systems (GSS) A&A efforts.
- Develop A&A documentation, including: System Security Plan (SSP), Information Technology Contingency Plan (ITCP), Incident Response Plan (IRP), CMP, Privacy Impact Assessment, e-Authentication Risk Assessment, Security Testing and Evaluation (ST&E) Plan, and Security Assessment Report (SAR).
- Conduct Security Categorization in accordance with FIPS 199 Standard.
- Execute ST&E, including conducting vulnerability and penetration testing against systems and applications undergoing A&A.
- Assess security controls based upon NIST SP 800-53A.
- Develop POA&M for applications and GSS.
- Assemble A&A packages for ATO.
- Execute validation and security test procedures based upon DoD, FISMA, NIST, and agencies' guidelines.
- Conduct manual systems review and testing, including executing Security Readiness Review (SRR) scripts, Gold Disks, AppDetective, Retina, and DISA STIGs.
- Work with system administrators to remediate findings and lock down infrastructure devices
- In further supporting A&A activities, assemble Security Authorization Package (SSP, SAR, and POA&M) and submit for Authorization to Operate (ATO) decision.
- Develop a Residual Risk Statement/Report that is included in the Risk Acceptance Recommendation Report.

*Security Engineering & Operations*
*Incident Response & Forensics Investigation*
*Hands-On How-To® Training*

| Daniel C. | IT Technical Writer |
|---|---|
| **Experience:** 11+ years of experience in technical writing, including data security, regulatory compliance, and security architecture. | **Education:** B.S. Psychology and English Literature, University of Pittsburgh, PA |

## General Qualifications to Meet Requirements

Experienced technical writer specializing in cybersecurity. Thorough knowledge of multiple cybersecurity frameworks, including NIST, CMMC, HITRUST, PCI, and HIPAA. Develops innovative tools to quantify risk and security control maturity.

## Relevant Experience and Positions Held

| **Stealth-ISS Group, Inc. – Technical Writer** | **04/2021 - Present** |
|---|---|

- Serves as a technical and proposal writer focused on cybersecurity engagements, including those for CMMC and NIST.
- Communicates technical information in reports tailored to the specific audience, including executive summaries, dashboarding, technical documentation, and presentations.

### STEALTH-ISS GROUP TECHNICAL WRITER EXPERIENCE

| | |
|---|---|
| **iBASEt – CMMC Pre-Assessment** | **04/2021 – Present** |
| **Akima – CMMC Pre-Assessment** | **04/2021 – Present** |
| **Absolute Dental – Cybersecurity and Risk Assessment** | **04/2021 – Present** |
| **PLX Inc. – CMMC Pre-Assessment and Remediation** | **04/2021 – Present** |

- Document findings and recommendations in reports that are technically accurate while easily understood by leadership
- Develop dashboards and graphics to visually convey the results of the assessments
- Ensure reports are internally consistent and that themes present across tests, findings, and domains are conveyed to support strategic remediation efforts

### ADDITIONAL EXPERIENCE

| **RSM US LLP (Formerly SecureState) – Technical Writer Supervisor** | **10/2014 – 04/2021** |
|---|---|

- Supervised a team of six technical writers focused on developing technical reports, proposals, and marketing material on cybersecurity topics.
- Served as one of the company's first technical writers and helped develop the role and technical writing program.
- Developed Written Information Security Programs for clients in the healthcare, technology, and local government industries. This included:
  - Gap assessments against applicable frameworks (e.g., CMMC, NIST frameworks, HITRUST, PCI, HIPAA, GDPR, CCPA)

  - Creation and management of a risk register
  - Presentations of findings to the client's leadership
  - Development of information security governance and risk management structures
- Conducted approximately 30 risk assessments, security control maturity assessments, compliance gap assessments, and remediation roadmap development for external clients
- Wrote approximately 500 reports to communicate the business risks of technical vulnerabilities and security control gaps, including reports for:
  - Penetration testing
  - Network architecture reviews
  - Risk assessments
  - Security control maturity assessments
  - Compliance gap assessments
  - Incident response

**Halfaker & Associates, LLC – Proposal Manager** **07/2012 – 05/2014**

- Managed technical proposal responses covering digital services, data analytics, cyber security, and cloud solution offerings
- Wrote secure software development lifecycle plans
- Developed project schedules and supported technical documentation efforts

**MicroTech, LLC – Proposal Manager / Lead VTC Facilitator** **06/2009 – 07/2012**

- Served as a writer and manager for IT proposal responses to Federal Government solicitations
- As Lead VTC Facilitator, served as the first point-of-escalation for video teleconferencing issues at the Missile Defense Agency, including daily support for a 3-Star General, Admirals, and other Department of Defense executives

| Robert D. | Operating Model Consultant |
|---|---|
| **Experience:** 25+ years in business strategy and development within IT security and infrastructure sectors | **Education:** Master of Business Administration (MBA), Open University Milton Keynes and Cambridge, 2005 |
| **Certifications**:<br>• PRINCE2 Practitioner<br>• ITIL Best Practice Methods and Frameworks<br>• Project Lifecycle Management<br><br>**Awards:**<br>• Global CEO Excellence Awards – IT Solutions CEO of the Year for South East USA 2020<br>• Global CEO Excellence Awards – IT Solutions CEO of the Year for South East USA 2019 | **Professional Memberships:**<br>• Information Systems Security Association (ISSA)<br>• ISACA<br>• Las Vegas Chamber of Commerce<br>• Vistage, CEO Group<br>• Chartered Managers Institute (MCMI) |

## General Qualifications to Meet Requirements

**An MBA-qualified CEO / Chief Information Officer / CISO** with a successful background within B2B, B2C, professional, financial, investment banking, insurance, leisure/gaming, construction, commercial & corporate sectors. Commercially-aware having founded and built an IT and cyber security consulting company to multi-million $ revenues, and with a broad range of IT experience having worked at the most senior levels for world-class organizations including 14 years at Deutsche Bank.

**Strategic approach to successful IT leadership**, engaging with key business stakeholders and 3rd parties to align technology roadmap with business strategy, delivering cost appropriate holistic IT solutions and business process change via best of breed and emerging technology solutions.

**PRINCE2 & ITIL accredited**, with strong experience of applying best practice frameworks and methods.

**Experience of driving change management**, business transformation, IT service transition, IT strategies, technology roadmaps, Service Orientated Architecture, PMO, vendor & client relationships, project delivery, IT Security, datacenters & DR, IT upgrades and systems migration, delivering optimized business benefit via the use of new technology globally.

**Exemplary leadership skills**, trusted vendor and business partner relationship management, a true collaborator and mentor, delivers real business results through people development.

## Relevant Experience and Positions Held

| **Stealth-ISS Group Inc. – CHIEF EXECUTIVE OFFICER** | **08/2016 – Present** |
|---|---|

- Instrumental in leading and growing innovative cybersecurity company

| | |
|---|---|
| • Promotes and steers the company culture, built on accountability and trust to deliver high quality solutions to our customers<br>• Led the company to 167th on the Inc. 5000 fastest growing companies list in 2018 and 387th in 2019<br>• Under leadership, company placed on VET50 list of fastest growing veteran-owned companies in both 2019 and 2020<br>• Relocated to US to focus on business development | |
| **Global-DTC – FOUNDER, CHIEF EXECUTIVE OFFICER** | **12/2014 – Present** |
| • Founded the company in the UK to offer general IT and specific Cyber Security consulting services<br>• Landed NATO BOA Agreement, and various Financial Institutional clients including HSBC<br>• **Delivered a Target Operating Model for HSBC IT Security Organization**<br>• Landed Global MSSP contract for project delivery, consultants, then some permanent recruitment<br>• Partnered with over 30 cyber companies to expand the DTC value proposition<br>• Trebled revenues year on year | |

# Thank you!

STEALTH

ISS GROUP

Get Sharp. Get Serious. Get Safe.

*Proposal for Consulting Services*

*for*

# ***Cybersecurity Risk & Vulnerability Assessment***

June 10, 2021

**Prepared for:**
Erie County Water Authority

**Prepared by:**
Rick Anderson, Senior Technology Consultant
Dimitrios Hilton, Executive Security Consultant

trueNORTH
consulting group

## Letter of Transmittal

140 Third Street South, Stillwater, Minnesota 55082
888.650.4580 ● 651.430.2772 ● www.tncg.com

June 10, 2021

Mr. Terrence D. McCracken, Secretary to the Authority
Erie County Water Authority
295 Main Street, Room 350
Buffalo, NY 14203

Dear Mr. McCracken:

True North Consulting Group, LLC. (True North/TNCG) is pleased to respond to the Erie County Water Authority's Request for Proposals for a Cybersecurity Risk & Vulnerability Assessment. True North fully understands and complies with the scope of work outlined in the RFP. TNCG acknowledges receipt of the Questions and Answers document.

True North has partnered with InfoSec Associates, LTD. (InfoSec) to ensure optimum success of the assessment process. True North has performed several like assessments nationally with InfoSec. True North selected InfoSec based on expertise, which is in concert with overall expertise as a unified commitment to the Erie County Water Authority.

Over the years, TNCG has performed hundreds of successful Cybersecurity Risk & Vulnerability Assessments throughout the United States. Please feel free to contact Rick Anderson for additional references if desired. Our Minnesota office will be involved from a project management perspective utilizing our full-time certified security risk and IT consultants to ensure Team TNCG meets and exceeds your expectations.

TNCG does not sell or represent any products of any type, nor are we affiliated with any vendors or manufacturers. This neutrality allows our firm to provide an objective, unbiased assessment of your needs and recommend the best available options. ***As our client, your best interest is our priority***.

We have submitted our response via email and have also mailed an original hard copy, as requested.

We look forward to hearing from you. If you have any questions, please feel free to contact Rick Anderson at (651) 705-1249 or at rick.anderson@tncg.com.

Sincerely,

Mike Indergard

Mike Indergard, Director of Strategic Planning
True North Consulting Group

## TABLE OF CONTENTS

Page

**PART 1 ... 4**

ITEM 1 – NAME OF INDIVIDUAL OR ORGANIZATION ... 4
ITEM 2 – NAME AND TITLE OF CONTACT PERSON ... 4
ITEM 3 – BUSINESS ADDRESS ... 4
ITEM 4 – TELEPHONE NUMBER ... 4
ITEM 5 – EMAIL ADDRESS ... 4
ITEM 6 – FAX NUMBER ... 4

**PART 2 ... 5**

ITEM 1 – CONSULTANT BUSINESS FORM ... 5
ITEM 2 – CONSULTANT TEAM ... 9

**PART 3 ... 20**

ITEM 1 – PROPOSED SCOPE OF SERVICE ... 20
ITEM 2 – HARDWARE AND SOFTWARE REQUIREMENTS ... 25
ITEM 3 – TIMEFRAME FOR DELIVERABLES ... 26
ITEM 4 – PRICE STRUCTURE ... 26

**PART 4 ... 34**

COMPANY BACKGROUND ... 34
CERTIFICATIONS ... 37
CUSTOMER SUPPORT ... 38
FINANCIAL CONDITION ... 39
SAMPLE REPORT ... 39

# PART 1

## Item 1 – Name of Individual or Organization

True North Consulting Group, LLC.

## Item 2 – Name and Title of Contact Person

Rick Anderson, Senior Technology Consultant

## Item 3 – Business Address

140 Third Street South, Stillwater, MN 55082

## Item 4 – Telephone Number

(888) 650-4580 (Main)

(952) 412-6843 (Rick Anderson)

## Item 5 – Email Address

rick.anderson@tncg.com

## Item 6 – Fax Number

None

## PART 2

### Item 1 – Consultant Business Form

1. Identify the Consultant's business or corporate structure:

   (a) If a corporation, including the following:

   - Date and State of Incorporation
   - List Name and Title of Executive Officers
   - Principal Place of Business
   - List all Related Principal or Subsidiaries Corporations
   - Closed or Publicly Traded
   - EIN

   (b) If a Partnership, including the following:

   - Date and State of Formation
   - Name of General Partners
   - Type of Partnership
   - Principal Place of Business
   - EIN

   (c) If a Joint Venture, including the following:

   - Date and State of Formation
   - Name, Address, and Business/Corporate Form, if any, of all Joint Venture Partners
   - Identify the Managing Partner of the Joint Venture
   - Principal Place of Business
   - EIN

   (d) If a Sole Proprietorship, including the following:

   - First date of operation
   - Principal Place of Business
   - EIN

   **(e) TNCG is a Limited Liability Company (LLC).**

   - Date and State of Formation: 2014 / Texas
   - Name of Owners: Russ Johnson – CEO, Tony Chojnowski – COO, Shane Jacobus – Vice President of Finance, and Jon Martin – Executive Director
   - Principal Place of Business: Waco, Texas
   - EIN: 46-5651592 / DUNS: 079464337

2. Identify the number of years your entity has been in business.

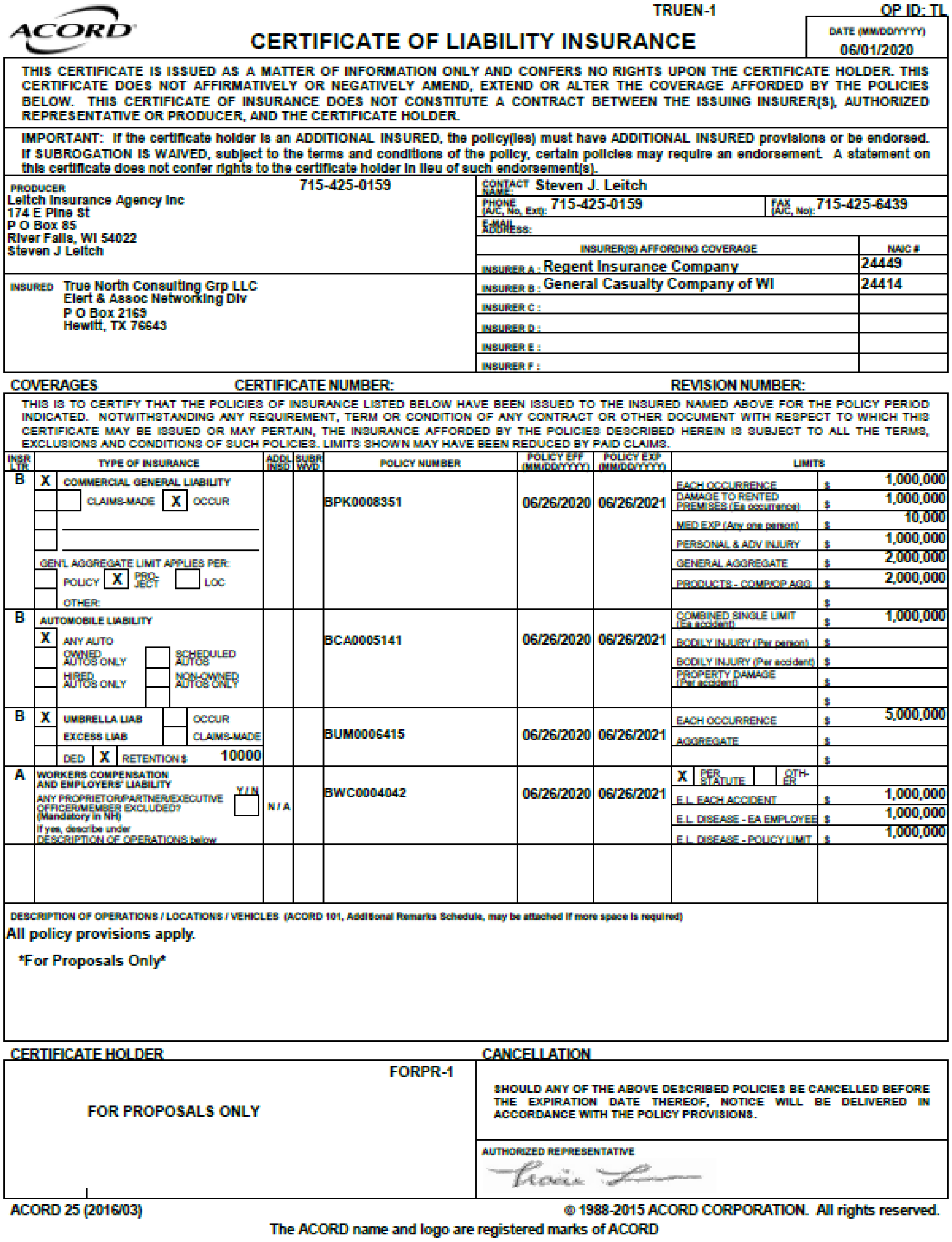
   37 years

3. Identify whether your business/corporate structure has changed in the past five years and if yes, describe the change.

   Changed to an LLC back in 2018

4. Identify the type and coverage amount of all insurance policies.

   General Liability Insurance Certificate



ACORD TRUEN-1 OP ID: TL

## CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY) 06/01/2020

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

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

PRODUCER 715-425-0159
Leitch Insurance Agency Inc
174 E Pine St
P O Box 85
River Falls, WI 54022
Steven J Leitch

CONTACT NAME: Steven J. Leitch
PHONE (A/C, No, Ext): 715-425-0159 FAX (A/C, No): 715-425-6439
E-MAIL ADDRESS:

| INSURER(S) AFFORDING COVERAGE | NAIC # |
|---|---|
| INSURER A : Regent Insurance Company | 24449 |
| INSURER B : General Casualty Company of WI | 24414 |
| INSURER C : | |
| INSURER D : | |
| INSURER E : | |
| INSURER F : | |

INSURED True North Consulting Grp LLC
Elert & Assoc Networking Div
P O Box 2169
Hewitt, TX 76643

COVERAGES CERTIFICATE NUMBER: REVISION NUMBER:

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

| INSR LTR | TYPE OF INSURANCE | ADDL INSD | SUBR WVD | POLICY NUMBER | POLICY EFF (MM/DD/YYYY) | POLICY EXP (MM/DD/YYYY) | LIMITS | |
|---|---|---|---|---|---|---|---|---|
| B | ☒ COMMERCIAL GENERAL LIABILITY<br>☐ CLAIMS-MADE ☒ OCCUR<br>☐<br>☐<br>GEN'L AGGREGATE LIMIT APPLIES PER:<br>☐ POLICY ☒ PRO-JECT ☐ LOC<br>☐ OTHER: | | | BPK0008351 | 06/26/2020 | 06/26/2021 | EACH OCCURRENCE | $ 1,000,000 |
| | | | | | | | DAMAGE TO RENTED PREMISES (Ea occurrence) | $ 1,000,000 |
| | | | | | | | MED EXP (Any one person) | $ 10,000 |
| | | | | | | | PERSONAL & ADV INJURY | $ 1,000,000 |
| | | | | | | | GENERAL AGGREGATE | $ 2,000,000 |
| | | | | | | | PRODUCTS - COMP/OP AGG | $ 2,000,000 |
| | | | | | | | | $ |
| B | AUTOMOBILE LIABILITY<br>☒ ANY AUTO<br>☐ OWNED AUTOS ONLY ☐ SCHEDULED AUTOS<br>☐ HIRED AUTOS ONLY ☐ NON-OWNED AUTOS ONLY<br>☐ ☐ | | | BCA0005141 | 06/26/2020 | 06/26/2021 | COMBINED SINGLE LIMIT (Ea accident) | $ 1,000,000 |
| | | | | | | | BODILY INJURY (Per person) | $ |
| | | | | | | | BODILY INJURY (Per accident) | $ |
| | | | | | | | PROPERTY DAMAGE (Per accident) | $ |
| | | | | | | | | $ |
| B | ☒ UMBRELLA LIAB ☐ OCCUR<br>☐ EXCESS LIAB ☐ CLAIMS-MADE<br>☐ DED ☒ RETENTION $ 10000 | | | BUM0006415 | 06/26/2020 | 06/26/2021 | EACH OCCURRENCE | $ 5,000,000 |
| | | | | | | | AGGREGATE | $ |
| | | | | | | | | $ |
| A | WORKERS COMPENSATION AND EMPLOYERS' LIABILITY<br>ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) Y / N ☐<br>If yes, describe under DESCRIPTION OF OPERATIONS below | N / A | | BWC0004042 | 06/26/2020 | 06/26/2021 | ☒ PER STATUTE ☐ OTH-ER | |
| | | | | | | | E.L. EACH ACCIDENT | $ 1,000,000 |
| | | | | | | | E.L. DISEASE - EA EMPLOYEE | $ 1,000,000 |
| | | | | | | | E.L. DISEASE - POLICY LIMIT | $ 1,000,000 |
| | | | | | | | | |

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

All policy provisions apply.

*For Proposals Only*

CERTIFICATE HOLDER

FORPR-1

FOR PROPOSALS ONLY

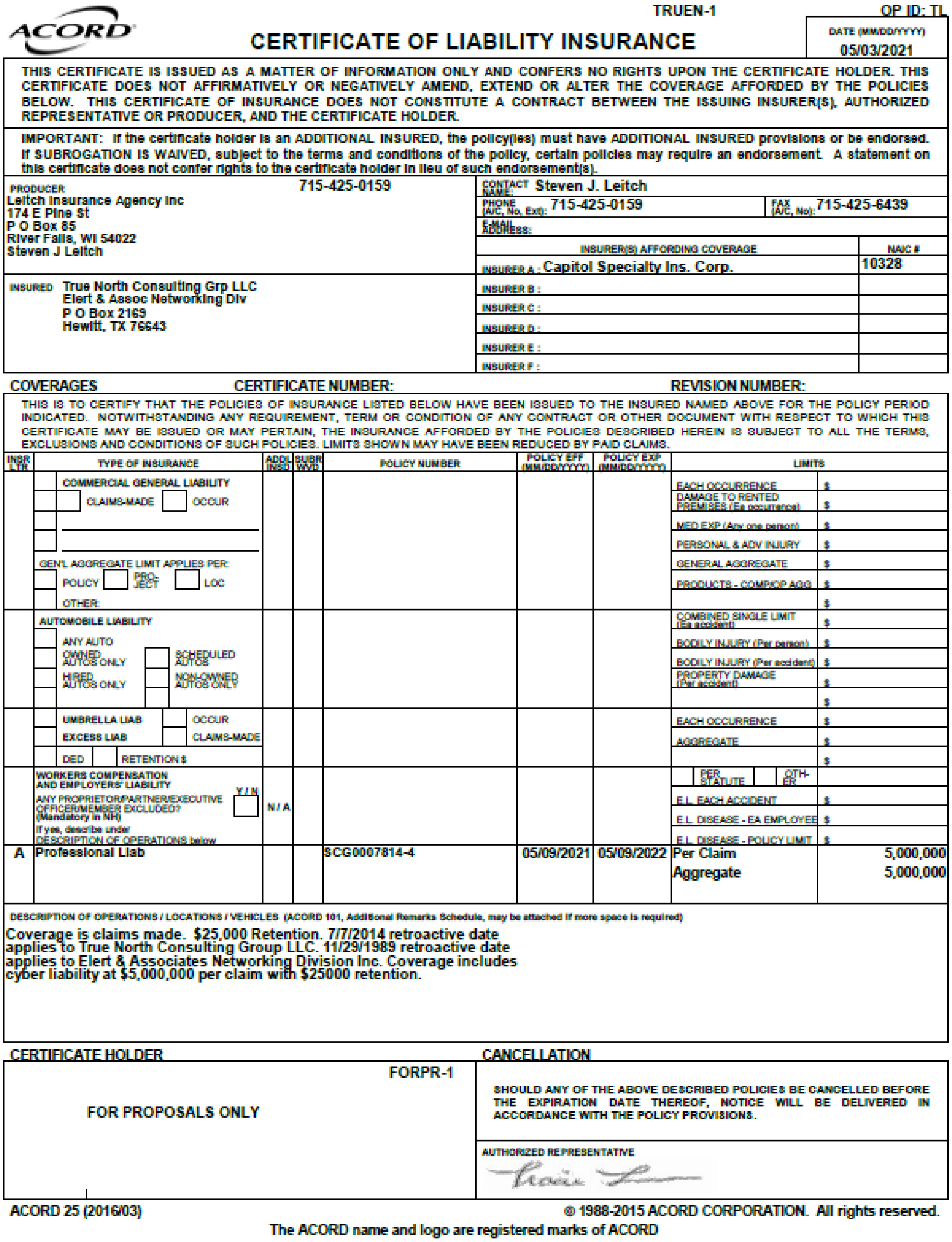
CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

ACORD 25 (2016/03)

Professional Liability Insurance Certificate



TRUEN-1 OP ID: TL

# CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY) 05/03/2021

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

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

PRODUCER 715-425-0159
Leitch Insurance Agency Inc
174 E Pine St
P O Box 85
River Falls, WI 54022
Steven J Leitch

CONTACT NAME: Steven J. Leitch
PHONE (A/C, No, Ext): 715-425-0159 FAX (A/C, No): 715-425-6439
E-MAIL ADDRESS:

| INSURER(S) AFFORDING COVERAGE | NAIC # |
|---|---|
| INSURER A : Capitol Specialty Ins. Corp. | 10328 |
| INSURER B : | |
| INSURER C : | |
| INSURER D : | |
| INSURER E : | |
| INSURER F : | |

INSURED True North Consulting Grp LLC
Elert & Assoc Networking Div
P O Box 2169
Hewitt, TX 76643

COVERAGES CERTIFICATE NUMBER: REVISION NUMBER:

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

| INSR LTR | TYPE OF INSURANCE | ADDL INSD | SUBR WVD | POLICY NUMBER | POLICY EFF (MM/DD/YYYY) | POLICY EXP (MM/DD/YYYY) | LIMITS | |
|---|---|---|---|---|---|---|---|---|
| | □ COMMERCIAL GENERAL LIABILITY<br>□ CLAIMS-MADE □ OCCUR<br>□<br>□<br>GEN'L AGGREGATE LIMIT APPLIES PER:<br>□ POLICY □ PRO-JECT □ LOC<br>OTHER: | | | | | | EACH OCCURRENCE<br>DAMAGE TO RENTED PREMISES (Ea occurrence)<br>MED EXP (Any one person)<br>PERSONAL & ADV INJURY<br>GENERAL AGGREGATE<br>PRODUCTS - COMP/OP AGG | $<br>$<br>$<br>$<br>$<br>$<br>$ |
| | AUTOMOBILE LIABILITY<br>□ ANY AUTO<br>□ OWNED AUTOS ONLY □ SCHEDULED AUTOS<br>□ HIRED AUTOS ONLY □ NON-OWNED AUTOS ONLY | | | | | | COMBINED SINGLE LIMIT (Ea accident)<br>BODILY INJURY (Per person)<br>BODILY INJURY (Per accident)<br>PROPERTY DAMAGE (Per accident) | $<br>$<br>$<br>$<br>$ |
| | □ UMBRELLA LIAB □ OCCUR<br>□ EXCESS LIAB □ CLAIMS-MADE<br>□ DED □ RETENTION $ | | | | | | EACH OCCURRENCE<br>AGGREGATE | $<br>$<br>$ |
| | WORKERS COMPENSATION AND EMPLOYERS' LIABILITY<br>ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) Y / N □<br>If yes, describe under DESCRIPTION OF OPERATIONS below | N / A | | | | | □ PER STATUTE □ OTH-ER<br>E.L. EACH ACCIDENT<br>E.L. DISEASE - EA EMPLOYEE<br>E.L. DISEASE - POLICY LIMIT | <br>$<br>$<br>$ |
| A | Professional Liab | | | SCG0007814-4 | 05/09/2021 | 05/09/2022 | Per Claim<br>Aggregate | 5,000,000<br>5,000,000 |

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

Coverage is claims made. $25,000 Retention. 7/7/2014 retroactive date applies to True North Consulting Group LLC. 11/29/1989 retroactive date applies to Elert & Associates Networking Division Inc. Coverage includes cyber liability at $5,000,000 per claim with $25000 retention.

CERTIFICATE HOLDER

FORPR-1

FOR PROPOSALS ONLY

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

ACORD 25 (2016/03)

5. Identify the name, address, and contract information for three (3) companies that the Consultant has performed similar services to those being sought by the Authority.

**Reference #1**

**Business Name:** Bi-State Development

**Contact Name:** Ms. Deborah Rowey / Ms. Crystal Messner

**Address:** 1 Metropolitan Square, 211 North Broadway, Suite 700, St. Louis, MO 63102

**Email Address:** dmrowey@bistatedev.org / cmmessner@bistatedev.org

**Phone Number:** (314) 982-1400 / (314) 982-1400 x3001

**Project Description:** Internal - External Vulnerability and SCADA Assessments along with summary/executive summary reports and suggested remediation

**Date of Project Completion:** The assessment process is still being conducted. It will be completed on time successfully within the next 40 days as promised.

**Reference #2**

**Business Name:** City of Palm Beach Gardens

**Contact Name:** Mr. Eric Holdt, Information Technology Administrator

**Address:** 10500 N Military Trail, Palm Beach Gardens, FL 33410

**Email Address:** eholdt@pbgfl.com

**Phone Number:** (561) 799-4142

**Project Description:** Cybersecurity Assessment and IT Security Overview

**Date of Project Completion:** 02/05/21-03/15/21

**Reference #3**

**Business Name:** Town of Dudley, Massachusetts

**Contact Name:** Mr. Jonathan Ruda, Town Administrator

**Address:** 71 West Main Street, Dudley, MA 01571

**Telephone Number:** (774) 275-1923

**Email Address:** jruda@dudleyma.gov

**Project Description:** Complete cybersecurity assessment along with consulting of IT applications throughout town to include Police and Fire departments. Currently working as consultants for a third project. This assessment process was originally conducted over a period of six weeks, along with two additional cybersecurity projects in play.

**Date of Project Completion:** Continuous vCISO

***Please Note:*** *Additional references are available upon request.*

6. If you are a certified, minority and/or women-owned business, submit a copy of the certification.

True North Consulting Group is not currently a minority and/or women-owned business.

## Item 2 – Consultant Team

(a) Relevant qualifications and experience, including educational degrees and any applicable licenses or certifications (e.g., CISSP, CISM, CGEIT, CRISC), and

Please see licenses and certifications listed in the resumes on the following pages and in Part 4 of Team TNCG's response.

(b) State and county of residence:

- Dr. Patrick Johnson: Texas, Hill County
- Mike Indergard: Texas, McLellan County
- Dimitrios Hilton: Minnesota, Hennepin County
- Tyrone Wilson: Virginia, Arlington County
- Joel Langill: Wisconsin, Outagamie County

(c) Scope of responsibility:

- Dr. Patrick Johnson, Project Manager, Cybersecurity Consultant
- Mike Indergard, Director of IT Network Consulting
- Dimitrios Hilton, Executive Security Consultant/SCADA OT Engineer
- Tyrone Wilson, Cybersecurity Consultant-Internal/External Vulnerability Applications
- Joel Langill, SCADA Consultant/Penetration Testing Applications

(d) Length of time working for consultant:

- Project Manager: Dr. Patrick Johnson, 5 yrs. Experience
- Security Engineer: Mike Indergard, 19 yrs. Experience
- SCADA OT Engineer: Dimitrios Hilton, 16 yrs. Experience
- Cybersecurity Consultant: Tyrone Wilson, 18 yrs. Experience
- SCADA Consultant: Joel Langill, 35 yrs. Experience

### Resumes

Please see Team TNCG's key personnel resumes on the following pages.

# Patrick Johnson

## Cybersecurity Practice Manager

### Education

California Intercontinental University

- Doctor of Business Administration – Information Systems & Enterprise Resource Management

University of North Texas

- Master of Science - Computer Education & Cognitive Systems

University of Texas at Arlington

- Bachelor of Science - Information Systems

### Areas of Expertise

- Cybersecurity
- Information systems development, implementations, and integration
- Networking and security infrastructure
- Project Management
- Technology Planning
- Fiscal Management
- Data Centers

### Training, Certifications, and Memberships

- COBIT 5: ISACA – Control Objectives for Information and Related Technologies
- ITIL Foundations: HDI – Information Technology Infrastructure Library
- CISSP: ISC2 – Certified Information Systems Security Professional
- (ISC)2 – International Information Systems Security Certification Consortium
- LISD – Bond Oversight Committee
- LISD – Technology Advisory Committee
- COSN – Consortium of School Networks
- Phi Kappa Phi – National Honors Society - UNT Denton Chapter
- TxDLA – Texas Distance Learning Association
- TCEA – Texas Computer Education Association
- ISTE – International Society for Technology in Education
- BPA – Business Professionals of America

### Significant Projects

**Network Services**

**Internet Resiliency Architecture** – Architected two disparate 5Gbps links to the Internet with redundant gear for firewalls, filtering, and routing providing; intent was to provide 24/7 uninterrupted access for teaching, learning, and district operations.

**Data Center Core Resiliency Architecture** – The core access routing and switching gear was completed replaced and implemented in a tiered and redundant fashion to ensure uninterrupted access for teaching, learning, and district operations.

**90% Server Virtualization** – Using VmWare virtualization technology, 90% of physical servers were removed from the datacenter. The result was lowered costs of power, HVAC, UPS load; provided flexibility of adding removing compute resources at will, lending to extreme growth capacity.

**State-of-the-Art Web Content Filtering** – New content filter stack was implemented with redundancy and scale in mind; solution allows for decryption of network traffic as more and more websites begin to use HTTPS to encrypt and hide traffic content. The ability to modify Web 2.0 content is also a differentiator in services offered to students.

**Disaster Recovery (DR) Plan Implemented** – Architected plans for business continuity and disaster recovery which included collaboration between network, infrastructure, and data services teams. The DR site was architected with the state-of-the-art converged computing Vblock platform. EMC and VmWare tools were integral to the plan and processes.

**Infrastructure Services**

• **District Wireless Access Initiative (DWAI)** – A complete overhaul of all wireless networking district-wide; included renovation of HVAC, data racks, copper cabling for 1 wireless access point for every classroom in the district at 69 campuses and 15 other facilities. Wireless access point count is 5800+. Provided 10Gbps fiber between data closets at all secondary campuses.

• **Unite Private Networks (UPN) Initiative** – provided 10Gbps fiber from each of the 69 campuses to the main LISD datacenter; partially funded through the Federal E-rate program and bond funds.

### Experience

2019 – Present True North Consulting Group

- Cybersecurity Practice Manager

2017 – 2019 Tarrant County

- Senior IT Resource Manager

2016 – 2017 EducationSuperHighway

- Senior Network Consultant

2015 – 2016 Lewisville Independent School District

- Interim Director of Network & Technical Services

# Mike Indergard
## Director of Strategic Planning

### Education

Baylor University

- Master of Information Systems

Texas State Technical College

- Network Administration

Texas Christian University

- Bachelor of Arts (History)

### Areas of Expertise

- Security architecture
- Wireless security
- NGFW
- VPN
- Security policy
- Nmap
- Project Management

### Training and Certifications

- Cisco CCNP Security
- Cisco CCNA
- Cisco CCNP R/S
- Cisco CCDA
- Cisco CCDP
- Microsoft MCSE 2003

### Significant Projects

**University of Texas at Arlington**

Lead for a network security consulting project that consisted of an overall network security assessment and gap analysis, re-architecture of the UTA RFC 1918 IP addressing scheme to support security-related initiatives, IP addressing scheme migration plan, Network Admission Control assessment and evaluation, endpoint protection evaluation, managed security services partner evaluation and recommendations, firewall configuration analysis and recommendations, east-west data center traffic protection evaluation and recommendations, and web application firewall recommendations.

**Aldine Independent School District**

Hired by Aldine ISD to design a Distributed Denial of Service mitigation solution and issue a Request for Proposal to address the risk of inbound and outbound DDoS attacks. The solution called for a hybrid on-premise/cloud-based solution that included a minimum of two network security appliances working in tandem with a cloud-based traffic scrubbing service to protect the district's 88,000 endpoints.

**Round Rock Independent School District**

Served as project manager for a cybersecurity assessment for a 50,000-student school district. The assessment scope consisted of a network and host discovery of the internal and external network, including reconnaissance, enumeration, and fingerprinting; vulnerability assessments of the public IP block and internal subnets for all 60 campuses including DMZ and data center subnets; manual and automated review and analysis of the dual firewall appliances and recommendations; and wireless testing focusing on authentication and configuration controls. Deliverables included an executive summary report of findings and recommendations, as well as vulnerability scan details and recommendations supporting remediation activities.

**Waxahachie Independent School District**

Conducted a network security assessment and issued recommendations for a district of over 8,000 students. Systems assessed included firewall architecture and configuration review, wireless policy and security configuration review, Active Directory Group Policy and Domain Admin role assessment, NTFS folder permissions evaluation, review of IP addressing scheme to accommodate implementation of security policy and assessed VPN traffic routing for site-to-site connections with district partners and for WISD user remote access.

### Experience

2017 – Present True North Consulting Group

- Director of Strategic Planning

2011 – 2017 Technology for Education

- Director of Technical Services

2009 – 2011 McLane Intelligent Solutions.

- IT Consultant

2006 – 2007 Technology for Education

- Systems Engineer

2001 – 2006 Coldwell Banker Realtors

- IT Administrator

# Dimitrios Hilton

## PROFESSIONAL SUMMARY

Accomplished Security Professional and IT Operational consultant for over 16+ years. Extensive experience and leadership in the Local Government space, as well and small and mid-sized private organizations. Uniquely combines his background in law enforcement with information security expertise to render security auditing deliverables and recommendations that are well received by management, which ultimately help organizations make immediate and long-term changes that improve their security posture.

## WORK HISTORY

InfoSec Associates, LTD – Minneapolis, MN (2014 – Present)

- Conduct Security Assessments (PCI, HIPAA, CJIS, NIST, SCADA, HITRUST)
- Conduct Security Analyst Services (SIEM, IPS/IDS, Endpoints, IR, Defense in Depth)
- Develop Security Policies & Procedures (PCI, CJIS, HIPAA, Organizational)
- Security Training (PCI, HIPAA, CJIS, custom needs)
- CIO / CISO Services (Virtual and On-Premise)
- Project Management Services

LOGIS (Local Government Information Systems) – Golden Valley, MN (2015 – 2019)

- Security Specialist for 50 local government organizations
- PCI Specialist for over ~ 100 PCI environments
- Conduct Security Assessments (PCI, HIPAA, CJIS, SCADA)
- Developed Security Budgets for numerous cities
- Internal Security Analyst duties (SIEM, IPS/IDS, Endpoints, IR)
- Developed Security Policies & Procedures (PCI, CJIS, HIPAA, Organizational)
- Security Training (Citywide, organizational, PCI, HIPAA, CJIS, SCADA, custom needs)
- Vulnerability Management Program (PCI ASV, Web Application, Network)
- Project Management (Pen Testing, Security Auditing, Payment Processing conversions)
- Law Enforcement Security (CJIS/FBI Audits, LE Technology Audits)

The IT Guy, LTD – Saint Paul, MN (2004-2014)

- Information Technology Consulting Company (President/Senior Consultant)
- Managed 1-5 Staff (Finance, IT Technicians, Developers)
- Client sizes range from 1-1000 end-users across multiple industries, including Healthcare, Retail POS/PCI, Law, SCADA/ICS, and many other business types
- Server, Storage, Workstation, Backup, Endpoint protection, and many other services

## EDUCATION

- Law Enforcement Certificate Program – Hennepin Technical College (2018)
- Post Grad – University of St. Thomas (1999) Superintendent/Principal Licensure
- M.S. Ed. – University of Pennsylvania (1992) – Education
- B.S. – Rutgers College (1990) – Dual Major Chemistry/Administration of Justice

## CERTIFICATIONS

- Minnesota POST Certification (March 2019)– Hennepin Tech Law Enforcement Center
- CISSP Security (Valid)
- CISA Auditor – Expected Q1 2020
- SCADA Security Certificate for Infrastructure (Valid)
- Emergency Medical Responder (Valid)
- CJIS Level 4 Training (Valid)

## PROFESSIONAL ACTIVITIES & ASSOCIATIONS

- ISC2 Security Congress – PCI Workshop Presenter (2017- Present)
- ISC2 (CISSP) Twin Cities Chapter President (2019 – Present)
- MN Government Finance Officers Association – Presenter PCI Seminar (2018)
- MS-ISAC Member

## Tyrone E. Wilson

### PROFESSIONAL SUMMARY

- Twenty-four years of Information Technology and Systems Configuration experience with 20 years focused on Information Systems & Network Security. Organizer of The D.C. Cybersecurity Professionals, a 7,800+ member meetup group. Currently holding positions of increasing responsibility while serving in the Army Reserves.
- Extensive expertise in Computer Network Defense; Project and Program Management; Vulnerability Assessments and Penetration Testing; Cyber Threat Analysis; Security Center Operations; Security System Architecture Assessments; Information Systems Engineering; Incident Response; Data Mining; Splunk; IPv6; Metasploit; Kali (Linux); Web Application Testing (Burp Suite Pro), Information Security Training (Pentester Prep, SOC Analyst Prep, Certified Ethical Hacker Practical, CISSP, CySA+, Net+, Sec+)

### EXPERIENCE

***ACS Cyber SEAL Program, Member*****..........................................................03/2017 – Present**
**Agile Cyber Security Solutions, LLC** (Purcellville, VA)

- Serves as a lead for various cybersecurity awareness, security assessment, and penetration testing engagements.
- Developed and lead multiple spear phishing engagements targeting medium to large corporations.
- Assists with network security assessments and stress testing of multi-million-dollar networks varying in agency.
- Assists with the development and delivery of cybersecurity awareness and penetration testing training.

***Founder & President*** **..............................................................................06/2013 – Present**
**Cover6 Solutions, LLC** (Arlington, VA)

- Presides over day-to-day operations of a 15-person company to include decision-making on strategies and policies.
- Sponsors, hosts, and presents material to a 7,000+ person Meetup group (D.C. Cyber Security Professionals) teaching various aspects of Information Security, Intro to Cyber, Penetration Testing, IPv6, and SOC Analyst Preparation
- Performs freelance penetration testing and training for various organizations and small groups.

***Program Manager, Penetration Testing*****..........................................................07/2015 – 02/2016**
**Fortalice Solutions** (Washington, D.C.)

- Developed and lead penetration testing team and built the underlining process framework.
- Conducted penetration tests on critical infrastructure, applications, and risk management programs.
- Provided technical information system security testing in support of the appropriate risk management processes.
- Provided quality assurance and technical reviews of deliverables, results, and internal documentation.
- Developed and lead strong working relationships with clients and client leads.

***Cyber Security Analyst, Subject Matter Expert (SME)*****.........................................07/2014 – 08/2015**
**Novetta Solutions / Department of Energy** (McLean, VA / Washington, D.C.)

- Managed and coordinates services essential to protecting, defending, and sustaining the three echelons of Department of Defense computer networks (NIPR, SIPR, and JWICS) on strategic infrastructure.
- Ingested emerging threat reports to generate protection plans for the enterprise.
- Coordinated the mitigation of over 20 high threat CND events since 01 January 2015.
- Presided over evaluation of endpoint applications, hardware, and network services.
- Provided training of security testing tools such as (Nmap, Netcat, Metasploit, Retina, Nessus, Kali, Wireshark, etc.)

***Senior Cyber Security Analyst 06/2011 – 11/2013***
**Salient Federal Solutions** (Fairfax, VA)

- Cyber security Subject Matter Expert (SME) responsible for the security posture of over 1000 systems at 19 locations
- Lead analyst responsible for signature management of IPv6 Intrusion Prevention & Detection System (Assure6)
- Developed and implemented incident response procedures for mitigating direct and indirect network attacks
- Coordinated the integration of the Splunk Enterprise threat management system into network structure
- Served as an Assistant Instructor for the IPv6 101 and IPv6 Security courses

***Cyber Threat Analyst, Non-Commissioned Officer in Charge 06/2010 – 05/2011***
**Regional Computer Emergency Response Team – Southwest Asia (RCERT-SWA)** (Camp Victory, Iraq)

- Computer Network Defense (CND) SME responsible for the security posture of the DoD's Global Information Grid (GIG) in Iraq and Kuwait
- Developed the SWA Cyber Intelligence Cell SharePoint Portal; increased overall site usage by over 400%, enhancing the cyber situational awareness for SWA units
- Acted as the Sr. CND Analyst while auditing five Forward Operating Bases (FOBs) in Iraq; scanned, analyzed, and recommended upgrades to security posture for over 10,000 systems
- Trained over 50 analysts on the utilization of network defense tools such as Centaur, ArcSight, Remedy, and the Host-Based Security System (HBSS) web console

***Senior Level Information Assurance Analyst/Fusion Cell Team Lead 08/2008 – 06/2010***
**Joint Task Force Global Network Operations, USCYBERCOM** (Ft. Meade, MD)

- Principal Engineer: Supported CND effort as a Tier 3 Information Assurance analyst and Intrusion Set SME
- Analyzed, characterized, and tracked malicious network activity within the Department of Defense (DoD)
- Performed network intrusion analysis based on logs, netflow, firewalls, and full packet capture utilizing tools unique to the intelligence community
- Collaborated with various CNDSPs, CERTs, NOCs, and Intel organizations. Analyzed origins, pathways, methodologies of cyber activities to model and predict future intrusions against the GIG

***Cyber Trends Analyst, Non-Commissioned Officer in Charge 05/2005 – 05/2008***
**1st Information Operations Command, Cyber Intelligence Center** (Ft. Belvoir, VA)

- Produced all source intelligence fusion used for weekly Army Network Analysis Report (ANAR) intelligence assessment which is used by the analytic community to determine possible threats to the Global Information Grid
- Developed and implemented the CIC's Trend Analysis Cell initial TTP's
- Led a four-person Trends Analysis team as the Senior Analyst; improved performance by 35%
- Developed and briefed intelligence products to senior Army officials via White Papers, Daily Intelligence Summaries, Network Intrusion Reports, Weekly Trends, CONOPs, JQRs, and SOPs
- Conducted open-source research and assessment of network trend data and malware mitigation effects to attenuate IP block ranges and facilitate maximum network functionality while simultaneously maintaining security
- Produced IP/Domain mitigation recommendation briefings for the Army Global Network Operations Support Center
- Participated in over 100 conferences and site visits
- Responsible for reviews of current and evolving technologies, tools, and summaries of cyber-related events
- Populated national and local databases with critical CNO information needed for strategic and tactical operations.

## EDUCATION

- University of Phoenix
- Bachelor of Science, Information Technology; Information Systems Security - 2018

## CERTIFICATIONS

- EC-Council Certified Ethical Hacker (CEH) Practical (CEH Master) - 2020
- eLearn Security Junior Penetration Tester (eJPT) - 2020
- CompTIA Security+ ce (Security+) - 2019
- CompTIA Network+ ce (Network+) - 2019
- Cisco Certified Network Associate (CCNA) Security - 2014
- IPv6 Forum Certified Engineer (Silver) - 2012
- EC-Council Certified Ethical Hacker (CEH) - 2007
- ArcSight Certified Advanced Security Analyst (ACASA) - 2006
- System Administrator/ Network Security Manager (SA/NSM) - 2003
- Information Assurance Security Officer (IASO) - 2003

## PROFESSIONAL EDUCATION

- Routing and Switching (CCNA), Secure Ninja – 2016
- Advanced Leader Course – US Army – 2014 (Distinguished Honor Graduate)
- IPv6 Essentials - SANS – 2012
- Penetration Testing & Ethical Hacking - SANS – 2012
- Basic Fiber Optics Course – US Army - 2010
- Certified Ethical Hacker, Boot Camp – 2007
- Securing Windows 2003 Server – US Army - 2005
- Information Systems Operator/Analyst Course – 2002
- Certified Information Systems Security Professional (CISSP), Intense School Boot Camp – 2007
- Basic Non-Commissioned Officer Course - 2007
- Computer Network Defense Course (CNDC) - 2003
- Primary Leadership Development Course – US Army - 2003 (Commandants List, Appeared in Leadership Board)

# Joel Thomas Langill

## PROFESSIONAL SUMMARY

Senior operational security professional focused on industrial automation and control systems with over 35 years of global industry experience in manufacturing, instrumentation, process control, physical and cybersecurity, functional safety, and production information systems working for companies in consumer products, packaging, pharmaceutical, petrochemical, automation, and engineering / procurement / construction industries with responsibilities covering conceptual and detailed design, process hazard analysis, risk assessment, security and vulnerability assessment, penetration testing, budgeting, cost estimating, installation, maintenance and support, upgrades and migrations, training, marketing, and sales leadership.

## PROFESSIONAL EXPERIENCE SUMMARY

**Founder and Managing Member** **2020 - present**

Industrial Control System Cyber Security Institute (ICSCSI) LLC, Hortonville, Wisconsin

*Provide comprehensive training curriculum encompassing all aspects of Industrial Control System history, architecture, design, installation, support, maintenance, and security through an integrated industrial control system security range and learning management system for delivery via live in-person, live streaming, and on-demand training models*

**Adjunct Professor** **2020 - present**

Texas A&M University – Commerce/RELLIS Campuses

*Instructor for first of its kind course on cybersecurity for industrial and facility-related control systems through the College of Science and Engineering and lead technical advisor in the design and commissioning of an advanced ICS/SCADA laboratory on the RELLIS campus for advanced research and development in industrial OT architectures and cybersecurity including spectrum research on 5G technologies*

**Director - Industrial Control System Cybersecurity Services** **2016 - 2021**

Amentum – Mission Engineering and Resilience (formerly AECOM – Management Services Group), San Antonio

*(Reporting to the Senior Vice President, Mission Engineering and Resilience)*

*Provide Industrial Control Security (ICS) architecture, engineering, and management expertise for new and existing customers, as well as internal working groups, including performance of risk, vulnerability, and threat assessments and penetration tests for ICS and associated infrastructure, as well as determination of root cause of ICS security breaches and research, recommend, and implement changes to procedures to protect data from future breaches*

**Consultant - Industrial Control System Cyber Security** **2011 - 2016**

Self-Employed

*Cybersecurity expert specializing in the identification, mitigation, and assessment of vulnerabilities within industrial control systems and their associated infrastructure covering local- and wide-area networks across a broad range of commercial and custom applications for industrial installations for clients in both public and private sectors via classified and unclassified activities including threat and security assessments, penetration testing, product evaluations, security architecture design*

**Founder and Website + Content Developer** **2010 - Present**

SCADAhacker.com (*now a part of ICSCSI LLC*)

*Developed and launched a website and broad social presence focused on relevant, candid, mission-critical information sharing related to operational security that has maintained active engagement from readers in more than 70 countries around the world and hosts the industry's most comprehensive resource library of standards, best practices, threat intelligence, event data, tools, methodologies, and product information targeting operational security and industrial control systems*

**Lead ICS/SCADA/DCS Instructor** **2010 - 2011**

InfoSec Institute, Chicago, IL

*Lead instructor of SCADA security certification course sanctioned by the Information Assurance Certification Review Board (IACRB) and the Certified SCADA Security Architect (CSSA) credentials*

**Staff Engineer & Security Consultant** **2008 - 2011**

ENGlobal - Automation Group, Inc., Houston, TX

*(Reporting to the Vice President/General Manager – South Region)*

*Provide specialized, advanced consulting services pertaining to complete automation solution architectures, implementation methodologies, and test strategies, including engineering audits and assessments of customer installations relating to cybersecurity, networking, automation, control, functional safety, and third-party system integration and included the original development of a packaged "drop-in" solution providing multiple layers of protection for allowing open and secure remote access to control systems networks*

**Various Positions – Technology and Consulting Leadership** **1991 - 2008**

Honeywell Process Solutions, Americas Region, Phoenix, AZ

*Held numerous positions within the organization, beginning as a Sales Engineer in the International Operations Group, advancing to consulting and technologist positions that focused on large system design and associated product development activities in a distinguished career as a global company resource and in-country activities in more than 50 countries including many of the developing nations and their critical infrastructure implementation and expansion*

**Control Systems Engineer** **1990 - 1991**

Shell Oil Company, Deer Park Manufacturing Complex, Deer Park, TX

*(Reporting to the Control Systems Specialty Team Leader – Refining West)*

*Provided control systems support to several areas within a large petrochemical complex that included beta testing for hydrostatic tank gauging technology, support of one of the largest multi variable blending applications, and advanced centrifugal compressor control strategies*

**Technical Cooperative Engineer** **1983 - 1986**

General Electric Company, Lighting Business Group, Cleveland, OH

*(Reporting to the Manager – Manufacturing Technology Programs Group)*

*Responsible for engineering and installation of process monitoring and vision inspection equipment on fluorescent lamp manufacturing machinery based on custom software development on real-time operating system (RSX-11M/S) that included role as a critical beta customer site for Digital Equipment Corp (DEC) real-time VAX operating system (ELN)*

## RELEVANT PROJECT EXPERIENCE

**United States Department of Defense – Department of the Army – IMCOM-E** **2019 - 2020**
Germany, Belgium, Italy
*Conduct Asset Inventory and Security Assessments on Facility-Related Control systems such as fire, closed-circuit television, access control, utility monitoring/control, lighting, and intrusion detection as part of the Risk Management Framework Assessment and Authorization activities at multiple garrisons and installations.*

**U.S. Department of Energy – Waste Isolation Pilot Plant (WIPP)** **2019**
Carlsbad, NM USA
*Conduct Vulnerability Assessment, Review, and Consultation as part of on-site activities associated with Dept. of Energy workplace practices, including a security review of the existing Industrial Control Systems as part of a larger company contract providing Operations & Maintenance Services to the facility.*

**U.S. Department of Defense - INDOPACOM** **2019**
Camp H.M. Smith – Aiea, HI USA
*Deliver specialized training on Defensive and Offensive Cyber Operations targeted at Industrial Control Systems covering SCADA and Facility-Related Control System architectures to multiple Cyber Protection Teams within the combatant command.*

**U.S. Central Intelligence Agency** **2016 - 2017**
Langley, VA USA
*Perform Security Assessment and Penetration Testing against power and energy management systems as part of a larger company contract to provide Operations & Maintenance Services to the Headquarter Campus. Results were used to understand existing risk exposure and fund short- and long-term funding for system and infrastructure upgrades.*

## EDUCATION

**University of Illinois**, B.S. Electrical Engineering with University Honors (“Bronze Tablet”) May 1987

## CERTIFICATIONS AND PROFESSIONAL DISTINCTIONS

- Certified SCADA Security Architecture – Information Assurance Certification Review Board 2011
- Advanced Incident Command System for Command & General Staff (ICS-400) - FEMA 2010
- Certified Ethical Hacker – EC Council 2010
- Certified Penetration Tester – Information Assurance Certification Review Board 2010
- TÜV Functional Safety Engineer (FS-Eng ID 1772-09) 2009
- U.S. Trademark (USPTO Serial No. 77728026) “viMAC” 2009
- U.S. Patent (USPTO Grant No. 8138927) “A Flare Characterization and Control System” 2007
- Honeywell Golden Eagles Club for Outstanding Performance 1996, 1999
- Emergency Medical Technician-Basic – Texas Department of Health 1991
- Industrial Rope Rescue – Roco Corporation 1991
- Industrial Firefighting – Texas Engineering Extension Service – Texas A&M University 1990
- Basic & Intermediate Rope Rescue – Roco Corporation 1990
- Advanced I & II Rope Rescue – Roco Corporation 1990

## BOOKS AND PUBLICATIONS

- Co-Author *“Industrial Network Security,”* 2nd ed., E. Knapp, J. Langill, Syngress, December 2014
- Technical Reviewer *“Mastering Metasploit,”* Nipun Jaswal, May 2014
- Technical Editor *“Applied Cyber Security and the Smart Grid,”* E, Knapp, R. Samani, Syngress, April 2013

# PART 3

## Item 1 – Proposed Scope of Service

### *Planning and Assumption Validation*

Team TNCG has an excellent reputation for proceeding carefully, cautiously, and creating well-thought-out project plans. If awarded this contract, we will assume that we will start off the project with an onsite visit to work through the network documentation in greater detail, view the SCADA IT/OT environment, and establish a more detailed action plan.

### *IT Cybersecurity Risk and Vulnerability Assessment*

As requested in Erie County Water Authority's RFP, Team TNCG's Risk Assessment will include the categories and subcategories of the NIST "Framework for Improving Critical Infrastructure Cybersecurity."

Team TNCG's lead assessor is also a certified SCADA Security Architect and has worked extensively in mixed IT/OT environments. We will provide you with real-life and practical recommendations to improve the Authority's security posture.

One of the best ways of conducting a valuable assessment is to have our assessor make an onsite visit to see and understand your IT and OT environment. Previous clients have greatly appreciated this approach, making the project much more beneficial to the client.

We will also include the following elements to your project as you requested in your RFP:

- Test for susceptibility to Advanced Persistent Threats (APTs) such as viruses, malware, Trojan horses, botnets, and other targeted attack exploits.
- Evaluate the Authority's current threat posture, including antivirus and Intrusion Detection and Prevention (IDP) capabilities.
- Evaluate the Authorities planned changes and improvements to the threat surface and assist in identifying and addressing security concerns.
- Review the Authority's current Supervisory Control and Data Acquisition (SCADA) water systems for security vulnerabilities.
- Review wireless network system components for security vulnerabilities, validating system-specific operating systems and firmware versions for known exploits and recommend upgrades, updates, and mitigations.
- Review current system-specific operating systems and firmware versions for known exploits and recommend upgrades, updates, and mitigations. This process includes firewalls, switches and routers, Microsoft Active Directory, email and file servers, web servers, wireless routers, WAN, VPN, VoIP, and CCTV systems.
- Assess VoIP network system components for security vulnerabilities, validating the system-specific operating system and firmware versions and reviewing for known exploits.

- Review existing IT policies and procedures and make recommendations for changes and/or additional policy and procedure development.
- Execute and review internal network vulnerability scans and external vulnerability and penetration scans and make recommendations to reduce the threat attack surface.

### *Change Controls*

Team TNCG uses a formal Change Control process and approval method before starting the actual technical penetration testing. This method ensures that all critical members of your team know:

- What network segments are being tested
- When (Date/Time window(s) you approve the testing to occur
- Impact cautions to prevent service disruptions.
- Emergency Contacts

Our clients greatly appreciate this most professional approach and the excellent written communication and documentation it provides.

### *Project Management & Status Meetings*

Team TNCG gladly and ordinarily provides frequent Status Meetings organized by our Project Manager. Our Project Manager is well organized, and meetings are productive, efficient, and designed to preserve valuable Authority leadership time. If additional status meetings are needed at any time during the project, we quickly accommodate those requests.

### *Technical Approach: SCADA System Vulnerability Assessment and Penetration Testing*

The vulnerability/penetrating test is conducted to simulate external attacker activity to include both automated and manual testing with the assistance of various industry-standard tools. The test team will analyze vulnerability/pen test results to identify significant findings that may pose a considerable risk to your internal web application(s) and internal network infrastructure. A Summary of Findings will be provided, which will contain a description of each vulnerability identified during the testing period and the recommended mitigation actions. Each recommendation should be thoroughly evaluated for its applicability and potential impact.

The penetration testing will be executed in three sequential phases. The first “remote” phase consists of planning to include finalizing the evaluation targets, transmittal of key documentation, including system architecture, network topology, network address spaces, and system/software vendor lists. This information provides a high-level classification of asset risk and aids in understanding the mapping of threats to operational impact. Scheduling of the physical assessment and testing can then be performed, providing a more accurate schedule and sequencing of the activities.

With three-fifths of the targets classified as OT devices, it is not practical to perform either the vulnerability assessment or penetration testing remotely. The most important aspect of these tests is the assurance that there will be no negative impact on the system's operation, including device availability, network traffic flow, and data integrity. The tools, techniques, and procedures used are based on prior use on operational systems to minimize the injection of unnecessary traffic and provide accurate data collection.

A combination of commercial active and passive vulnerability scanners will be used in conjunction with benchmarks, configuration files, and command-line functions (e.g., PowerShell) to expose both embedded weaknesses due to software vulnerabilities and unintentional faults due to configuration choices. On-site access also allows for the observation of existing policies, procedures, and practices that can enhance the accuracy of the actual level of unmitigated risk present. This information will be used to develop a strategy for penetration testing that will comprise a combination of host-based, network-based, and device-based attack vectors. The client will approve the decision on attack vectors applied to the operational components.

The final "remote" phase focuses on the organization and development of a report detailing the overall methodology used, weaknesses discovered and their severity, and recommendations based on vendor data and personal experience to remediate the risk to an acceptable level. Critical and high severity vulnerabilities will be further analyzed using temporal and environmental factors to present the risk more accurately to the client. This report will also be produced as a presentation allowing for a joint executive briefing of the findings.

During a typical engagement, the test team will use a variety of tools that may include:

- Google, Spiderfoot (Open Source Intelligence/Research)
- ARIN, RIPE, Farsight DNSDB Scout (IP Space and Passive DNS Records)
- Wayback Machine (website archive repository)
- Crunchbase (an information repository for private and public companies)
- Burp Suite, Acunetix, Nikto (web application audit and vulnerability identification)
- Retire.js (discovers old/retired javascript libraries)
- GoBuster (web site directory discovery by brute forcing)
- Builtwith (Technology information profiler tool "Relationships")
- Nmap (Network Mapper)
- S3Scanner (identification of S3 buckets)
- Nessus (vulnerability identification
- Powersploit, Powershell Empire (exploitation)

***Web Application Security Assessment***

The Web application review will examine the client' web application infrastructure for the following vulnerabilities:

- Application assessment based on OWASP, SANS, CWE, WASC standards OWASP TOP 10 – Site: https://www.owasp.org/index.php/Top_10-2017_Top_10
  - > A1 Injection (XML and SQL): Web applications pass parameters when they access external systems (databases) or the local operating system. If an attacker can embed malicious commands in these parameters, the external system may execute those commands on behalf of the Web application, which may allow an attacker to compromise the system.
  - > A2 Broken Authentication and Session Management: Account credentials and session tokens are not properly protected. Attackers who can compromise passwords, keys, session cookies, or other tokens can defeat authentication restrictions and assume other users' identities. This includes flagging session tokens (for example, cookies) as "secure," not exposing session IDs in the URL, and incorporating appropriate time-outs and rotation of session IDs after a successful login.

> A3 Sensitive Data Exposure: Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

> A4 XML External Entities (XXE): Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

> A5 Broken Access Control: Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as accessing other users' accounts, viewing sensitive files, modifying other users' data, changing access rights, etc.

> A6 Security Misconfiguration (including cookies): A strong server configuration baseline is critical to a secure Web application. These servers have many configuration options that affect security and are not secure “out of the box.”

> A7 Cross-Site Scripting (XSS): XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser, which can hijack user sessions, deface websites, or redirect the user to malicious sites.

> A8 Insecure Deserialization: Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

> A9 Using Components with Known Vulnerabilities: Web applications often make use of libraries, frameworks, and software modules. An attack based on vulnerable components can result in data loss or server takeover. Known vulnerabilities may undermine application defenses.

> A10 Insufficient Logging & Monitoring: Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to attack systems further, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

- Unvalidated Input: Information from Web requests is not validated before being used by a Web application. Attackers can use these flaws to attack back-end components through a Web application.
- Unsecure Access Controls: Restrictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access other user accounts, view sensitive files, or use unauthorized functions.
- Improper Error Handling: Error conditions that occur during normal operation are not handled properly. If an attacker can cause errors to occur that the Web application does not handle, they can gain detailed system information, deny service, cause security mechanisms to fail, or crash the server.
- Unsecure Storage: Web applications frequently use cryptographic functions to protect information and credentials. These functions and the code that integrates them have been proven to be difficult to code securely, frequently resulting in weak protection.

- Denial of Service (DoS) – if applicable: Attackers can consume Web application resources to a point where other legitimate users can no longer access or use the application. Attackers can also lock users out of their accounts or even cause the entire application to fail.
- Buffer Overflows – if applicable: Web application components in some languages that do not properly validate input can be crashed and, in some cases, be used to take control of processes. These components can include common gateway interfaces (CGIs), libraries, drivers, and web application server components.
- Controlled execution of automated tools to identify vulnerabilities that are presented to an application user in the form of an "anonymous user" and an "authorized user" (depending on the nature of the application, testing may include several authorized user roles).
- If a web application firewall or intrusion prevention system is deployed, determine if testing will include a 'shields down' phase for only the penetration tester.
- Testing will include testing for most recent vulnerabilities and exploits (i.e., Heartbleed, Poodle, etc.).
- Use manual techniques to confirm the vulnerabilities found by the automated scanning. The results of this phase are used in the later section titled "Exploitation."
- Perform testing to determine if a client session can be hijacked.
- Tools used in this phase include BurpSuite and Zed Attack Proxy.

### *Application Manual Penetration Testing/Exploitation*

After using automated scanning tools, the Penetration Tester reviews the output to verify the findings to eliminate false positives manually. A key part of our methodology is to address false positives by verifying and cross-referencing them against our extensive vulnerability knowledge base and well-known industry Best Practice Frameworks such as OWASP. Weaknesses are also correlated against our knowledge base to determine if potential false negatives were omitted. To verify if the vulnerability is a false-positive, we often will need to attempt to exploit the vulnerability. We never just completely rely on vulnerability scan reports but instead perform verification and exploitation to determine if the finding is valid. The Penetration Tester often discovers vulnerabilities during the manual testing phase that the automated scanners overlooked, such as performing manual tests using a web application proxy. This phase includes:

- Analysis of vulnerabilities identified. Vulnerabilities identified are exploited (*i.e.,* malicious code injection) under a mutually agreeable confirmation process with the Erie County Water Authority stakeholders
- Exploitation of inherent weakness in the design and implementation of security controls
- Privilege escalation, business logic exploitation, bypassing input validation, injection techniques, XSS testing, parameter manipulation, authentication, authorization bypass, etc.

### *Deliverables and Remediation Recommendations*

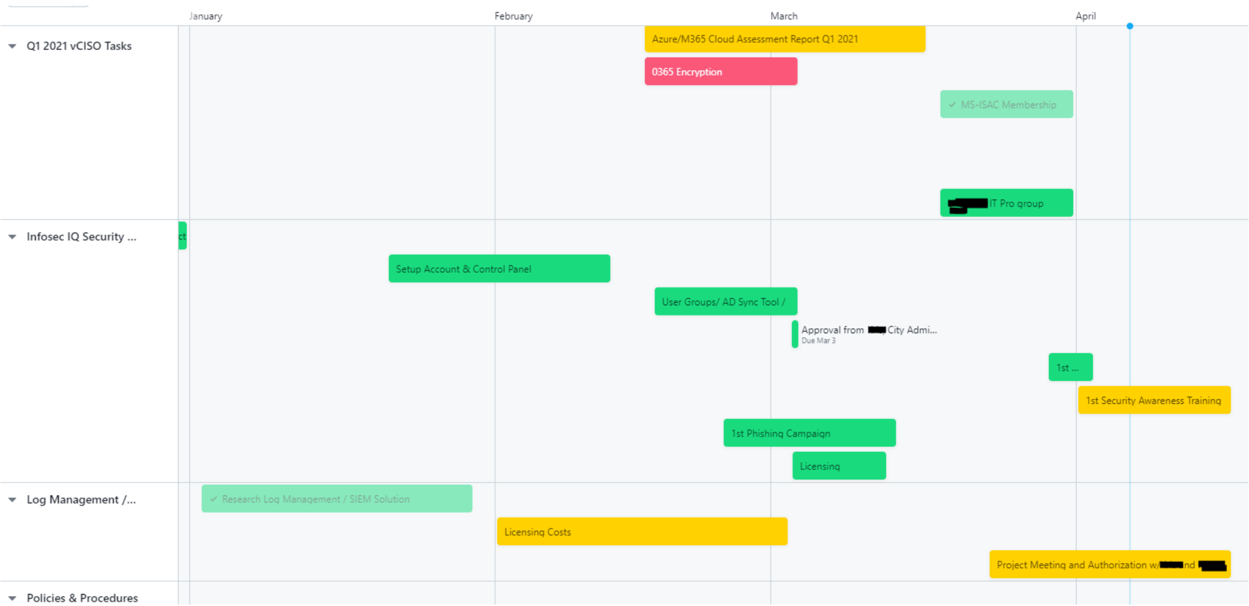
Team TNCG reports have been well received by local government organizations in the past. Team TNCG provides a "Full Report," which includes a comprehensive outline of background, scope, methodology, detailed findings/recommendations, and additional documents that provide the greatest level of detail if anyone desired to focus on that level of detail. Team TNCG can prepare additional variations of the Full Report to meet the needs of the Authority. For example, Team TNCG can create a redacted Public Executive Summary or a slightly more un-redacted Executive Summary for your Management or Board.

Team TNCG can also organize the Full Report so that sections can be distributed to discrete business units if appropriate in the Authority's case.

Our reports have been regarded as being clear, concise, and developed to meet all professional standards and deliver the content in a manner that makes life easier for top-level management. This overall process makes remediation easier and makes it possible to track those remediation efforts in other software or project management documents.

### *Security Roadmaps and Ongoing Assessment Updates*

Team TNCG's Risk Assessment results are easily converted into an actionable Security Roadmap. Our software allows us to update remediated results on a Quarterly and/or annual basis to demonstrate progress. Roadmaps would be developed in conjunction with key Authority staff but reflect the current Gap Analysis reports generated in our Risk Assessment.


January
February
March
April
Q1 2021 vCISO Tasks
Azure/M365 Cloud Assessment Report Q1 2021
0365 Encryption
✓ MS-ISAC Membership
[redacted] IT Pro group
Infosec IQ Security ...
ct
Setup Account & Control Panel
User Groups/ AD Sync Tool /
Approval from [redacted] City Admi...
Due Mar 3
1st ...
1st Security Awareness Training
1st Phishing Campaign
Licensing
Log Management /...
✓ Research Log Management / SIEM Solution
Licensing Costs
Project Meeting and Authorization w/[redacted]nd [redacted]
Policies & Procedures

Team TNCG's highly visual Road Maps are very beneficial to Technical and non-technical stakeholders. Our Security Practitioners are very skilled at conducting report meetings and status updates to technical and non-technical stakeholders and administrators.

## Item 2 – Hardware and Software Requirements

(a) Describe the required hardware and/or software necessary to implement Consultant's plan, if any.

None

(b) Describe the limitations of the service and/or equipment, if any.

No limitations were identified.

(c) Identify whether the required hardware and/or software will be provided by Consultant or the Authority.

Team TNCG will provide all hardware and or software for the assessment process.

## Item 3 – Timeframe for Deliverables

A detailed timeline will be provided before the official kickoff meeting to ensure the Erie County Water Authority is in concert with the overall assessment process. The timeframe and overall scope of work address the project deliverables, work breakdown and tasks, schedule and dependencies, weekly status reports, full results of vulnerability testing, gaps and mitigation plans, and a prioritized roadmap of activities in conjunction with the Erie County Water Authority to enhance the future cybersecurity position. Team TNCG will meet and/or exceed the expectations for the Authority's cybersecurity risk and vulnerability assessment process outlined in the RFP and associated Q&A details.

| **Week #** | **Tasks** |
|---|---|
| Week 1 | Kickoff - Onsite Visit |
| Week 2 | NIST Assessment (Framework for ICIC) - Weekly Status Reports-Updates |
| Week 3 | NIST Assessment (Framework for ICIC) - Weekly Status Reports-Updates |
| Week 4 | NIST Assessment (Framework for ICIC) - Weekly Status Reports-Updates |
| Week 5 | NIST Assessment (Framework for ICIC) - Weekly Status Reports-Updates |
| Week 6 | Application Penetration Testing - Weekly Status Reports-Updates |
| Week 7 | Application Penetration Testing - Weekly Status Reports-Updates |
| Week 8 | External Network Penetration Testing - Weekly Status Reports-Updates |
| Week 9 | SCADA Internal Penetration Testing - Weekly Status Reports-Updates |
| Week 10 | SCADA Internal Penetration Testing - Weekly Status Reports-Updates |
| Week 11 | Report Writing |
| Week 12 | Draft and Final Report Process |

## Item 4 – Price Structure

1. Detailed Price Structure

| **Week #** | **Tasks** | **Cost** |
|---|---|---:|
| Week 1 | Kickoff - Onsite Visit | $525 |
| Week 2 | NIST Assessment (Framework for ICIC) | $6,150 |
| Week 3 | NIST Assessment (Framework for ICIC) | $6,150 |
| Week 4 | NIST Assessment (Framework for ICIC) | $6,150 |
| Week 5 | NIST Assessment (Framework for ICIC) | 3,775 |
| Week 6 | Application Penetration Testing | $4,200 |
| Week 7 | Application Penetration Testing | $6,800 |
| Week 8 | External Network Penetration Testing | $6,250 |
| Week 9 | SCADA Internal Penetration Testing | $5,900 |
| Week 10 | SCADA Internal Penetration Testing | $5,900 |
| Week 11 | Report Writing | $3,900 |
| Week 12 | Draft and Final Report Process | $2,800 |
| | **Total Cost** | **$58,500** |

2. **Sample TNCG Consultant Agreement**

## CONTRACT WITH INDEPENDENT CONSULTANT
## TECHNOLOGY CONSULTING SERVICES

**THIS CONTRACT** is made effective as of this ____ day of _________, 2021, by and between the Erie County Water Authority, with an address for purposes of this Contract at _________________________ , and True North Consulting Group, LLC, a limited liability company of the State of Texas, with an address for purposes of this Contract at P.O. Box 2169, Hewitt, TX 76643 ("Consultant"). **NOW, THEREFORE,** for and in consideration of the mutual promises and covenants contained herein, the parties hereto agree as follows:

1. **Independent Consultant**. In all respects pertaining to this Contract, Consultant is and shall act as an independent Consultant (i.e., a person who is independently employed to do a piece of work according to Consultant's own methods and control except as to the result of the work) and Consultant shall neither be nor act as the agent, employee, or servant of _________. Neither Consultant nor Consultant's employees shall be entitled to any of the benefits established for _________ employees, nor be covered by _________'s Workers' Compensation Program.

1.1 The services to be performed by Consultant under this Contract, as well as professional fees, are further described in the _______'s RFP Attachment A for _________________ as well as Attachment B: _________, dated ______________ (X pages) which are incorporated herein for all purposes, as further discussed in Paragraph 24 below.

1.2 Without limiting the generality of the foregoing, it is understood and agreed:

(a) That all persons employed by Consultant in the performance of this Contract shall be employees of Consultant and not employees of _________; and

(b) That Consultant shall not enter into any contract with a third party that purports to obligate or bind _________.

2. **Indemnification**. CONSULTANT SHALL INDEMNIFY, DEFEND, AND HOLD HARMLESS THE _________, ITS OFFICERS, AGENTS, AND EMPLOYEES, FROM ANY AND ALL LOSS, COST, DAMAGE, EXPENSE, AND CLAIMS (INCLUDING, BUT NOT LIMITED TO, ATTORNEY'S FEES) AND LIABILITY OF ANY KIND FOR ANY ACTS OR OMISSIONS OF CONSULTANT, ITS OFFICERS, AGENTS OR EMPLOYEES, IN PERFORMANCE OF THIS CONTRACT.

3. **Gratuities**. Consultant acknowledges that Consultant will be advised of _________'s policies relating to ethics, including, but not limited to, _________'s General Code of Ethics and Consultant has not intentionally or knowingly violated any _________ policy. Except as otherwise provided in Paragraph 3.1 of this Contract, _________ may terminate this Contract at any time upon a finding by _________'s Board of Trustees ("Board") that Consultant, or an authorized agent or another representative of Consultant, has:

(a) Intentionally or knowingly offered, conferred, or agreed to confer on a _________ officer or employee any benefit as consideration for the recipient's decision, opinion, recommendation, vote, or other exercise of discretion in the recipient's capacity with _________; or

(b) Conferred a benefit on a _________ officer or employee following the award of a contract to Consultant that, using a reasonable and prudent person test, has the appearance of influencing such award.

3.1 This provision on "Gratuities" is not meant to and shall not apply to attendance at or the hosting of social functions unrelated to _________'s official business projects/matters; nor shall this provision apply to reported campaign contributions as contemplated under the Texas Election Code, nor to the payment of nominal amounts for meals and other activities that are related to ongoing _________ official business project(s) in which Consultant is currently involved with _________ and/or a third party and where the _________ is a guest of Consultant; except, however, this exception shall not excuse compliance with other rules of law and/or ethical behavior as may otherwise be applicable to any person and/or company.

3.2 In the event the _________, pursuant to this provision, terminates this Contract, _________ shall be entitled, in addition to any other rights and remedies the _________ may have, to recover or withhold the amount of the cost incurred by Consultant in providing such gratuities.

4. **Termination of Agreement**

4.1 Termination by _________. In the event of unsatisfactory performance by Consultant, as solely determined by _________, or in the event of a breach of this Contract by Consultant that is not cured within 30 days of written notification by the town administrator or designee of such unsatisfactory performance or breach, _________ may terminate the Contract at any time following the 30-day written notice period. Said termination shall occur without penalty to _________, including loss of projected profits to Consultant. Consultant shall remain liable to _________ for any damages caused to _________ due to Consultant's unsatisfactory performance or breach of contract.

4.2 In the event of termination for unsatisfactory performance or breach of contract by Consultant, Consultant shall continue its performance under the terms and conditions of this Contract until such time written notification is received by Consultant from _________ authorizing Consultant to "Stop Work."

4.3 Effect of Termination on Compensation. Termination of this Contract shall not relieve either party of its obligation to pay amounts due, or to give any credit due, for services rendered prior to the effective date of a breach of contract or termination. The _________ shall pay Consultant for undisputed amounts for services performed up to the time of termination.

5. **General Provisions**

5.1 Damages for Breach of Contract. In the event of a breach of this Contract by Consultant resulting in damages to _________, _________ shall be entitled to reasonable attorney's fees and costs incurred by _________, in addition to all other damages which _________ is legally entitled to recover.

6. **Force Majeure**. In the event performance of this Contract, or any obligation hereunder, is prevented, restricted, or interfered with by reason of acts of God or of the public enemy, acts of the Government in its sovereign capacity, fires, floods, epidemic, strikes, picketing or boycotts, or any other circumstances caused by natural occurrences or third-party actions beyond the reasonable control and without the fault or negligence of the party whose performance is affected, the party so affected, upon giving prompt notice to the other party, shall be excused from such performance on a day-to-day basis to the extent of such prevention, restriction or interference (and the other party shall likewise be excused from performance of its obligations on a day-to-day basis until the delay, restriction or interference has ceased), provided, however, that the party so affected shall use its best reasonable efforts to avoid or remove such causes of nonperformance and both parties shall proceed whenever such causes are removed or cease. This Paragraph 6 shall not prevent _________ from exercising its options under any other provisions of this Contract.

7. **Assignment**. All terms and provisions of this Contract shall be binding upon and inure to the benefit of the parties hereto and their successors and permitted assigns, including successors by reason of amalgamation or other corporate merger or reorganization. Neither party may assign this Contract or assign or delegate its obligations under this Contract without the prior written consent of the other party.

8. **Waiver**. No waiver of the terms of this Contract or failure by either party to this Contract to exercise any option, right, or privilege on any occasion or through the course of dealing shall be construed to be a waiver of any subsequent breach or of any option, right, or privilege on any subsequent occasion.

9. **Modifications**. In order to become binding on the parties and constitute a modification of this Contract, all changes to the Deliverables and/or Services provided by Consultant shall be set forth in a written agreement, in the form of an amendment to this Contract, signed by an authorized representative of both Parties in advance of receipt of the Deliverables or the services required by the changes. All such modifications shall specify any associated price or adjustment of the price, and any modification to any associated delivery date.

10. **Payment of Invoices**.

10.1 This assessment is for a _________________________________ All payments to Consultant shall be for services rendered and/or deliverables received, unless otherwise specifically provided herein under “Special Terms and Conditions.”

Payment Address:
True North Consulting Group
P.O. Box 2169
Hewitt, TX 76643
Attention: Accounts Payable

Invoices shall be submitted as follows:
________________________
________________________
________________________
Attention: Accounts Payable

10.2 Invoices, at a minimum, shall reflect and/or comply with the following for each level of service billed:

(a) Contract Number and Purchase Order Number;

(b) Invoice shall be itemized and transportation charges, if allowed by the Contract, shall be listed separately;

(c) Taxes must be shown separately on the invoice. Do not include federal or state taxes or any taxes for which _________ is exempt.

11. **Disputes**. In the event of any dispute concerning a question of law or fact, or both, arising under the Contract, which the parties are unable to resolve by mutual agreement, either party may pursue any right or remedy which it may have at law or in equity in a court of competent jurisdiction in McLennan County, Texas. There shall be no interruption in the prosecution of the work, and Consultant shall proceed diligently with the performance of this Contract pending final resolution of any dispute, claim, or final litigation arising under or related to this Contract between the parties hereto.

12. **Governing Law**. This Contract shall be governed by and interpreted or construed in accordance with the laws of the State of Texas and shall be subject to the exclusive jurisdiction of the courts therein. Venue for any court action brought by either party under this Contract shall remain exclusively in McLennan County, Texas.

13. **Publicity**. Consultant shall not use in advertising or publicity or other public disclosure the _________’s name for purposes of listing _________ as Consultant’s client without the prior written approval of _________.

14. **Conflicts of Interest**. Neither party shall pay any commissions or fees or grant any rebates to any employee or officer of the other party under this Contract, without the other party’s prior written approval.

15. **Compliance with Equal Employment Opportunity Regulations**. Consultant shall not discriminate in the performance of this Contract based on race, color, religion, sex, or national origin unless the characteristic is a bona fide occupational qualification for performance under it.

16. **Sexual Harassment**. All employees, agents, and personnel of Consultant having access to the _________'s premises shall fully comply with the policy of the _________ to provide a work environment free from all forms of sexual harassment.

17. **Copyrights and Patents**. In the event Consultant develops materials or products resulting in a copyright or patent related to the performance of this Contract, the interest in copyright shall vest in the _________, unless otherwise agreed to in writing by the parties.

18. **Notices**. All notices or other communications required or permitted to be made or given hereunder by one party to the other party shall be in writing and shall be deemed to have been given when hand-delivered with a signed receipt of the party being notified or when sent by certified mail, regardless of whether or not received, on the third (3rd) business day of the party being notified after deposit in the United States mail, postage prepaid, with return receipt requested, and, in all cases, properly addressed to such other party as set forth below or at such other address as may be specified by either party hereto by written notice sent or delivered in accordance with the terms hereof:

| | *Mailed* | *Hand-Delivered* |
|---|---|---|
| _________: | ________________<br>________________<br>________________ | SAME |
| *Consultant:* | True North Consulting Group<br>140 Third Street South<br>Stillwater, MN 55082<br>Attention: Rick Anderson | True North Consulting Group<br>140 Third Street South<br>Stillwater, MN 55082<br>Attention: Rick Anderson |

19. **Security and Acceptable Use**. Consultant agrees that it and its personnel, while on _________ premises, shall fully comply with the security regulations in effect at such facility, and shall fully comply with all restrictions and regulations relating to any data system utilized at such facility. Failure of Consultant to comply with _________'s security regulations and/or acceptable use policy shall be a cause for immediate termination of this Contract and shall be in addition to _________'s termination options under Paragraph 4 of this Contract.

20. **Severability**. If any term, provision, covenant, or condition of this Contract is held by a court or regulatory body of competent jurisdiction to be invalid, void, or unenforceable, the rest of the Contract shall remain in full force and effect and shall in no way be affected, impaired, or invalidated.

21. **Retention of and Access to Records**. Consultant shall retain all books, documents, papers, and records that are directly pertinent to the Contract. Consultant shall make said materials available for audit, examination, excerpt, and transcription to the _________, sub-grantee or grantee of funds, or their authorized representatives for a period of at least seven (7) years following termination of the Contract.

22. **Reimbursable Travel Expenses**. Not applicable to this project as this is a "Firm Fixed-Price" Contract.

23. **Contract Term.** ____________________ unless extended by the _________ for additional services.

24. **List of Documents Incorporated**

The following documents are hereby incorporated in and made a part of this Contract, and Consultant hereby acknowledges receipt of a copy of each such document, to-wit:

(a) ____________________________
(b) ____________________________

In the event of a conflict in the terms and conditions, the terms of this Contract shall have first priority, the terms of the RFP listed in (a) above shall have second priority, and the terms of the Consultant's proposal listed in (b) above shall have last priority.

25. **Authority**. Each party has full power and authority to enter into, perform, and execute this Contract, and each person signing this Contract on behalf of either party has been properly authorized and empowered to enter into and execute this Contract. Each party further acknowledges that it has read this Contract, understands it, and agrees to be bound by it.

26. **Special Terms and Conditions**. Payment for the project is net 30 days from date of completion and acceptance by _________ for services provided as outlined in RFP and response by True North Consulting Group.

27. **Entire Agreement.** Except for written amendments, supplements, or modifications made after the execution of this Contract, this Contract represents the entire agreement between the parties with respect to the subject matter of this Contract and supersedes all prior negotiations, representations, and agreements, either oral or written.

28. **No Waiver**. By entering into this Contract, the _________ is not waiving any governmental or sovereign immunities provided to the _________ under law.

**IN WITNESS WHEREOF**, the parties have executed this Contract on the date or dates indicated below to be effective as of the date specified above.

**TRUE NORTH CONSULTING GROUP, LLC**

By: ____________________________________
(Signature)

Name: ____________________________________
(Print)

Title: ____________________________________

Date: ____________________________________

________________________________________

By: ____________________________________
(Signature)

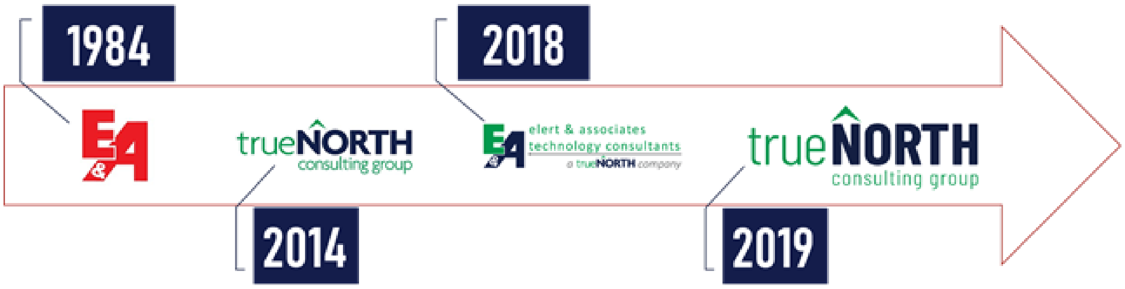
Name: ____________________________________
(Print)

Title: ____________________________________

Date: ____________________________________

## PART 4

### Company Background


1984
E&A
trueNORTH consulting group
2014
2018
E&A elert & associates technology consultants a trueNORTH company
trueNORTH consulting group
2019

True North Consulting Group (True North/TNCG) was founded from the Texas Division of Elert & Associates (E&A), a 37-year-old independent technology consulting firm headquartered in Stillwater, MN. True North is based in Texas and has seamlessly continued to maintain E&A-Texas client accounts and to serve most states in the southern part of the country. In 2018, True North Consulting Group and Elert & Associates merged and became one company – True North Consulting Group. True North now includes a consulting staff of 45+ specialists.

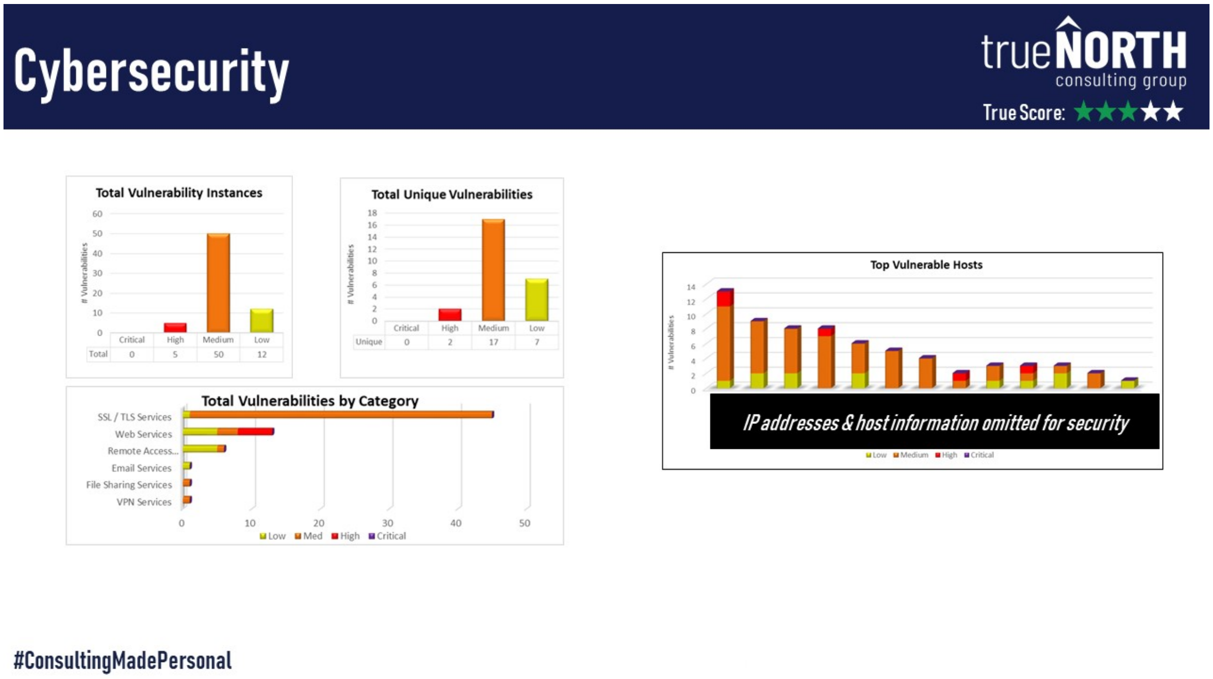
TNCG has assisted well over 1,500 public- and private-sector clients improve their assessment needs for the past 37 years. We provide cybersecurity, vulnerability assessments, penetration testing, IT information technology plans, PCI, SCADA Compliance, and security program development and planning. Executives are IT industry veterans who possess both subject matter technical expertise and extensive experience in managing large-scale projects.

Since 1984, TNCG has been providing managed services, assessing security controls, performing technical vulnerability assessments, and on-site consulting services related to clients' IT infrastructure, information systems, and applications security. Our highly experienced security professionals utilize automated tools followed by thorough manual testing for verification and exploitation/escalation of identified potential vulnerabilities. All tests follow a pre-approved test plan, and client representatives are encouraged to witness the testing process. Our findings are meticulously documented in our Assessment Report.

We are confident that the combination of our vast experience in conducting technical security vulnerability assessments, our executives' direct and practical approach, our staff's strong technical qualifications, our focus on IT Security, Cybersecurity services, and our meticulous project management and operations expertise will help the Erie County Water Authority achieve a stronger security posture based on the performance of the activities described in this proposal.

TNCG is an IT consulting firm that focuses on cybersecurity and physical security. Unlike other companies where information security may just be one area in a large portfolio of services, for us, it is one of our specialties. Virtually 100% of our client engagements are related to security applications. TNCG is an innovative leader in IT services, specializing in networking and information systems security consulting for state and local organizations as well as commercial entities. TNCG focuses on helping clients meet their network infrastructure and information security goals by establishing close working relationships and mapping clients' goals and mission requirements to proven solutions. At all times, TNCG maintains an awareness of clients' established policies and procedures and ensures that all our work efforts are compliant with government regulations and corporate industry best practices.

Often overlooked and ignored, we conduct internal and external security vulnerability tests to evaluate cyber threats, risks, and vulnerabilities to the organization.



Cybersecurity

trueNORTH consulting group

True Score: ★★★★★

Total Vulnerability Instances

|  | Critical | High | Medium | Low |
|---|---|---|---|---|
| Total | 0 | 5 | 50 | 12 |

Total Unique Vulnerabilities

|  | Critical | High | Medium | Low |
|---|---|---|---|---|
| Unique | 0 | 2 | 17 | 7 |

Total Vulnerabilities by Category

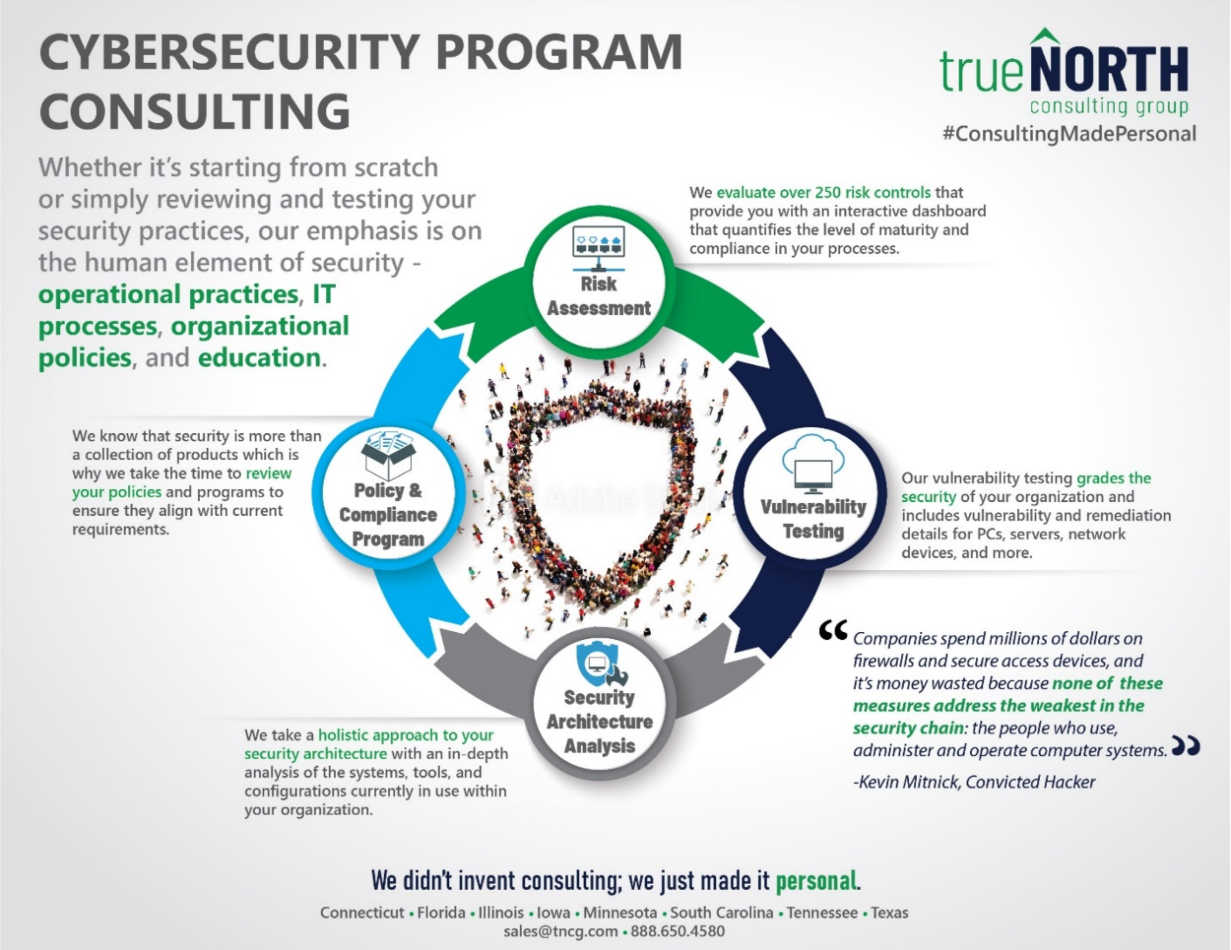
Top Vulnerable Hosts

*IP addresses & host information omitted for security*

#ConsultingMadePersonal

***Experience***

As an independent consulting firm, it comes as no surprise that our approach to security is not centered around purchasing more security tools. Frankly, many organizations have too many tools, leading to a false sense of security and tying up valuable resources that could be more effectively used for developing stronger operational practices, IT processes, organizational policies, and education.



CYBERSECURITY PROGRAM CONSULTING

trueNORTH consulting group

#ConsultingMadePersonal

Whether it's starting from scratch or simply reviewing and testing your security practices, our emphasis is on the human element of security - **operational practices**, **IT processes**, **organizational policies**, and **education**.

We evaluate over 250 risk controls that provide you with an interactive dashboard that quantifies the level of maturity and compliance in your processes.

Our vulnerability testing grades the security of your organization and includes vulnerability and remediation details for PCs, servers, network devices, and more.

We take a holistic approach to your security architecture with an in-depth analysis of the systems, tools, and configurations currently in use within your organization.

We know that security is more than a collection of products which is why we take the time to review your policies and programs to ensure they align with current requirements.

> *"Companies spend millions of dollars on firewalls and secure access devices, and it's money wasted because **none of these measures address the weakest in the security chain**: the people who use, administer and operate computer systems."*
>
> *-Kevin Mitnick, Convicted Hacker*

We didn't invent consulting; we just made it personal.

Connecticut • Florida • Illinois • Iowa • Minnesota • South Carolina • Tennessee • Texas
sales@tncg.com • 888.650.4580

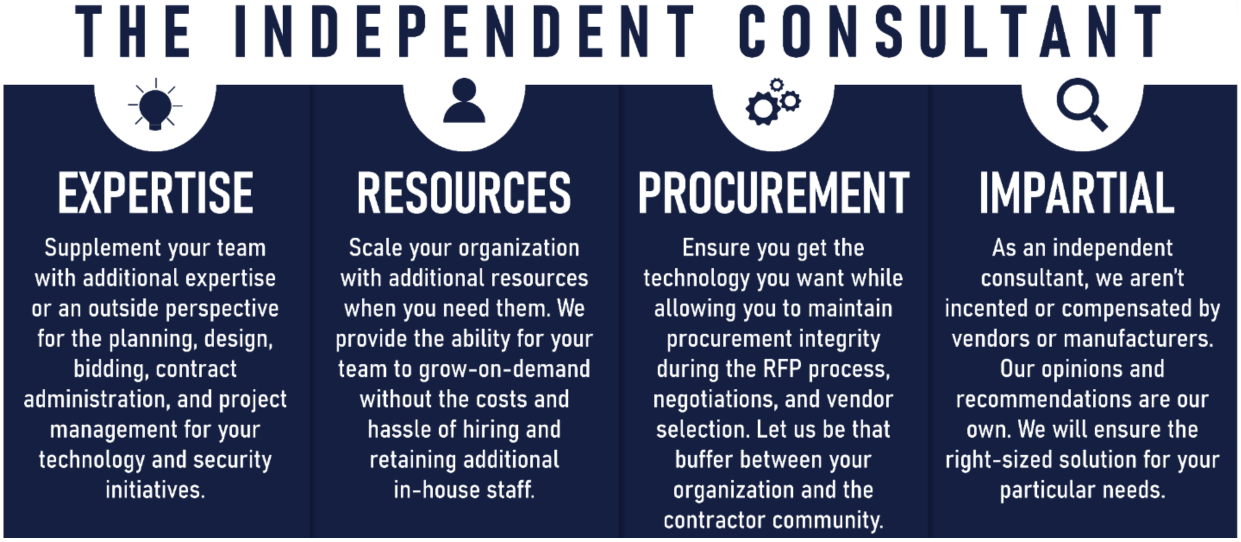
True North has cybersecurity and IT professionals on staff and supplements in-house resources as necessary or required for specialized expertise or additional capacity. TNCG offers consulting services for Information Technology, Cybersecurity, Physical Security, and Construction, focusing on public entities such as K12, Higher Education, City, County, and State Government. TNCG has performed work for organizations nationwide. TNCG excels in areas such as strategy, budgeting, programming, assessments, design, BIM/CAD, and contract administration across all business areas. TNCG acts as an unbiased third-party to assist clients with short-, mid-, and long-term goals and service execution strategies.

## Certifications

| | |
|---|---|
| CCNA | Cisco Certified Network Associate, Routing and Switching |
| CCNP R&S | Cisco Certified Network Professional, Routing and Switching |
| CCNP Voice | Cisco Certified Network Professional, Voice |
| CCNP Security | Cisco Certified Network Professional, Security |
| CCDP | Cisco Certified Design Professional |
| CISA | Certified Information Systems Auditor |
| CISM | Certified Information Security Manager |
| CISSP | Certified Information Systems Security Professional (ISC2) |
| CPP | Certified Protection Professional (ASIS) |
| CRISC | Certified in Risk and Information System Controls (ISACA) |
| CEH | Certified Ethical Hacker (EC-Council) |
| CTS | Certified Technology Specialist |
| CTS-D | Certified Technology Specialist - Design |
| ECSE | Ekahau Certified Survey Engineer |
| ENP | Emergency Number Professional (NENA) |
| GIAC | Global Information Assurance Certifications |
| | (a) Security Essentials Certification (GSEC) |
| | (b) Certified Intrusion Analyst (GCIA) |
| | (c) Certified Enterprise Defender (GCED) |
| | (d) Certified Windows Security Administrator (GCWSA) |
| | (e) Certified Defensible Security Architecture (GDSA) |
| | (f) Certified Detection Analyst (GCDA) |
| | (g) Certified Defending Advanced Threats (GDAT) |
| | (h) Certified Information Security Professional (GISP) |
| | (i) Certified Strategic Planning, Policy, and Leadership (GSTRT) |
| | (j) Certified Incident Handler (GCIH) |
| LEED AP | Leadership in Energy and Environmental Design, Accredited Professional |
| PMP | Project Management Professional (PMI) |
| PSP | Physical Security Professional (ASIS) |
| RA | Registered Architect (Texas) |
| RCDD | Registered Communications Distribution Designer (BICSI) |
| RCCD/OSP | Outside Plant Specialist (BISCI) |
| RTPM | Registered Telecommunication Project Manager (BISCI) |
| SC-SDT | Security Center System Design Training (IP Video and Card Access) |
| USGBC | U.S. Green Building Council Membership |

FCC General Class Radiotelephone License
HIPAA Academy Certified
Microsoft Security Competency
SCADA Certified

**Customer Support**



## THE INDEPENDENT CONSULTANT

### EXPERTISE

Supplement your team with additional expertise or an outside perspective for the planning, design, bidding, contract administration, and project management for your technology and security initiatives.

### RESOURCES

Scale your organization with additional resources when you need them. We provide the ability for your team to grow-on-demand without the costs and hassle of hiring and retaining additional in-house staff.

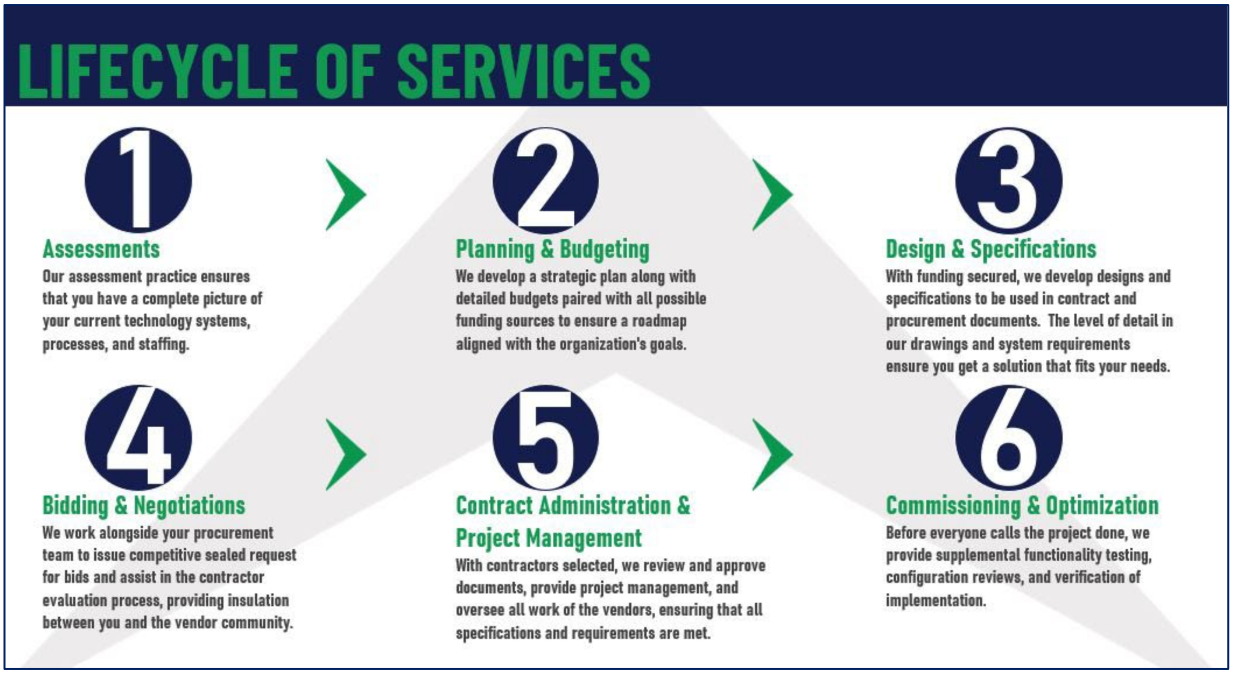
### PROCUREMENT

Ensure you get the technology you want while allowing you to maintain procurement integrity during the RFP process, negotiations, and vendor selection. Let us be that buffer between your organization and the contractor community.

### IMPARTIAL

As an independent consultant, we aren't incented or compensated by vendors or manufacturers. Our opinions and recommendations are our own. We will ensure the right-sized solution for your particular needs.

With hundreds of years of combined experience in technology and security, our processes have evolved alongside the industry. True North is a mature consulting firm that has the advantage of being able to look back over our prior experiences to help shape and guide what tomorrow’s processes and systems should look like.



## LIFECYCLE OF SERVICES

1 **Assessments**
Our assessment practice ensures that you have a complete picture of your current technology systems, processes, and staffing.

2 **Planning & Budgeting**
We develop a strategic plan along with detailed budgets paired with all possible funding sources to ensure a roadmap aligned with the organization's goals.

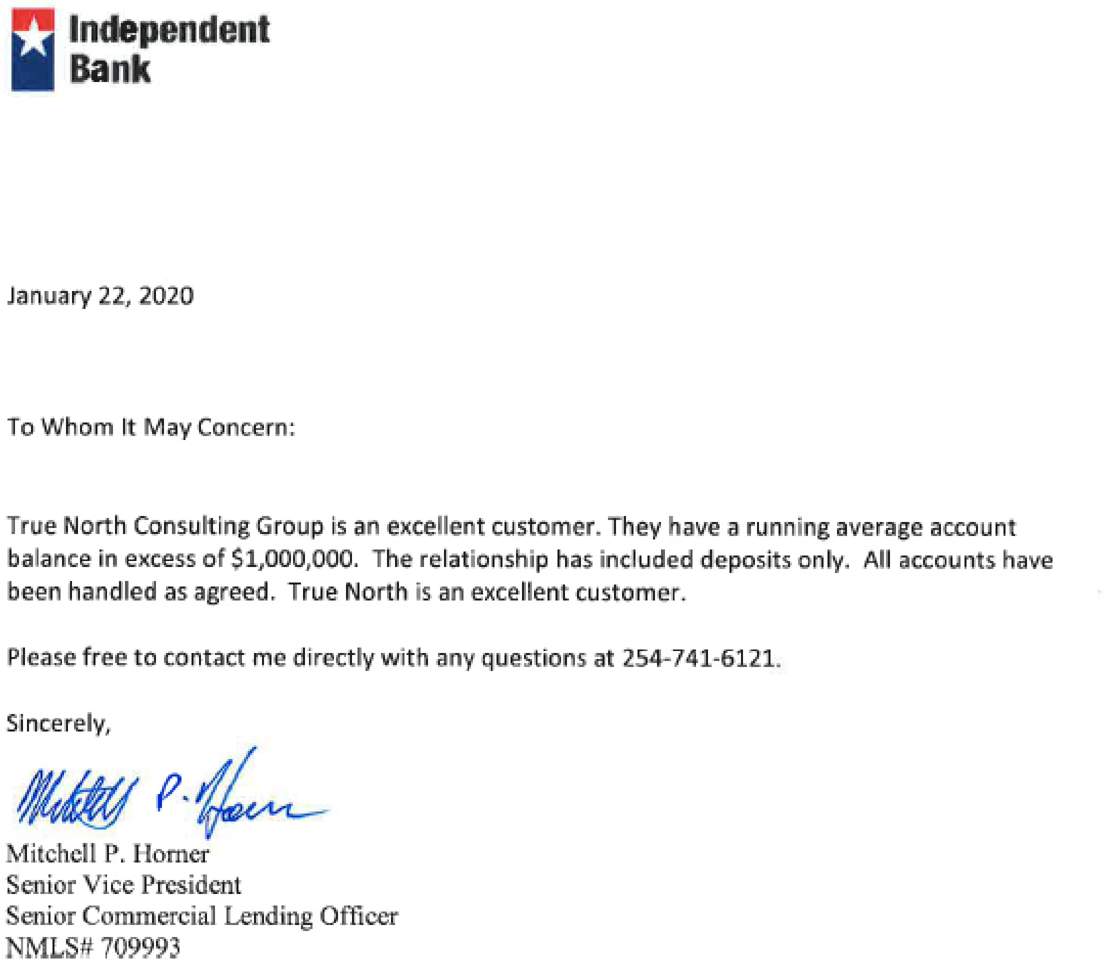
3 **Design & Specifications**
With funding secured, we develop designs and specifications to be used in contract and procurement documents. The level of detail in our drawings and system requirements ensure you get a solution that fits your needs.

4 **Bidding & Negotiations**
We work alongside your procurement team to issue competitive sealed request for bids and assist in the contractor evaluation process, providing insulation between you and the vendor community.

5 **Contract Administration & Project Management**
With contractors selected, we review and approve documents, provide project management, and oversee all work of the vendors, ensuring that all specifications and requirements are met.

6 **Commissioning & Optimization**
Before everyone calls the project done, we provide supplemental functionality testing, configuration reviews, and verification of implementation.

## Financial Condition



Independent Bank

January 22, 2020

To Whom It May Concern:

True North Consulting Group is an excellent customer. They have a running average account balance in excess of $1,000,000. The relationship has included deposits only. All accounts have been handled as agreed. True North is an excellent customer.

Please free to contact me directly with any questions at 254-741-6121.

Sincerely,

Mitchell P. Horner
Senior Vice President
Senior Commercial Lending Officer
NMLS# 709993

## Sample Report

Please see Team TNCG's sample report on the following pages.

REDACTED

# Application and Infrastructure Risk Assessment

February 19, 2018

***Submitted to:***

REDACTED

**Report Submitted by:**

True North Consulting Group

FOR OFFICIAL USE ONLY - CONFIDENTIAL

# TABLE OF CONTENTS

**1. EXECUTIVE SUMMARY** .......... 9

1.1 SUMMARY OF VULNERABILITIES .......... 10

1.2 SUMMARY OF RECOMMENDATIONS .......... 12

**2. TESTING APPROACH** .......... 13

2.1 TESTING SCOPE AND METHODOLOGY .......... 13

*2.1.1 Infrastructure Vulnerability Testing* .......... *13*

*2.1.2 Web Application Scanning and Manual Testing* .......... *16*

*2.1.3 Code Review* .......... *17*

2.2 TOOLS USED .......... 17

**3. SECURITY TESTING DETAILS** .......... 19

3.1 INFRASTRUCTURE TESTING .......... 19

3.2 WEB APPLICATION SCANNING AND MANUAL TESTING .......... 20

*3.2.1 REDACTED* .......... *21*

*3.2.2 REDACTED* .......... *22*

*3.2.3 REDACTED* .......... *24*

*3.2.4 REDACTED* .......... *24*

*3.2.5 Applications Not Requiring Authentication* .......... *25*

3.3 CODE REVIEW .......... 26

*3.3.1 High Severity Finding* .......... *26*

*SQL Injection- Systemic* .......... *26*

*Cross Site Scripting (XSS)- Systemic* .......... *30*

*Cross Site Request Forgery (CSRF)* .......... *32*

*Insecure Direct Object References- Systemic* .......... *34*

*Failure to Restrict URL Access- Systemic* .......... *36*

*3.3.2 Medium Severity Findings* .......... *38*

*Open URL Redirection* .......... *38*

*Trust Boundary Violation- Systemic* .......... *39*

*Unencrypted ASP.NET ViewState* .......... *40*

*Username Enumeration* .......... *41*

*Weak Password Policy* .......... *42*

*Denial of Service Via Disk Storage Exhaustion* .......... *43*

*Log Files Are Publicly Accessible* .......... *44*

*Privileged Database SA Account In Use* .......... *45*

*Unsalted Password Hashes* .......... *46*

*Browser Caches Sensitive Information* .......... *47*

*Insecure Test Code Present* .......... *49*

*3.3.3 Low Severity Findings* .......... *50*

*Verbose Error Messages*......50
*Cookies Not Marked Secure*......51
*Cookie HTTPOnly Flag Not Set*......52
*Plain Text Passwords in Configuration Files*......53
*Browser Autocomplete Enabled*......55
*Sensitive Information Sent Via HTTP GET*......56
*Site Lacks ClickJacking Defense*......57
*HTTP Response Contains Plain Text Credentials*......58
*Sensitive Information Logged*......59
*Lack of Account Lockout*......60

**4. RISK ASSESSMENT**......61

**5. MAJOR FINDINGS AND RECOMMENDATIONS**......62

**6. GUIDE TO VULNERABILITY MATRIXES**......65

5.1 THREAT(S) AGAINST THE SYSTEM......65
5.2 TECHNICAL AND OPERATIONAL VULNERABILITIES......65
5.3 MITIGATING SECURITY CONTROLS (TECHNICAL, PROCEDURAL)......66
5.4 LIKELIHOOD OF SUCCESSFUL EXPLOITATION......66
5.5 IMPACT ON MISSION......66

**APPENDIX A: SERVICES MATRIX**......67

**APPENDIX B: WEB APPLICATION VULNERABILITIES MATRIX**......68

**APPENDIX C: CODE REVIEW VULNERABILITY MATRIX**......69

**APPENDIX D: SERVER VULNERABILITY MATRIX**......70

**APPENDIX E: DATABASE VULNERABILITY MATRIX**......71

**APPENDIX F: PLANS OF ACTION AND MILESTONES**......72

**APPENDIX G: SCREEN CAPTURES**......73

**APPENDIX H: RAW DATA RESULTS**......74

# LIST OF FIGURES

FIGURE 1: SUMMARY OF RISK RATINGS ........ 11

FIGURE 2: TNCG TESTING METHODOLOGY ........ 15

FIGURE 3: NMAP SCAN ON THE DATABASE SERVER ........ 19

FIGURE 4: REDACTED MENU HAS CERTAIN SELECTIONS FOR ADMINISTRATORS ONLY ........ 21

FIGURE 5: BY MANUALLY MAKING A GET REQUEST A NORMAL USER CAN ACCESS ADMIN FUNCTIONS.... 22

FIGURE 6: ERROR MESSAGE DISPLAYED THAT WEB SCANNERS INTERPRETED AS SQL INJECTION ........ 22

FIGURE 7: ERROR MESSAGE INDICATES THAT SQL INJECTION MAY BE POSSIBLE ........ 22

FIGURE 8: REDACTED LOGIN PAGE ........ 23

FIGURE 9: ADD A SINGLE QUOTE TO THE LOGTYPE PARAMETER CAUSES A SQL ERROR ........ 23

FIGURE 10: DATABASE ERROR MESSAGE INDICATES THAT SQLI MAY BE POSSIBLE ........ 23

FIGURE 11: THE CBOEEDOBMO PARAMETER IS TAMPERED WITH TO ADD SCRIPTING LANGUAGE TO CAUSE THE BROWSER TO VISIT A THIRD-PARTY SITE ........ 23

FIGURE 12: THE FIGURE ABOVE SHOWS THE USER BEING REDIRECTED TO A THIRD-PARTY SITE ........ 23

FIGURE 13: THE XSS IS EXECUTED IN THE RETIREMENT PLANNER PORTION OF THE APPLICATION ........ 23

FIGURE 14: SIMILAR VULNERABILITY EXISTED IN THE ADMINISTRATOR USER LOG FUNCTIONALITY ........ 23

FIGURE 15: REDACTED APPLICATIONS ........ 24

FIGURE 16: VIEWSTATE ERROR MESSAGE WHEN ATTEMPTING TO MODIFY PARAMETERS ........ 24

FIGURE 17: XSS IS ENTERED INTO THE POST REQUEST USING BURP ........ 24

FIGURE 18: XSS IS EXECUTED ........ 24

FIGURE 19: GENERIC ERROR MESSAGE ........ 25

FIGURE 20: SPECIAL CHARACTERS WERE NOT ALLOWED ........ 25

FIGURE 21: VIEWSTATE ENCRYPTION IS NOT BEING UTILIZED ........ 25

FIGURE 22: XSS IS ENTERED INTO THE POST REQUEST ........ 26

FIGURE 23: THE XSS IS EXECUTED AND COOKIE INFORMATION IS DISPLAYED ........ 26

FIGURE 24: ENTERING A SINGLE QUOTE TO THE TXT_YEAR PARAMETER CAUSES A DATABASE ERROR MESSAGE ........ 26

FIGURE 25: BURP IS USED TO PERFORM SQLI TO DISPLAY THE DATABASE VERSION ........ 26

FIGURE 26: THE VERSION INFORMATION IS DISPLAYED SHOWING THAT THE SQLI WAS SUCCESSFUL ........ 26

FIGURE 27: THE SQLSTRINGFIX METHOD WITHIN THE REDACTED RESOURCE ........ 28

FIGURE 28: THE SQLSTRINGFIX METHOD BEING RUN AGAINST THE SQLSSN STRING ........ 28

FIGURE 29: SQL INJECTION OCCURRING WHEN THE USER INPUT IS PLACED INTO A STATEMENT UTILIZING STRING CONCATENATION ........ 28

FIGURE 30: USER INPUT BEING STORED WITHIN A SESSION VARIABLE IN THE REDACTED CLASS ........ 28

FIGURE 31: THE USER INPUT CONTAINED IN THE SESSION VARIABLE IS USED TO DYNAMICALLY CREATE A SQL STATEMENT ........ 29
FIGURE 32: USER INPUT BEING REFLECTED BACK WITHIN A RESPONSE WITHOUT PERFORMING HTML ENCODING ON THE DATA, ALLOWING FOR SCRIPT EXECUTION ........ 30
FIGURE 33: THE USER INPUT IS LATER REFLECTED WHEN THE HTML BODY IS LOADED ........ 30
FIGURE 34: REQUEST.QUERYSTRING VALUE USED WITHIN THE PAGE_LOAD METHOD WITHOUT OUTPUT ENCODING OR MODIFICATION IN THE REDACTED CLASS ........ 31
FIGURE 35: A FORM SUBMISSION TO AN ADMINISTRATIVE FUNCTION WITHIN REDACTED'S CODE ........ 32
FIGURE 36: A FORM SUBMISSION WITHIN REDACTED IN THE REDACTED CODE ........ 32
FIGURE 37: REDACTED CLASS WHERE THE SERVER SIDE APPLICATION BLINDLY ACCEPTS ARBITRARY VALUES REPRESENTING REDACTED THAT A USER MAY NOT BE ASSIGNED TO ........ 34
FIGURE 38: EXAMPLE OF AN ADMINISTRATIVE RESOURCE IN REDACTED BEING ACCESSED WITHOUT AN ACCESS CONTROL CHECK WITHIN THE PAGE_LOAD METHOD ........ 36
FIGURE 39: EXAMPLE OF A REDIRECTION FUNCTION WITHIN REDACTED ........ 38
FIGURE 40: A USER SUBMITTED VALUE BEING COPIED INTO A SESSION VARIABLE WITHIN REDACTED AND THE REDACTED CODE ........ 39
FIGURE 41: EXAMPLE WITHIN THE REDACTED APPLICATION'S REDACTED CLASS ........ 39
FIGURE 42: THE REDACTED CLASS WITHIN REDACTED RETURNS SEVERAL DIFFERENT MESSAGES DEPENDING UPON THE ACCOUNT'S STATUS AND THE INFORMATION PROVIDED BY THE REMOTE USER ........ 41
FIGURE 43: REDACTED PASSWORD VALIDATOR THAT DOES NOT ALLOW SPECIAL CHARACTERS TO BE USED ........ 42
FIGURE 44: LOG ROTATION FUNCTION WITHIN REDACTED THAT USES THE PRIMARY C: DRIVE ........ 43
FIGURE 45: LOG FILE BEING STORED TO A WEB ACCESSIBLE DIRECTORY WITHIN REDACTED. ........ 44
FIGURE 46: THE WEB.CONFIG FILE FOR THE REDACTED APPLICATION ........ 45
FIGURE 47: A PASSWORD BEING MD5 HASHED WITHOUT A SALT WITHIN THE REDACTED CLASS ........ 46
FIGURE 48: THE BASEPAGE.MD5ENCRYPT(STRING) METHOD THAT DOES NOT UTILIZE A SALT ........ 46
FIGURE 49: TEST CODE WITHIN REDACTED IN THE REDACTED CLASS THAT IS VULNERABLE TO XSS. ........ 49
FIGURE 50: WEB.CONFIG FILE FOR REDACTED THAT TURNS CUSTOM ERRORS OFF AND ENABLES VERBOSE ERRORS TO BE RENDERED ........ 50
FIGURE 51: THE DATABASE CONNECTION STRING WITHIN REDACTED, STORED IN PLAIN TEXT WITHIN THE WEB.CONFIG FILE ........ 53
FIGURE 52: SOCIAL SECURITY NUMBER (PIN) SENT WITHIN AN HTTP GET REQUEST WITHIN THE REDACTED APPLICATION ........ 56
FIGURE 53: THE USER'S PASSWORD DISPLAYED WITHIN AN HTTP RESPONSE ........ 58
FIGURE 54: SOCIAL SECURITY NUMBERS BEING LOGGED IN PLAIN TEXT ........ 59
FIGURE 55: REDACTED'S LOGIN FUNCTION DOES NOT LOCK A USER'S ACCOUNT AT THE SERVER ........ 60

# LIST OF TABLES

TABLE 1: SYSTEM INVENTORY ........ 13
TABLE 2: APPLICATION INVENTORY ........ 16
TABLE 3: VULNERABILITY ASSESSMENT TOOLS ........ 18
TABLE 4: SQL INJECTION ........ 26
TABLE 5: XSS ........ 30
TABLE 6: CSRF ........ 32
TABLE 7: INSECURE DIRECT OBJECT REFERENCES ........ 34
TABLE 8: FAILURE TO RESTRICT URL ACCESS ........ 36
TABLE 10: OPEN URL REDIRECTION ........ 38
TABLE 11: TRUST BOUNDARY VIOLATION ........ 39
TABLE 12: UNENCRYPTED VIEWSTATE ........ 40
TABLE 13: USERNAME ENUMERATION ........ 41
TABLE 14: WEAK PASSWORD POLICY ........ 42
TABLE 15: DENIAL OF SERVICE VIA DISK STORAGE EXHAUSTION ........ 43
TABLE 16: LOG FILES ARE PUBLICLY ACCESSIBLE ........ 44
TABLE 17: PRIVILEGED DATABASE SA ACCOUNT IN USE ........ 45
TABLE 18: UNSALTED PASSWORD HASHES ........ 46
TABLE 19: BROWSER CACHES SENSITIVE INFORMATION ........ 47
TABLE 20: INSECURE TEST CODE PRESENT ........ 49
TABLE 21: VERBOSE ERROR MESSAGES ........ 50
TABLE 22: COOKIES NOT MARKED SECURE ........ 51
TABLE 23: COOKIE HTTPONLY FLAG NOT SET ........ 52
TABLE 24: PLAIN TEXT PASSWORDS IN CONFIGURATION FILES ........ 53
TABLE 25: BROWSER AUTOCOMPLETE ENABLED ........ 55
TABLE 26: SENSITIVE INFORMATION SENT VIA HTTP GET ........ 56
TABLE 27: SITE LACKS CLICKJACKING DEFENSE ........ 57
TABLE 28: HTTP RESPONSE CONTAINS PLAIN TEXT CREDENTIALS ........ 58
TABLE 29: SENSITIVE INFORMATION LOGGED ........ 59
TABLE 30: LACK OF ACCOUNT LOCKOUT ........ 60
TABLE 31: RISK ASSESSMENT ........ 61
TABLE 32: SERVICES MATRIX ........ 67
TABLE 33: WEB APPLICATION VULNERABILITIES MATRIX ........ 68
TABLE 34: CODE REVIEW VULNERABILITY MATRIX ........ 69
TABLE 35: SERVER VULNERABILITY MATRIX ........ 70

TABLE 36: DATABASE VULNERABILITY MATRIX ........ 71
TABLE 37: REDACTED POA&MS........ 72
TABLE 38: SCREEN CAPTURE DOCUMENT ........ 73

# Revision History/Change Record

| Date | Description | Version | Author |
|---|---|---|---|
| 1/18/2018 | Draft Report | 1.0 | True North Consulting Group |
| 2/11/2018 | Draft Report Updated Based on REDACTED Comments | 1.1 | True North Consulting Group |
| 2/19/2018 | Final Report | 1.2 | True North Consulting Group |

# 1. EXECUTIVE SUMMARY

This report summarizes the activities, findings, and recommendations performed under the application and infrastructure risk assessment task, issued by the REDACTED (REDACTED) to True North Consulting Group Corporation (TNCG). All material presented in this report was derived independently based on scans, tests, reviews, and observations.

Under this contract, REDACTED tasked TNCG to conduct an application and infrastructure risk assessment to evaluate the level of security protecting their critical web applications. Previously REDACTED has had assessments performed that identified vulnerabilities in their web applications; however, this is the first time that an in-depth review was performed on the applications.

After completion of the testing and other evaluation activities, it is TNCG's overall opinion that the implementation and management of the technical security architecture supporting the REDACTED web applications requires some strengthening in order to more effectively restrict unauthorized access. Throughout the performance of the application assessment, TNCG discovered that REDACTED has effectively implemented multiple controls for protecting application resources. However, several areas were identified where improvements in the application security architecture could further enhance REDACTED's security posture.

Like any other enterprise, REDACTED will always face new security challenges and the need for continuous improvement.

Under this project, TNCG performed comprehensive tests covering certain components of REDACTED's web application infrastructure spectrum:

- **Web Application Assessment** – attempting to break in from the public Internet
- **Code Review** – identifying vulnerabilities within application source code and assessing their root cause
- **Infrastructure Assessment** – Nmap and Nessus scan on servers to evaluate the degree of standardization to industry best practices. Also included security vulnerabilities in databases and evaluation of the router/switch and firewall configuration for conformance with industry best practices

The majority of the activities described in this report took place between October 13th and December 26th of 2018. All testing activities were conducted externally with coordination and assistance from the REDACTED IT staff. Initially, a test plan was developed and test activities were coordinated with the REDACTED IT and Security teams. Once the test plan was approved, TNCG began the assessment.

The infrastructure was primarily assessed by performing Nmap and Nessus scans on the database and web server both from internal and external perspectives. Externally, only ports 80 and 443 were open. Internally, the port scans showed that the majority of open services were required for business purposes; however, there were a few that should be investigated. The Nessus scans did discover some vulnerabilities with the server components mainly in patch levels of both Microsoft and third-party patches. Database scans were also performed using AppDetective and the results show that while there are some issues that need to be addressed that the overall security posture of the database was fairly secure. The testing team also performed interviews with the REDACTED security team and reviewed the firewall configuration file. Perhaps one of the larger weaknesses in REDACTED's infrastructure is the fact that they rely on a third-party to perform all monitoring and intrusion detection on those components hosted at the REDACTED facility. While many organizations utilize third-parties to provide monitoring services it is imperative that the services provided meet REDACTED security objectives. From the evidence presented and observations made by the testing team we feel this is an area that can be strengthened. Items that could be implemented to improve this area include but are not limited to the following:

- SLA enforcing patching process and status
- Monthly patching reports
- Allowing REDACTED to conduct periodic unannounced security scans
- Providing REDACTED security scans to REDACTED so they can be entered into a SIEM or other product such as Core Insight.
- Security monitoring at the application level

Testing of the applications occurred in two phases; dynamic web application testing conducted on the staging environment using valid test accounts and a static code analysis portion where complete source code was provided to the testing team. The results from both phases identified similar issues. As expected the results of the static code analysis did identify a greater number of issues as the source code was provided. Vulnerabilities discovered included SQL injection, Cross-site Scripting (XSS), Cross-site Request Forgery (CSRF), privilege escalation, and password hashes not being salted for example. The majority of these vulnerabilities were a result of data not being correctly validated and other coding mistakes. These results show the need for the development of secure coding standards at REDACTED as well as additional developer security training.

Most of the discovered weaknesses can be addressed with minimal financial outlay, but they do require time and trained personnel.

The more serious vulnerabilities are discussed below; all other vulnerabilities appear in the body of the document and the appendices of this report.

## 1.1 Summary of Vulnerabilities

The major vulnerability trends that TNCG identified are the following:

- SQL Injection
- Reflective XSS
- Privilege Escalation
- Cross-site Request Forgery
- Weakness in application code
- Microsoft and third-party patches missing
- Open ports that should be reviewed

- Database settings that can be strengthened
- Intrusion detection and incident response need to be improved at the application layer

The graph below provides an overview of the risk levels noted during the assessment. For complete details on all discovered findings please see the Vulnerability Matrices located in the Appendix.

**Figure 1: Summary of Risk Ratings**

## 1.2 Summary of Recommendations

The summary of recommendations that TNCG proposes are the following:

- Fix the specific vulnerabilities identified in the application code
- Develop a secure coding standard to be followed by REDACTED developers
- Provide regular secure coding training to REDACTED developers
- Review the recommended database settings and verify that REDACTED is following an approved STIG for deployment.
- Analyze the patching process to identify root causes of missing patches.
- Review all services that are currently enabled and disable those services that are not needed.

Due to the dynamics of both REDACTED's application/IT infrastructure and the discovery of new vulnerabilities/exploits, this assessment should be viewed as a snapshot of potential vulnerabilities at this time. TNCG suggests that REDACTED perform vulnerability assessments on a regular basis to identify any new vulnerabilities and issues in its application infrastructure.

TNCG wishes to thank REDACTED and REDACTED for their assistance and expertise during these tests.

# 2. TESTING APPROACH

The information in this section describes the methodology that TNCG used when executing the tests, the applications and Internet Protocol (IP) address ranges that were examined, and the tools that were used.

## 2.1 Testing Scope and Methodology

TNCG produced a detailed test plan that contained the methodology and steps that would be taken to complete each task. A Rules of Engagement (ROE) that described what TNCG could and could not do during the testing was also developed. These documents were submitted to REDACTED in advance for approval. Upon approval of the test plan, the testing commenced. All testing was conducted in close coordination with the REDACTED security and IT teams.

The testing activities were divided into three major phases described below.

### *2.1.1 Infrastructure Vulnerability Testing*

**Objective**

The objective of the infrastructure assessment phase was to determine if there were weaknesses in the security controls of those infrastructure components (i.e. database, routers, firewall, servers) that a malicious user could exploit to compromise the confidentiality, integrity, and/or availability of REDACTED's systems and data.

**Scope**

The scope included those components listed in the table below:

**Table 1: System Inventory**

| Type | Model | Quantity | Manufacturer | Operating System | IP Address | Location |
|---|---|---|---|---|---|---|
| Web server -Stage | PowerEdge<br>R610/Win2003 x86<br>(32 bit) | 1 | Dell | Windows 2003 | REDACTED | REDACTED |
| Web server – SecureStage | PowerEdge<br>R610/Win2003 x86<br>(32 bit) | 1 | Dell | Windows 2003 | REDACTED | REDACTED |

| Type | Model | Quantity | Manufacturer | Operating System | IP Address | Location |
|---|---|---|---|---|---|---|
| Database Server | PowerEdge<br>R710/Win2003 x86<br>(32 bit) | 1 | Dell | Windows 2003 | REDACTED | REDACTED |
| Firewall, router | Cisco ASA 5540 this unit also has a Cisco ASA SSM-40 IDS module installed, 1 power supply, power is connected to a Baytech device in rack our | 1 | Cisco | N/A | REDACTED | REDACTED |
| DB2 database | | 1 | | | REDACTED | REDACTED |

**Task**

The figure below illustrates TNCG's proven methodology.

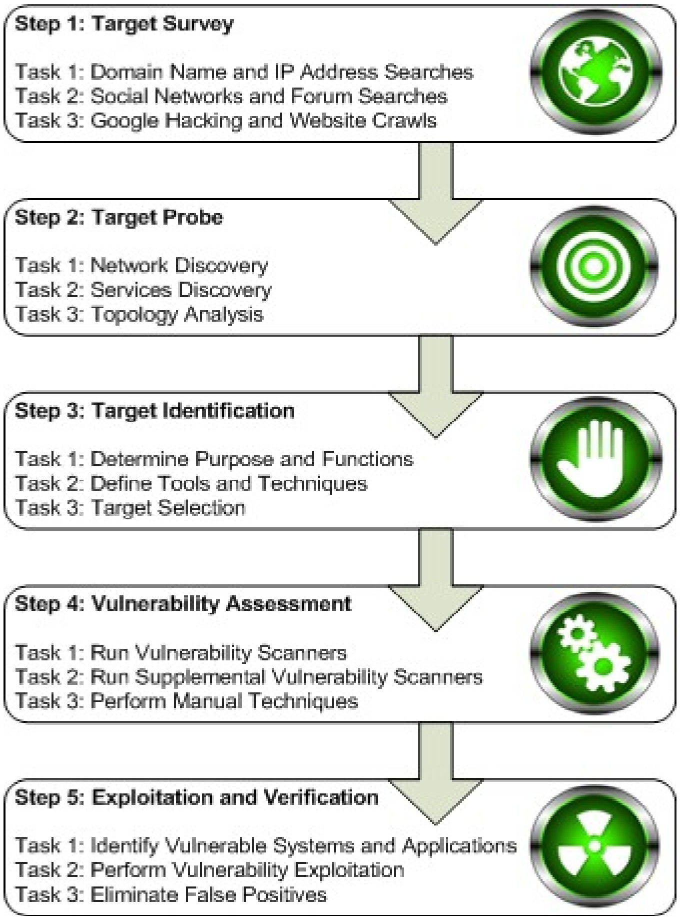

Step 1: Target Survey
Task 1: Domain Name and IP Address Searches
Task 2: Social Networks and Forum Searches
Task 3: Google Hacking and Website Crawls
Step 2: Target Probe
Task 1: Network Discovery
Task 2: Services Discovery
Task 3: Topology Analysis
Step 3: Target Identification
Task 1: Determine Purpose and Functions
Task 2: Define Tools and Techniques
Task 3: Target Selection
Step 4: Vulnerability Assessment
Task 1: Run Vulnerability Scanners
Task 2: Run Supplemental Vulnerability Scanners
Task 3: Perform Manual Techniques
Step 5: Exploitation and Verification
Task 1: Identify Vulnerable Systems and Applications
Task 2: Perform Vulnerability Exploitation
Task 3: Eliminate False Positives

**Figure 2: SeNet's Testing Methodology**

Server components were scanned using Nessus and Nmap, while the databases were examined using AppDetective. Network device configurations were manually reviewed for security misconfigurations.

### *2.1.2 Web Application Scanning and Manual Testing*

**Objective**

The objective of this phase was to determine if there were weaknesses in the web application security controls that a malicious user could exploit to compromise the confidentiality, integrity, and/or availability of REDACTED's systems and data.

**Scope**

The web applications that were included in the scope are listed below:

**Table 2: Application Inventory**

| Application | URL |
|---|---|
| REDACTED | REDACTED |
| REDACTED | REDACTED |
| REDACTED | REDACTED |
| REDACTED | REDACTED |
| REDACTED | REDACTED |
| REDACTED | REDACTED |
| REDACTED | REDACTED |
| REDACTED | REDACTED |
| REDACTED | REDACTED |
| REDACTED | REDACTED |
| REDACTED | REDACTED |
| REDACTED | REDACTED |
| REDACTED | REDACTED |
| REDACTED | REDACTED |
| REDACTED | REDACTED |
| REDACTED | REDACTED |
| REDACTED | REDACTED |
| REDACTED | REDACTED |

**Task**

Since REDACTED has recently had a web application vulnerability assessment performed, the focus of this component of testing involved assessing the application to determine if any application/business logic flaws exist that could be exploited. This type of vulnerability is often difficult to locate via traditional web application vulnerability scans and static code analysis. In order to conduct the Web application testing, we obtained a number of temporary valid accounts representing the various Web application user roles for the test scenarios.

In addition to the manual web application discussed above, we performed additional automated web application vulnerability scans to determine if any additional vulnerabilities had been introduced since the previous test.

### 2.1.3 Code Review

**Objective**

The objective of this phase was to determine if there were weaknesses in the source code of the web applications that an unauthorized user could exploit to compromise the confidentiality, integrity, and/or availability of REDACTED web applications and data.

**Scope**

The same set of applications that were in-scope for the web application testing were reviewed during this phase.

**Task**

In addition to the black-box approach to the application assessment, TNCG performed code reviews that blend manual and automated testing in a way that maximizes efficiency while thoroughly covering the code base with manual analysis. The following areas were examined in the manual analysis phase of the source code review:

- Authentication- forms based authentication and single sign on (SSO).
- Authorization- role based access control as well as access to individual objects and documents.
- Session Management- evaluating the application’s session token generation algorithms, handling, and lifetime.
- Business Logic- areas of the application that should follow an expected workflow that may be circumvented through various attack vectors.
- Data Protection- measuring the security of how data is protected at rest including persistent user data, logged information, and data that may propagate to external services and data stores with other agencies.
- Encryption- assessing the cryptographic algorithms, implementations and logic used within the applications.
- Logging and Auditing- evaluating the events logged and determining where gaps in monitoring may exist in the event of an attack or malicious user activity.
- All issues within the OWASP Top 10 such as SQL Injection, Cross Site Scripting, and Cross Site Request Forgery (CSRF).

## 2.2 Tools Used

TNCG used a combination of commercial, open-source, and custom scripts to perform the risk assessment tasks. These tools included:

## Table 3: Vulnerability Assessment Tools

| Tool | License | Purpose and Description |
|---|---|---|
| Burp Suite | Commercial | An integrated platform for performing security testing of Web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through finding and exploiting security vulnerabilities. |
| Nessus | Commercial | A leading general-purpose vulnerability scanner that can check for over 40,000 vulnerabilities for a large variety of operating systems, applications, and services. |
| Nipper | Commercial | Automates configuration analysis and security audits of network devices supporting 60+ different network firewalls, switches and routers from a wide range of manufacturers such as Cisco, HP, Juniper, Check Point, and Extreme networks. |
| AppScan | Commercial | Next-generation Web application vulnerability scanner that provides automated security assessments for vulnerabilities including but not limited to: SQL injection, cross-site scripting, SSL/parameter/Java analysis, and source code disclosure. |
| Fortify | Commercial | Static and dynamic code analysis review tools. |
| Appscan Source Edition | Commercial | Static and dynamic code analysis review tools. |
| CAT.NET | Commercial | Static and dynamic code analysis review tools. |
| W3af | Open-Source | An open-source Web application attack and auditing framework used to discover and exploit various Web application and Web server vulnerabilities. W3af also can be used as a Web proxy for analyzing HTTP requests. |
| Metasploit | Open-Source | An open-source penetration testing framework that consists of tools to discover vulnerabilities for multiple information systems. Metasploit also contains over 600 exploits with 200+ payloads that allow successful exploitation in a controlled environment of vulnerabilities discovered. |
| Nikto | Open-Source | A general-purpose Web server scanner that can discover unsecure configurations and test for basic vulnerabilities in Web sites/Web applications such as XSS, SQL injection, and flaws in coding. |
| Nmap | Open-Source | A leading open-source port scanner with the ability to detect live hosts using multiple protocols including ICMP/TCP/UDP and scan all 65,535 ports within an efficient timeframe. Nmap can also utilize scripts to help detect network-based vulnerabilities on scanned hosts. |
| Wireshark | Open-Source | A network protocol analyzer that lets you capture and interactively browse the traffic running on a computer network. It has a rich and powerful feature set and is world's most popular tool of its kind. |
| Custom Scripts | Proprietary | TNCG develops some in-house scripts using dynamic programming languages such as Perl, Python, Shell scripts and Ruby. Scripts used have been tested on SeNet’s development network to help ensure that there are no negative impacts on client systems. |

**NOTE**: *This list is not intended to be all-inclusive. Depending on ports and services that are discovered to be running, other tools may have been used with REDACTED’s permission.*

# 3. SECURITY TESTING DETAILS

This section provides a detailed account of the vulnerabilities that were noted and the recommendations to mitigate those findings. It also describes the processes and techniques that TNCG used to identify the vulnerabilities.

## 3.1 Infrastructure Testing

The infrastructure testing phase focused on three levels:

- Server
- Database
- Devices

In order to perform the testing, the testing team was provided with VPN credentials in order to scan the components without filtering to interfere with the tests. For the server testing, Nmap and Nessus scans were conducted on both the database server and the web server. Port scans were performed first using Nmap. As seen in the figure below on a scan conducted against the database server (REDACTED) the majority of the ports open were needed for business purposes.

**Figure 3: Nmap scan on the database server.**

Based on the port scan results there was not much evidence to indicate that the servers were not hardened adequately. There were some areas, such as port 1311 for Dell OpenManage that should be verified to determine that the service is being used for a business purpose. The second server, staging (REDACTED) had more services open then the database server. In addition to HTTP, which was expected, it also had enabled FTP, SMTP, and DB2. All services running should be examined and those not needed for business purposes should be disabled.

Port scans were also performed from an external perspective (i.e. not connected to the VPN) in order to assess the perimeter security. No ports were discovered to be open on the database server and only HTTP and HTTPS were open externally on the web server. This shows that correct filtering is taking place at the firewall level.

Nessus scans were then run against the two servers. The scans were configured to execute with valid credentials so that a complete scan could be performed. In addition to the authenticated scans, compliance policy scans were used to compare the servers to established benchmarks such as those from the Center for Internet Security (CIS). The results show that the servers were not out of compliance in most of the areas when compared against the benchmarks. However, several patches were missing on the servers. Both patches from Microsoft and from third-party applications such as Flash and Adobe were not at the most recent level.

AppDetective was used to assess the database for the Microsoft SQL Server (MSSQL). Multiple policies were used to compare the current security level to established benchmarks. First, database scans were conducted against the MSSQL database. The results of the scan show that while many controls and settings were in place, a number of issues were discovered that need to be addressed. These findings are summarized below and listed in detail in the database appendix.

- Weak password
- Excessive permissions on extended stored procedures
- Permissions not revoked from the group Public
- Auditing standards need to be increased

The testing team also examined the network security controls protecting the application servers. Currently, REDACTED is relying on REDACTED to perform a certain level of intrusion detection and incident response on those systems hosted in their data center. We were provided with the firewall configuration and the configuration file for the IDS. Reviews of the firewall configuration only show minor issues that need to be addressed. The IDS configuration file revealed that not all the signatures that should be enabled were. For example, in the configurations we examined we did not see substantial evidence of signatures related to web application attacks such as SQL injection. Also the signatures appeared to be outdated with not many new signatures in place with dates more recent then 2007. Additionally we examined the SLA between REDACTED and REDACTED and performed interviews with REDACTED security administrators. It is the testing team's opinion that the level of security that REDACTED is providing needs to be increased. It is SeNet's belief that REDACTED should more actively be monitoring and reporting on application level attacks; as well as taking a more proactive approach to the security monitoring and detection. During all of our web application testing not once did REDACTED send any alerts to REDACTED about the scan activities. TNCG performed web application scans from multiple source IP addresses at various time frames. Some of these source IP addresses were provided to REDACTED and REDACTED, but others were not. The majority of these scans were conducted from the Internet while not connected to the VPN, and should have been detected. Also in the past there have been incidents that REDACTED should have detected but did not. TNCG believes this fact is relevant because combined with the current scan activity not being detected this indicates a trend of malicious activity being missed.

It is recommended that REDACTED either place their own IDS sensors that they manage and control at the REDACTED facility or have the logs sent from REDACTED's IDS to REDACTED for collection in their Security Incident Event Management (SIEM) system. Since much of the traffic to REDACTED's applications is protected by SSL, the current IDS will not be able to see and inspect that traffic. REDACTED should consider implementing a solution that decrypts the traffic for inspection prior to sending it to the web servers. Another protection mechanism that should be considered is a web application firewall (WAF).

## 3.2 Web Application Scanning and Manual Testing

The designated REDACTED web applications were examined using both automated and manual techniques. The decision was made to perform the majority of the testing in the staging environment because availability of the production application is extremely important. The environment that was tested closely mirrors the production environment and only minor differences were present. Any vulnerabilities and findings noted in the staging environment are likely present on production.

Prior to starting the testing, an overview of the REDACTED web applications was provided to the testing team. This enabled the team to better understand the application and tailor testing scenarios. With the overview of the application complete the active testing phases commenced. Initially, all of the applications were examined using Burp Suite. Burp is an integrated platform for performing security testing of web applications. The testing team enabled the proxy functionality and as the applications were navigated we were able to see the HTTP requests between the client and the server. This allowed us to better understand how the applications operated. At the same time the active scanning engine of Burp was used to scan the applications for vulnerabilities. AppScan, a commercial web application scanner, was also used to scan each of the applications. Where appropriate, scans were performed using different accounts (i.e. normal user and administrator).

The scan results identified several potential issues, including SQL injection, XSS, and CSRF among others. Once the automated testing was complete the testing team verified the results and performed additional testing using manual techniques to identify flaws in the application's logic. Many of the vulnerabilities discovered by the scans were false positives; however, some were determined to be valid. The following section provides detailed descriptions of some of the weaknesses (for a complete listing please see the TVA matrices in the Appendix) that were identified during testing for each of the applications, together with illustrative screen shots and other documentation.

### *3.2.1 REDACTED*

The target URL for the REDACTED application was:

REDACTED

A number of test accounts were provided for testing purposes:

- TNCG
- FOTest
- HQTest
- PTest

The *TNCG* account was an administrator account while the other accounts were normal users.

Privilege Escalation

One of the key differences between the admin account and the normal user accounts is that there are certain menu items that are only accessible to the admin user. This is illustrated in the figure below.

**Figure 4: REDACTED menu has certain selections for administrators only.**

When viewed in the web browser a normal user cannot select these menu items as they are not enabled. However, by manipulating the HTTP requests by using a local proxy it is possible for a normal user to access and make changes via the administrator menu options.

**Figure 5: By manually making a GET request a normal user can access admin functions.**

This shows that the application is just restricting the view and not enforcing access to menu items via role-based access control (RBAC) or some other mechanism.

SQL Injection

Both AppScan and Burp scan results identified potential SQL injection in the REDACTED application. Many of the areas that the application flagged came from requests that were made when the user was not authenticated to the application. This causes the error message in the figure below to be displayed.

**Figure 6: Error message displayed that web scanners interpreted as SQL injection.**

While this has the appearance of SQL injection, this message occurs when a request is made to a resource when the user is not authenticated. This message gives away information that an attacker could use and the verbosity should be reduced.

While the above example is one where we believe the scanner gave a false-positive, there were others that indicate that SQL injection may be possible. By entering a single quote to certain requests (i.e. GET /REDACTED) an input validation error resulted.

**Figure 7: Error message indicates that SQL injection may be possible.**

The above error message typically indicates that data is not being validated correctly and is susceptible to SQL injection attacks.

Other vulnerabilities noted in the REDACTED application were:

- SSL cookie without secure flag set
- Password field with autocomplete enabled
- Cacheable HTTPS response

### *3.2.2 REDACTED*

The REDACTED series of applications is one of the most used set of applications provided by REDACTED. It consists of ways to manage the user’s accounts and retirement applications. The target URL for the normal user was REDACTED. The admin login for the application was REDACTED.

The testing team was provided with two normal user accounts and an administrator account.

In order to access the applications, authentication is required. For authentication the userID is the individual's social security number (SSN). Both the userID and password are obfuscated when entered into the application (as seen below). It is transmitted to the backend database, and although unlikely, it is possible that it could be intercepted.

**Figure 8: REDACTED login page.**

If possible REDACTED should consider using a different method to authenticate users rather than their social security number. This would decrease the risk of privacy exposure in the event of a future compromise or attack.

### SQL Injection

In the admin portion of the application the testing team did identify a potential SQL injection vulnerability in the *system log administration* functionality. By entering a single quote in the POST request for the *LogType* parameter a database error message can be generated.

**Figure 9: Add a single quote to the LogType parameter causes a SQL error.**

**Figure 10: Database error message indicates that SQLi may be possible.**

### XSS

Reflective XSS was discovered in both the administrator and user portions of the application. Both were found in POST requests and could be used to execute remote code on a victim's system. In the figures below code is entered to cause the user's browser to visit a third-party site and execute the code.

**Figure 11: The cboEEDOBMO parameter is tampered with to add scripting language to cause the browser to visit a third-party site.**

**Figure 12: The figure above shows the user being redirected to a third-party site.**

**Figure 13: The XSS is executed in the retirement planner portion of the application.**

**Figure 14: Similar vulnerability existed in the administrator user log functionality.**

### *3.2.3 REDACTED*

The REDACTED applications are accessed in the same method as the REDACTED applications (REDACTED) using a SSN for login userID. The testing team was provided with two testing accounts:

- 400357625
- 400785217

The list of REDACTED applications that were tested are illustrated in the figure below.

**Figure 15: REDACTED applications.**

The REDACTED application had many of the same medium and low vulnerabilities that the other applications were vulnerable to. These included:

- Cross-site Request Forgery
- Cookie weaknesses
- Detailed error pages
- Viewstate not encrypted

Manual attempts were made in the application to escalate privileges and access other user's data, none were successful. The testing team used their proxy to change and manipulate variables, in almost all of those cases error messages similar to the one below were encountered.

**Figure 16: Viewstate error message when attempting to modify parameters.**

The testing team was able to identify a XSS vulnerability in the application at the login (indicating the same item affects REDACTED). By modifying a POST request we were able to demonstrate that the application was vulnerable as indicated below.

**Figure 17: XSS is entered into the POST request using Burp.**

**Figure 18: XSS is executed.**

### *3.2.4 REDACTED*

The target URL for REDACTED testing was REDACTED. Two accounts were provided, a normal user and an administrator user. During the web application scanning process, the testing team did encounter performance issues. REDACTED was the only application tested that resulted in scanning issues. However, even with these issues the testing team was able to get enough data to analyze. Manual testing was also performed and several attempts to modify data, escalate privileges, and perform XSS resulted in a generic error message and in some cases causing the user to become logged out of the application.

**Figure 19: Generic error message.**

Other controls such as a warning banner, session timeout, account lockout and requiring users to change their passwords were also in place.

Password Complexity

While users were required to change their passwords, special characters were not allowed. This makes it easier for a malicious user to guess or brute force the password.

**Figure 20: Special characters were not allowed.**

Viewstate Weaknesses

An issue which was consistent across multiple ASP.Net applications that utilize Viewstate is that encryption was not being used. While MAC is enabled and used this can easily be decoded and potentially sensitive information obtained.

**Figure 21: Viewstate encryption is not being utilized.**

### *3.2.5 Applications Not Requiring Authentication*

While the majority of the applications provided by REDACTED do require authentication, there are some that do not. These are primarily minor applications that provide public information and not sensitive data. The applications that fall into this category are listed below:

- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED
- REDACTED

Dynamic (Reflective) XSS

The scanners identified some areas where dynamic XSS was possible. While this is not as serious of a threat as is a persistent XSS vulnerability, it is still a security concern. Below is an example of how using dynamic XSS can enable an individual to display a user’s cookie information.

**Figure 22: XSS is entered into the POST request.**

**Figure 23: The XSS is executed and cookie information is displayed.**

### SQL Injection

During testing, a SQL injection vulnerability was found in the Request Tracking application. During the POST request for the Archive Records functionality the user input is not correctly validated making SQL injection possible as seen in the figures below.

**Figure 24: Entering a single quote to the txt_Year parameter causes a database error message.**

**Figure 25: Burp is used to perform SQLi to display the database version.**

**Figure 26: The version information is displayed showing that the SQLi was successful.**

## 3.3 CODE REVIEW

The code review portion of the assessment consisted of both manual and automated testing techniques. REDACTED provided the testing team with all of the application code that was in-scope for this assessment. The testing effort began with a manual review of the code in order to identify “low-hanging fruit” that could easily be exploited by an attacker. We then used Fortify, a static code analysis tool in order to perform a more detailed analysis. The results of the tool were then examined manually to further investigate and identify false-positives.

Many of the same vulnerabilities were discovered in the code review portion as in the web application testing phase. As expected, the code review phase did identify a number of additional vulnerabilities that put REDACTED applications at risk. Access to the code also allowed the testing team to confirm vulnerabilities that could not be easily detected via dynamic web application testing.

The remainder of this section provides examples of the types of vulnerabilities noted during this phase. For each type of vulnerability an example is provided that illustrates in detail the issue.

### *3.3.1 High Severity Finding*

#### *SQL Injection- Systemic*

**Table 4: SQL Injection**

| Application | Class / Procedure | Line(s) of Code |
|---|---|---|
| REDACTED | REDACTED | 212-219 |
| REDACTED | REDACTED | 75-80<br>160-178 |
| REDACTED | REDACTED | 79-120<br>160-178 |
| REDACTED | REDACTED | 66-67 |
| REDACTED | REDACTED | 76-81<br>119-125<br>145-146<br>151-153<br>243-244 |
| REDACTED | REDACTED | 52-54<br>382-404 |
| REDACTED | REDACTED | 60-68<br>110-114 |
| REDACTED | REDACTED | 86-87 |
| REDACTED | REDACTED | 74-76 |
| REDACTED | REDACTED | 297-298<br>303-304<br>367-371 |
| REDACTED | REDACTED | 218 |
| REDACTED | REDACTED | 222<br>224 |
| REDACTED | REDACTED | 282 |
| REDACTED | REDACTED | 87<br>123-124<br>351<br>562-564<br>590-592 |
| REDACTED | REDACTED | 60-64<br>95-96<br>100-101<br>106-107<br>110-113<br>120-122 |
| REDACTED | REDACTED | 516-535 |
| REDACTED | REDACTED | 818-841 |
| REDACTED | REDACTED | 16-44 |
| REDACTED | REDACTED | 13-21 |
| REDACTED | REDACTED | 22-25 |
| REDACTED | REDACTED | 17-24 |
| REDACTED | REDACTED | 2742-2842 |

| Application | Class / Procedure | Line(s) of Code |
|---|---|---|
|  |  | 2844-2874<br>3030-3067 |
| REDACTED | REDACTED | 418-422 |
| REDACTED | REDACTED | 40-41 |

## Description

Several applications take untrusted user input and allows for it to be directly injected into database statements. The root cause of the issue is a lack of prepared statements utilizing bind variables. In many places throughout the code, SQL statements are created dynamically by concatenating strings that contain user controllable and potentially hostile input.

As an example, in several locations within REDACTED, the application places user supplied input into SQL statements. The application first attempts to limit a user's ability to enter an apostrophe by appending an additional apostrophe to the input. However, a user can prepend a slash to the input, effectively rendering the added apostrophe useless. This can be performed utilizing Microsoft SQL's ESCAPE clause as well as several encoding techniques that will bypass the programmatic filtering method.

## Evidence

**Figure 27: The sqlStringFix method within the REDACTED resource.**

**Figure 28: The sqlStringFix method being run against the sqlssn string.**

**Figure 29: SQL Injection occurring when the user input is placed into a statement utilizing string concatenation.**

Another unique example of SQL Injection was discovered within the REDACTED application. The injection occurred utilizing data that was stored within a session variable utilizing user-tainted data. The application accepts the data, but at a later point in time utilizes the value contained within the session in order to execute a SQL statement. As a result, it is possible to trigger an injection within the application. The next few examples demonstrate this.

**Figure 30: User input being stored within a session variable in the REDACTED class.**

**Figure 31: The user input contained in the session variable is used to dynamically create a SQL statement.**

## Recommendations

Utilize prepared statements as opposed to dynamically creating queries with string concatenation. Each variable should be individually bound, which ensures that the database interpreter is able to distinguish between code and data within queries.

Input validation and filtering should not be considered a mitigating solution for SQL Injection, as they do not solve the problem at its root cause. Additionally, filter evasions are often common due to flawed implementations as well as occasionally vulnerable frameworks themselves.

## Additional Information

OWASP SQL Injection Guide

https://www.owasp.org/index.php/SQL_Injection

OWASP SQL Injection Prevention Cheat Sheet

https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet

MS SQL ESCAPE Clause

http://blogs.msdn.com/b/zainala/archive/2008/08/17/using-and-escape-clause-in-sql-server-like-query.aspx

Using SQL Escape Sequences

http://msdn.microsoft.com/en-us/library/ms378045(v=sql.90).aspx

Escape Single Quotes in MS SQL

http://www.techtamasha.com/escape-single-quotes-and-wild-cards-_-in-ms-sql/20

## *Cross Site Scripting (XSS)- Systemic*

**Table 5: XSS**

| Application | Class / Procedure | Line(s) of Code |
|---|---|---|
| REDACTED | REDACTED | 167-180 |
| REDACTED | REDACTED | 4 |
| REDACTED | REDACTED | 327 |
| REDACTED | REDACTED | 258 |
| REDACTED | REDACTED | 8-9 |
| REDACTED | REDACTED | 79 |
| REDACTED | REDACTED | 7 |
| REDACTED | REDACTED | 12 |
| REDACTED | REDACTED | 164-176 |
| REDACTED | REDACTED | 100-228 |

### Description

The application is vulnerable to XSS in many locations. **As this is a systemic finding, only a sampling of vulnerable areas has been provided within this report.** Security controls to mitigate this issue were found to be completely absent from the application except within isolated instances.

XSS occurs when an attacker can inject script or HTML data into the code returned within a rendered page or resource. XSS can be used to hijack sessions, execute unauthorized transactions on a user's behalf, and deliver malicious payloads to compromise an end user's system. Within the application, XSS occurred due to a lack of contextual output encoding and escaping as well as weak server-side input validation.

When JavaScript or HTML code is submitted with a request, it is rendered without modification within the application's response. As a result, attackers have the ability to cause victim users to execute arbitrary code within their browsers or apps rendering the response.

Both JavaScript and HTML context XSS were discovered. Each context requires a slightly different approach to exploit as well as different output encoding and escaping formats to defend against.

XSS occurring within a JavaScript context results in the attacker submitted code being injected inline within a script.

### Evidence

This example was found within REDACTED's REDACTED code, lines 167-180.

**Figure 32: User input being reflected back within a response without performing HTML encoding on the data, allowing for script execution.**

**Figure 33: The user input is later reflected when the HTML body is loaded.**

**Figure 34: Request.QueryString value used within the Page_Load method without output encoding or modification in the REDACTED class.**

## Recommendations

As the identified instances of XSS were found within both HTML and JavaScript contexts, the proper mitigation is to output encode the data. The HTML data reflected back should be HTML encoded, while the JavaScript output must be escaped or encoded within the JavaScript context's set of characters.

Prior to rendering user data within a response, encode the data utilizing either built-in functions or a third party library. In the event data is placed into a block of JavaScript code or within Cascading Style Sheets, then proper escaping of characters relevant within those contexts would have to be performed as well.

In addition to output encoding, it is also recommended to perform strong input validation for fields where it is possible to do so. As an example, a zip code field's format is well known and can be validated with a Regular Expression that looks for five digits or five digits, a dash, and an additional four digits. Any submissions that do not meet these criteria could immediately be rejected.

For usage of element.innerHTML, it is recommend to use element.textContent when the content is expected to only be composed of plain text. Otherwise, encode the data first with an HTML encoder, then followed by the JavaScript context. This will prevent script execution within both the outer and nested contexts.

## Additional Information

OWASP XSS Prevention Cheat Sheet

https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet

OWASP XSS Guide

https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

OWASP DOM-Based XSS Prevention Cheat Sheet

https://www.owasp.org/index.php/DOM_based_XSS_Prevention_Cheat_Sheet

Mozilla innerHTML Reference

https://developer.mozilla.org/en-US/docs/DOM/element.innerHTML

## *Cross Site Request Forgery (CSRF)*

**Table 6: CSRF**

| Application | Class / Procedure | Line(s) of Code |
|---|---|---|
| REDACTED | All | * |
| REDACTED | All | * |
| REDACTED | All | * |

### Description

Nearly every sensitive form within the Classic ASP applications identified above is vulnerable to CSRF. The applications utilizing Classic ASP were found to be systemically vulnerable to CSRF, while the ASP.NET applications were vulnerable within select, limited instances.

By default, the browser will always send cookies within requests to a domain that it has existing cookies for. This occurs regardless of whether the request was generated by the user or by resources loaded within a respective web page. If an attacker were to pre-craft an HTTP request containing an action with parameters to be submitted, the victim's browser would submit this request. This could be achieved by either sending links with malicious URLs or by storing this on public websites that are commonly frequented by the application's user demographics.

CSRF generally occurs when a submission does not require a random value to be present within a request. As a result, an attacker can determine in advance the appropriate values to force the victim to send. Within this application, it was found to be possible to force users to modify account settings as well as case information without their consent.

### Evidence

A form submission to an administrative function within REDACTED's code that does not contain any values that cannot be pre-computed by an attacker. This indicates that the request is vulnerable to CSRF.

**Figure 35: A form submission to an administrative function within REDACTED's code**

A form submission within REDACTED in the REDACTED code that allows for session variables to set within the victim's context using untrusted input and without their awareness. This may be used to trigger fraudulent transactions on a victim's behalf.

**Figure 36: A form submission within REDACTED in the REDACTED code**

### Recommendations

Require a cryptographically random nonce to be submitted with every sensitive form submission. This can be tied to the user's session server side. Every request that should contain this value must be checked to ensure that it matches the expected value. In the event the value does not match, this should be logged server side and flagged as suspicious behavior, as it is often a clear indicator of malicious activities.

The most straightforward approach to implementing CSRF protection within the application would be to generate a token when logging in and saving it as a session variable. Within each form that results in a state changing operating being executed, a hidden form field can be utilized in order to cause the token to be submitted every time. At the server side, prior to allowing the transaction to execute, the application should check to ensure that the CSRF token submitted with the session token matches the expected value.

Anti-CSRF protections must be applied to both GET and POST requests. Utilizing HTTP POST does not prevent CSRF, as attackers have multiple ways available to control the HTTP method within victim requests.

**Additional Information**

OWASP CSRF Guide

https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)

OWASP CSRF Prevention Cheat Sheet

https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet

## *Insecure Direct Object References- Systemic*

**Table 7: Insecure Direct Object References**

| Application | Class / Procedure | Line(s) of Code |
|---|---|---|
| REDACTED | REDACTED | 34-37, 39 |
| REDACTED | REDACTED | 209, 225 |

### Description

Many requests allow the user to submit arbitrary values by modifying the request utilizing a tool such as an intercepting proxy. By tampering with parameters, an attacker can access objects that they were not intended to have access to. While the application may not have directly presented the user with the option to select a specific object, by modifying a value (i.e.- within an account number), it becomes possible to access any object directly. **The examples shown within the report represent a sampling of Insecure Direct Object Reference findings with unique characteristics. These do not include all findings as this issue was widespread throughout the application. REDACTED must implement an enterprise-wide set of controls to address this issue.**

The root cause of this issue is the fact that REDACTED does not adequately check to ensure that a user is authorized for specific database records prior to serving them. Additionally, due to the fact that the applications heavily utilize predictably formatted social security numbers, the difficulty in guessing these numbers is decreased. In many cases it is possible to brute-force through the entire range of possible social security numbers to either execute a state changing transaction or query for data that you are not authorized for.

### Evidence

Example from the REDACTED application’s REDACTED class where the REDACTED value can be tampered with by an attacker to gain access to unassigned REDACTED.

**Figure 37: REDACTED class where the server side application blindly accepts arbitrary values representing REDACTED that a user may not be assigned to.**

### Recommendations

It is recommended to build access controls as close to the data access as possible. Records such as transaction history should have data that should associate the owner with the record. At the time of a request, the identifier present within the data should be checked against the user’s identity such as the account ID associated with the current session.

In general, access to tampering with the account number should be reduced throughout the application. Any parameters (such as an account number) that should never be modified by a user should be removed from client-side access. Hidden form fields can still be manipulated by a remote attacker, and are not considered an anti-tampering solution.

### Additional Information

OWASP Insecure Direct Object References

https://www.owasp.org/index.php/Top_10_2010-A4-Insecure_Direct_Object_References

## *Failure to Restrict URL Access- Systemic*

**Table 8: Failure to Restrict URL Access**

| Application | Class/Procedure | Line(s) of Code |
|---|---|---|
| REDACTED | REDACTED | * |
| REDACTED | REDACTED | * |
| REDACTED | REDACTED | * |
| REDACTED | REDACTED | * |
| REDACTED | REDACTED | * |

### Description

There are several administrative resources within the applications that can be accessed by regular users by directly browsing to each respective resource. While these resources are not linked or exposed to regular users under normal circumstances, by knowing their location, it is possible to access them and to submit requests using these privileged functions. REDACTED did not consistently implement security controls against elevation of privileges via unrestricted URL access.

The root cause of this issue is the lack of an authorization check when a user attempts to access a given resource. As the application only expects users to access resources displayed to them through the user interface, the backend logic does not include checks to ensure that the requested resource is authorized for the current user's role.

### Evidence

**Figure 38: Example of an administrative resource in REDACTED being accessed without an access control check within the Page_Load method.**

### Recommendations

Prior to serving privileged resources, the applications should first check the user's access level to ensure that they are authorized to access the resource. This can be achieved programmatically or through ASP.NET's Role Provider. The ASP.NET Role Provider is available to the .NET applications, while the Classic ASP applications can either utilized a mixed environment with ASP.NET or implement programmatic checks to determine a user's role when a page request loads.

### Additional Information

Implementing a Role Provider

http://msdn.microsoft.com/en-us/library/8fw7xh74(v=vs.100).aspx

OWASP Top 10- Failure to Restrict URL Access

https://www.owasp.org/index.php/Top_10_2010-A8-Failure_to_Restrict_URL_Access

## Failure to Restrict URL Access

http://www.jmelton.com/2010/08/17/the-owasp-top-ten-and-esapi-part-11-failure-to-restrict-url-access/

### 3.3.2 Medium Severity Findings

### Open URL Redirection

**Table 10: Open URL Redirection**

| Application | Class/Procedure | Line(s) of Code |
|---|---|---|
| REDACTED | REDACTED | 16 |
| REDACTED | REDACTED | 55<br>58<br>61 |
| REDACTED | REDACTED | 313 |
| REDACTED | REDACTED | 933 |
| REDACTED | REDACTED | 32<br>38<br>44<br>50 |

#### Description

An HTTP parameter can be utilized to control the URL that a user is redirected to utilizing the redirection functions available at the server. In the event an attacker sends a phishing email to a user containing a request with a malicious redirection URL, the user could be redirected to an arbitrary website or resource.

#### Evidence

Example of a redirection function within REDACTED that can be abused in order to send users to unexpected resources.

**Figure 39: Example of a redirection function within REDACTED**

#### Recommendations

Consider removing a user's ability to influence URL redirection decisions. This can be achieved by removing the user input from redirection URLs, and replacing this with server generated, trusted input.

#### Additional Information

OWASP Top 10 A10- Unvalidated Redirects and Forwards

https://www.owasp.org/index.php/Top_10_2010-A10-Unvalidated_Redirects_and_Forwards

## *Trust Boundary Violation- Systemic*

**Table 11: Trust Boundary Violation**

| Application | Class/Procedure | Line(s) of Code |
|---|---|---|
| REDACTED | * | * |
| REDACTED | * | * |
| REDACTED | * | * |

### Description

Trust boundary violations typically occur when a program mixes trusted and untrusted data within related data structures. As developers generally expect session variables to be trusted server-side resources, it is typically treated as trusted data. Without clearly established boundaries, programmers will likely miss locations where trust boundaries are breached and data becomes untrusted.

Within several applications, this behavior was encountered frequently. Data sent within user requests was associated with session objects at the server. The untrusted data placed into session objects was later utilized for various purposes including database calls, enforcing authorization, and identifying the user.

### Evidence

A user submitted value being copied into a session variable within REDACTED and the REDACTED code. The values stored within the variables are later used for sensitive functions.

**Figure 40: A user submitted value being copied into a session variable within REDACTED and the REDACTED code.**

Example within the REDACTED application’s REDACTED class. The *varssa* variable is used extensively throughout the application.

**Figure 41: Example within the REDACTED application’s REDACTED class.**

### Recommendations

Avoid storing both trusted and untrusted data within the same data structure. Ensure that session objects are never written to utilizing the data obtained via user input. This will reduce the likelihood of untrusted data being mistaken for trusted data within a server side context.

REDACTED should consider enforcing this requirement via its secure development standard. Developers should be discouraged from implementing this pattern within future code as it significantly increases the likelihood of undesired behavior.

### Additional Information

OWASP Trust Boundary Violation

https://www.owasp.org/index.php/Trust_Boundary_Violation

### *Unencrypted ASP.NET ViewState*

**Table 12: Unencrypted ViewState**

| Application | Class / Procedure | Line(s) of Code |
|---|---|---|
| REDACTED | *.aspx | * |
| REDACTED | *.aspx | * |
| REDACTED | *.aspx | * |
| REDACTED | *.aspx | * |
| REDACTED | *.aspx | * |
| REDACTED | *.aspx | * |
| REDACTED | *.aspx | * |
| REDACTED | *.aspx | * |
| REDACTED | *.aspx | * |

#### Description

ASP.NET provides the ViewState feature in order to allow developers to persist data throughout a user's session across callbacks without requiring multiple database queries to retrieve the data. The ViewState is represented as a Base64 encoded value that is embedded into the actual web page itself.

Within the .NET applications, it was found that several pieces of sensitive data were present within the ViewState including names, addresses, usernames, and social security numbers. As the value is encoded, this is not considered a security control in the same manner as proper encryption.

The presence of sensitive unencrypted data within the ViewState increases the likelihood of unauthorized disclosure through dumping of a browser cache as well as through XSS attacks that scrape data from a victim's browser.

#### Recommendations

TNCG recommends enabling ViewState encryption at the web.config level. This will ensure that all usage of ViewState throughout the application is fully encrypted, reducing the surface for unintentional disclosure of PII.

In places where the ViewState is not actually utilized or consumed by the server, TNCG recommends disabling the ViewState within those controls. This will also improve performance, as the ViewState's size adds to the amount of data transmitted within requests and responses.

#### Additional Information

Microsoft- Securing ViewState

http://msdn.microsoft.com/en-us/library/ms178199(v=vs.85).aspx

ASP.NET ViewState Overview

http://msdn.microsoft.com/en-us/library/bb386448(v=vs.100).aspx

## *Username Enumeration*

**Table 13: Username Enumeration**

| Application | Class / Procedure | Line(s) of Code |
|---|---|---|
| REDACTED | REDACTED | 122-139 |
| REDACTED | REDACTED | 118-137 |
| REDACTED | REDACTED | * |

### Description

It is possible to enumerate user accounts that are present within several applications by utilizing the variances in error messages at the login and forgotten password pages. Additionally, the excessive usage of social security numbers as identifiers also increases the likelihood of successful brute force enumeration of user identifiers.

### Evidence

**Figure 42: The REDACTED class within REDACTED returns several different messages depending upon the account's status and the information provided by the remote user.**

### Recommendations

The application should return generic, uniform responses regardless of an account's current status. While this may prove to be a slight inconvenience to users, this will increase the level of difficulty required to enumerate accounts as the attacker will not get immediate feedback through differences in HTTP responses.

### Additional Information

OWASP Testing for User Enumeration

https://www.owasp.org/index.php/Testing_for_User_Enumeration_and_Guessable_User_Account_(OWASP-AT-002)

## *Weak Password Policy*

**Table 14: Weak Password Policy**

| Application | Class/Procedure | Line(s) of Code |
|---|---|---|
| REDACTED | REDACTED | 205-208 |
| REDACTED | REDACTED | 23-45 |
| REDACTED | REDACTED | * |

### Description

The applications do not consistently enforce proper restrictions on password length, complexity, or composition. As a result, the level of difficulty required to perform password-guessing attacks is decreased. Both REDACTED and REDACTED do not require users to utilize special characters within their passwords.

### Evidence

REDACTED password validator that does not allow special characters to be used. This decreases the maximum amount of entropy available for the password.

**Figure 43: REDACTED password validator that does not allow special characters to be used.**

### Recommendations

Strong password requirements should be implemented within the application to mitigate the risk of brute force or dictionary attacks. Do not rely on client-side data validation.

Best practices indicate that passwords will follow all or most of the following guidelines:

- Case-sensitive password
- Minimum password length of 7
- Maximum password length of at least 20
- Allow special characters
- Require at least one number and/or special character
- Do not allow any part of the username to appear in the password
- Do not allow any form of the word "password" or other common dictionary words
- Do not allow the name of the application to be used as a password
- Do not allow the same character three or more times in succession
- Do not restrict the number of times a user can change his password

### Additional Information

OWASP Password Complexity & Length

https://www.owasp.org/index.php/Password_length_&_complexity

## *Denial of Service Via Disk Storage Exhaustion*

**Table 15: Denial of Service via Disk Storage Exhaustion**

| Application | Class / Procedure | Line(s) of Code |
|---|---|---|
| REDACTED | REDACTED | 37, 41, 50, 54, 58, 62, 66 |
| REDACTED | REDACTED | 16 |
| REDACTED | REDACTED | 40 |
| REDACTED | REDACTED | 51 |
| REDACTED | REDACTED | 36, 42, 53, 59, 65, 71, 77 |

### Description

Several applications use the primary disk partition (the C: drive) for storing logs generated by the application. An attacker can abuse this behavior by sending an excessive amount of requests that trigger write operations to the log. The attacker will eventually be able to fill up all available disk space, leading to Denial of Service (DoS) conditions on the system. Legitimate processes and applications that require usage of the system disk will be unable to write to files and normal operations may be impacted.

### Evidence

**Figure 44: Log rotation function within REDACTED that uses the primary C: drive.**

### Recommendations

Use a separate disk partition for storing log files. In the event the partition where the log files are stored is exhausted by an attacker, it should not impact the overall availability and stability of the underlying operating system.

### Additional Information

OWASP Application Denial of Service

[https://www.owasp.org/index.php/Application_Denial_of_Service](https://www.owasp.org/index.php/Application_Denial_of_Service)

## *Log Files Are Publicly Accessible*

**Table 16: Log files are Publicly Accessible**

| Application | Class / Procedure | Line(s) of Code |
|---|---|---|
| REDACTED | REDACTED | 37, 41, 50, 54, 58, 62, 66 |
| REDACTED | REDACTED | 16 |
| REDACTED | REDACTED | 51 |
| REDACTED | REDACTED | 36, 42, 53, 59, 65, 71, 77 |

### Description

Several applications store server logs within publicly accessible web directories. The logs do not appear to have access control restrictions placed upon them, and as a result it is possible for a malicious user or attacker to forcefully browse to the log files. An attacker can utilize brute force techniques in order to guess the log file names. Within the logs, social security numbers and other highly sensitive pieces of information are present in plain text.

### Evidence

**Figure 45: Log file being stored to a web accessible directory within REDACTED.**

### Recommendations

Modify the log file path to use a location that is not directly accessible through the web root. A user should never be able to directly access log files remotely. Ensure that the log files stored on the system are restricted with the appropriate level of permission using the principles of least privilege access.

### Additional Information

OWASP Logging Cheat Sheet

https://www.owasp.org/index.php/Logging_Cheat_Sheet

## *Privileged Database SA Account In Use*

**Table 17: Privileged Database SA Account in Use**

| Application | Class / Procedure | Line(s) of Code |
|---|---|---|
| REDACTED | REDACTED | 69 |
| REDACTED | REDACTED | 65 |
| REDACTED | REDACTED | 61 |

### Description

The use of the Microsoft SQL Server ‘sa’ account to access database objects is highly discouraged. The danger lies in the privileged relationship the application has with the database server. If SQL Injection is introduced, more damaging actions could take place such as re-enabling xp_cmdshell and directing the database server to call out to the attacker’s machine, therefore enabling remote access. Additionally, all database objects could be accessed, destroyed or otherwise manipulated by an unauthorized party.

### Evidence

The web.config file for the REDACTED application which shows the SA account referenced within the database connection string.

**Figure 46: The web.config file for the REDACTED application**

### Recommendations

Create a lower privileged account user that can access only the databases and tables required for operations. The account should be limited in its access rights, and should only have access to the operations explicitly required for the application to function as intended.

### Additional Information

OWASP Guide to Authorization

https://www.owasp.org/index.php/Guide_to_Authorization#Principle_of_l east_privilege

## *Unsalted Password Hashes*

**Table 18: Unsalted Password Hashes**

| Application | Class / Procedure | Line(s) of Code |
|---|---|---|
| REDACTED | REDACTED | 472 |
| REDACTED | REDACTED | 10-33 |

### Description

The REDACTED application stores user passwords in hashed format within the database. However, the passwords are not salted prior to being stored in the database, which decreases the amount of time required to perform brute force attacks against hashes to recover the original passwords. In the event of a backend database breach, an attacker may be able to crack a significant amount of passwords. This issue is elevated in risk due to the presence of weak password policies in conjunction with a lack of salting.

### Evidence

**Figure 47: A password being MD5 hashed without a salt within the REDACTED class.**

**Figure 48: The BasePage.MD5Encrypt(string) method that does not utilize a salt.**

### Recommendations

Prior to storing a user's password within the database, the value should first be hashed. The benefit to using a hashing algorithm instead of a symmetric encryption algorithm is the one-way relationship from a plain text value to a hash. By also using a strong salt and running multiple iterations over the hashed value, it significantly increases the amount of computing required to discover the original value.

SHA-512 or SHA-256 are the recommended hashing algorithms for implementing this security enhancement. MD5 should not be used.

### Additional Information

OWASP Password Storage Cheat Sheet

https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet

## *Browser Caches Sensitive Information*

**Table 19: Browser Caches Sensitive Information**

| Application | Class / Procedure | Line(s) of Code |
|---|---|---|
| REDACTED | * | * |
| REDACTED | * | * |
| REDACTED | * | * |
| REDACTED | * | * |
| REDACTED | * | * |
| REDACTED | * | * |
| REDACTED | * | * |
| REDACTED | * | * |
| REDACTED | * | * |
| REDACTED | * | * |
| REDACTED | * | * |
| REDACTED | * | * |
| REDACTED | * | * |
| REDACTED | * | * |
| REDACTED | * | * |

### Description

Web browsers cache a significant amount of information by default in order to optimize the user experience. When a resource is cached and it is re-requested by a user, it is served from the local file system as opposed to requesting it from the server.

All cached information is stored locally on the user's device or system. In the event of a system compromise or a lost device, an attacker may be able to recover cached data. As the REDACTED applications contain information that can be considered high in value to many, this risk increases the likelihood that information will be leaked to unauthorized parties.

Setting various HTTP headers that instruct browsers not to cache data contained within responses may prevent caching. Within each application, it was discovered that each of the required headers were not utilized, making it likely that multiple browsers will cache documents.

### Recommendations

For the pages identified to contain cacheable sensitive information, ensure that the three primary anti-caching HTTP headers are utilized. These include:

- Pragma: no-cache
- Cache-Control: no-cache, no-store, must-revalidate
- Expires: 0

The anti-caching headers can be applied in one of two ways: within code, and at the web server.

IIS can be used to add the additional headers to responses that will instruct browsers not to cache information considered highly sensitive such as social security numbers.

**Additional Information**

Anti-Caching Headers

http://www.jtmelton.com/2012/05/23/year-of-security-for-java-week-21-anti-caching-headers/

How to Prevent Caching in Internet Explorer

http://support.microsoft.com/kb/234067

HTTP Caching

http://code.google.com/p/doctype-mirror/wiki/ArticleHttpCaching

## *Insecure Test Code Present*

**Table 20: Insecure Test Code Present**

| Application | Class / Procedure | Line(s) of Code |
|---|---|---|
| REDACTED | REDACTED | * |
| REDACTED | REDACTED | * |
| REDACTED | REDACTED | * |
| REDACTED | REDACTED | * |
| REDACTED | REDACTED | * |

### Description

Within many different places throughout the applications, unused (and often unlinked) test code is present. In the locations identified, it does not appear as though the code serves a specific purpose to the business. The code is also vulnerable to several classes of issues including XSS and information leakage.

The root cause of this issue appears to be a gap within the deployment process where applications are not checked for test code prior to releasing an update into production.

### Evidence

**Figure 49: Test code within REDACTED in the REDACTED class that is vulnerable to XSS.**

### Recommendations

Prior to allowing a release into production, REDACTED should carefully review the new code introduced to ensure that it does not include unintended functionality. In the event test or unwanted code makes it into production, REDACTED can increase its likelihood of detecting these issues by performing application security assessments regularly.

### Additional Information

OWASP Information Leakage

https://www.owasp.org/index.php/Information_Leakage

### *3.3.3 Low Severity Findings*

### *Verbose Error Messages*

**Table 21: Verbose Error Messages**

| Application | Class / Procedure | Line(s) of Code |
|---|---|---|
| REDACTED | Web.config | 19 |
| REDACTED | Web.config | 25 |
| REDACTED | Web.config | 26 |

#### Description

Many pages throughout REDACTED's applications are configured to return verbose error messages that disclose information about the application's server side functionality. This is due to a combination of the absence of exception handling along with explicitly configuring the application to return verbose errors. In some places, the application is coded to explicitly display exception information and stack traces.

#### Evidence

**Figure 50: Web.config file for REDACTED that turns custom errors off and enables verbose errors to be rendered.**

#### Recommendations

Ensure that verbose error messages are not leaked back to clients. Within any code that explicitly returns error messages for diagnostic purposes, ensure that the output of the diagnostic messages does not contain specific error details. Error messages should be useful enough to let a user know that an error has occurred, but generic enough to never reveal application-specific information. This usually includes stack traces, debug messages, and any other information that describes the code or application's architecture.

Within the ASP.NET applications, ensure that custom errors are enabled within the *web.config* file.

For all applications, search the source code for instances of the string "*.message*" and evaluate their business requirements. If there is no legitimate business reason to utilize their information, remove them from the source code. Searching the code for this string will reveal many instances of verbose error messages being rendered.

#### Additional Information

CWE- Information Exposure Through Error Messages

http://cwe.mitre.org/data/definitions/209.html

ASP.NET Displaying a Custom Error Page

http://www.asp.net/web-forms/tutorials/deployment/deploying-web-site-projects/displaying-a-custom-error-page-cs

## *Cookies Not Marked Secure*

**Table 22: Cookies Not Marked Secure**

| Application | Class/Procedure | Line(s) of Code |
|---|---|---|
| REDACTED | Web.config | N/A |
| REDACTED | Web.config | N/A |
| REDACTED | Web.config | N/A |
| REDACTED | Web.config | N/A |
| REDACTED | Web.config | N/A |
| REDACTED | N/A | N/A |
| REDACTED | N/A | N/A |
| REDACTED | Web.config | N/A |

### Description

Setting the "*secure*" flag on a cookie ensures that it cannot be passed except over a secure (HTTPS) connection. It provides an extra layer of defense against cookie stealing attacks by ensuring that the cookie cannot be intercepted in plain text over an insecure HTTP channel. As all privileged authenticated functionality appears to be served over HTTPS, the cookies will continue to work normally.

### Recommendations

For the .NET applications, within the application's master web.config file, add a line within the system.web element that contains:

*<httpCookies requireSSL="true" />*

For the Classic ASP applications, set the "*secure*" attribute within the Response.Cookies collection at the time a cookie is set after authentication:

### Additional Information

ASP.NET Setting the Secure Flag

http://stackoverflow.com/questions/1442863/how-can-i-set-the-secure-flag-on-an-asp-net-session-cookie

Response.Cookies Collection

http://msdn.microsoft.com/en-us/library/ms524757.aspx

## *Cookie HTTPOnly Flag Not Set*

**Table 23: Cookie HTTPOnly Flag Not Set**

| Application | Class / Procedure | Line(s) of Code |
|---|---|---|
| REDACTED | Web.config | N/A |
| REDACTED | Web.config | N/A |
| REDACTED | Web.config | N/A |
| REDACTED | Web.config | N/A |
| REDACTED | Web.config | N/A |
| REDACTED | N/A | N/A |
| REDACTED | N/A | N/A |
| REDACTED | Web.config | N/A |

### Description

By default, cookies set within the browser for a given domain can be accessed using JavaScript. Under normal circumstances, this can only be performed from scripts running from the same domain only. This protection is known as the “same origin policy” and is intended to reduce the impact and increase the difficulty in performing session hijacking attacks.

Several of REDACTED’s applications do not set the “HTTPOnly” flag when cookies are set. As a result, a successful XSS attack can allow an attacker to hijack a user’s cookies during an authenticated session, giving them complete access to the account within the victim user’s context.

The “HTTPOnly” flag instructs the browser to prevent cookie access from scripts loaded by the browser. This significantly raises the level of difficulty required to hijack user sessions, even with a working XSS exploit.

### Recommendations

Add the “HTTPOnly” flag to cookies when they are set. As it did not appear during testing that cookies are generally accessed through scripting, this should provide minimal impact to regular operations and availability.

### Additional Information

OWASP HTTPOnly

[https://www.owasp.org/index.php/HttpOnly](https://www.owasp.org/index.php/HttpOnly)

## *Plain Text Passwords in Configuration Files*

**Table 24: Plain Text Passwords in Configuration Files**

| Application | Class / Procedure | Line(s) of Code |
|---|---|---|
| REDACTED | REDACTED | 73-94 |
| REDACTED | REDACTED | 18, 24, 30 |
| REDACTED | REDACTED | 23, 26, 29, 32, 35, 38 |
| REDACTED | REDACTED | 81 |
| REDACTED | REDACTED | 32, 38, 49, 55, 61, 67, 73, 91, 95, 99, 103, 107 |
| REDACTED | REDACTED | 9-10 |
| REDACTED | REDACTED | 20 |

### Description

Several applications store the plain text passwords used for database access within configuration files. Within several applications, the passwords are hardcoded into the applications. An attacker that gained access to source code either through a code disclosure vulnerability or by gaining access to a web server, would be able to utilize the password to potentially elevate their access levels.

Additionally, the surface for exposing credentials is broadened due to the likelihood that developer systems may have copies of the source code. In the event of a lost laptop or a system compromise, an attacker would be able to retrieve the credentials from a developer machine.

### Evidence

**Figure 51: The database connection string within REDACTED, stored in plain text within the web.config file.**

### Recommendations

Encrypt the database connection strings stored within the web.config utilizing the resources provided below. This will work for the ASP.NET applications. For the Classic ASP applications, TNCG recommends considering a mixed mode environment where the Classic ASP applications can leverage parts of the .NET framework's security features.

Passwords currently hardcoded into the applications should be moved to either a web.config file or a global.asa file.

### Additional Information

SANS Securing SQL String

http://www.sans.org/reading_room/whitepapers/application/securing-sql-connection-string_1371

## Encrypt Database Connection String

http://stackoverflow.com/questions/8876936/encrypt-database-connection-string-in-asp-net-web-config

## Browser Autocomplete Enabled

**Table 25: Browser Autocomplete Enabled**

| Application | Class/Procedure | Line(s) of Code |
|---|---|---|
| REDACTED | * | N/A |
| REDACTED | * | N/A |
| REDACTED | * | N/A |
| REDACTED | * | N/A |
| REDACTED | * | N/A |
| REDACTED | * | N/A |
| REDACTED | * | N/A |
| REDACTED | * | N/A |

### Description

When a user submits requests for fields that do not have autocomplete disabled, their information is cached within the browser. A malicious user with access to the local system or a remote attacker that leverages XSS can extract information from the victim's browser. When autocomplete is disabled, modern browsers generally honor this setting and do not cache the information.

Autocomplete was enabled in many places that enable sensitive behaviors including the user login form and within forms used to enter social security numbers.

### Evidence

Please see the Burp and AppScan results.

### Recommendations

To disable autocomplete, the *autocomplete="off"* attribute should be included within forms or individual fields where autocomplete is required to be disabled.

### Additional Information

OWASP Application Security FAQ

https://www.owasp.org/index.php/OWASP_Application_Security_FAQ

Mozilla Autocomplete Guide

https://developer.mozilla.org/en/how_to_turn_off_form_autocompletion

Turning Off the Autocomplete Feature For a Textbox

http://forums.asp.net/t/1513943.aspx/1

## *Sensitive Information Sent Via HTTP GET*

**Table 26: Sensitive Information Sent Via HTTP GET**

| Application | Class / Procedure | Line(s) of Code |
|---|---|---|
| All applications | | |

### Description

The user's password and social security numbers are sent within HTTP GET requests. This will cause the password to be cached within a user's history, exposing it to theft through attacks such as XSS as well as local access to the user's system. Additionally, there may be servers in transit between the client and the server where logging may occur such as within reverse proxy servers or within application server logs. In the event those systems were breached, user passwords and social security numbers would be exposed in plain text.

### Evidence

**Figure 52: Social security number (pin) sent within an HTTP GET request within the REDACTED application.**

### Recommendations

Utilize the HTTP POST method to submit passwords and social security numbers rather than the GET method. This will remove the parameters from the user's browser history and will also decrease the likelihood of unanticipated logging in transit to the server.

### Additional Information

N/A

## *Site Lacks ClickJacking Defense*

**Table 27: Site Lacks ClickJacking Defense**

| Application | Class / Procedure | Line(s) of Code |
|---|---|---|
| REDACTED | * | N/A |
| REDACTED | * | N/A |
| REDACTED | * | N/A |
| REDACTED | * | N/A |
| REDACTED | * | N/A |
| REDACTED | * | N/A |
| REDACTED | * | N/A |
| REDACTED | * | N/A |

### Description

ClickJacking is a UI Redress Attack that allows an attacker to utilize transparent or opaque layers to trick users into clicking on buttons or other controls that trigger state changing operations. The attacker is able to hijack the clicks intended for their page and is able to route them to another application such as those owned by REDACTED.

A potential use for an attacker would be to utilize this within a social engineering attack. A phishing email could be used to trick a victim into visiting a website to enter information and click on buttons. The REDACTED application could be carefully placed underneath what the user actually sees, and the result would be unauthorized transactions executing within REDACTED’s application.

### Evidence

Please see the Burp and AppScan results.

### Recommendations

Configure the application or web server to set the X-FRAME-OPTIONS: Deny HTTP response header. This will instruct browsers to not allow the site to be loaded within a frame.

## *HTTP Response Contains Plain Text Credentials*

**Table 28: HTTP Response Contains Plain Text Credentials**

| Application | Class / Procedure | Line(s) of Code |
|---|---|---|
| REDACTED | REDACTED | 137 |

### Description

The REDACTED application returns a user's password to them in plain text after logging into the application. Within the page's source code, the password is stored within a hidden form field. Due to the presence of widespread caching within the application, this can allow the user's plain text password to persist indefinitely on their local system.

### Evidence

**Figure 53: The user's password displayed within an HTTP response.**

### Recommendations

If a legitimate business purpose does not exist, remove the functionality that renders the plain text password within the response page. After authentication, the user should be identified by the application utilizing the session token. Therefore, passwords should not be required after authenticating.

## *Sensitive Information Logged*

**Table 29: Sensitive Information Logged**

| Application | Procedure / Class | Line(s) of Code |
|---|---|---|
| REDACTED | REDACTED | 62-65 |
| REDACTED | * | N/A |
| REDACTED | * | N/A |
| REDACTED | * | N/A |
| REDACTED | * | N/A |
| REDACTED | * | N/A |
| REDACTED | * | N/A |
| REDACTED | * | N/A |
| REDACTED | * | N/A |

### Description

Throughout the applications, many sensitive values are logged within plain text including social security numbers, user passwords, and other highly sensitive data. While logging and auditing are essential for both troubleshooting as well as reconstructing security events, it is important to ensure that logging does not place sensitive information at risk.

### Evidence

**Figure 54: Social security numbers being logged in plain text.**

### Recommendations

Perform a comprehensive review of the information being logged by each application. Determine if the information being logged has a legitimate purpose or usefulness to support operational needs. If a specific value such as a password or other sensitive identifier is determined to not be required for troubleshooting purposes, remove that information from being logged.

Additionally, ensure that all logs are backed up in a secure manner and are never accessible by remote users.

### Additional Information

OWASP Logging Cheat Sheet

https://www.owasp.org/index.php/Logging_Cheat_Sheet

## *Lack of Account Lockout*

**Table 30: Lack of Account Lockout**

| Application | Class / Procedure | Line(s) of Code |
|---|---|---|
| REDACTED | REDACTED | 10-325 |

### Description

Within the REDACTED and REDACTED applications, failed login attempts are tracked via session variables that are incremented by one every time a failed login occurs. While the failed login count is tracked within a session variable, it is not tracked in persistent storage such as a database. This behavior allows for an attacker to request a new cookie by not providing a previous cookie that identified the session in order to clear the failed login counter. Combined with a weak password policy as well as well-known, predictable Social Security Numbers, it is possible to launch fully automated brute force attacks against the authentication mechanism.

As an example, if a user attempts to log in incorrectly three consecutive times, the failed login counter will exceed its threshold and will disallow further attempts by that session identifier to login for a period of time. However, if the attacker does not provide the cookie on subsequent requests, the application will assign the client a new session token. With a new session token, any variables tracked by previous tokens are not applicable to the user at that point.

### Evidence

REDACTED's login function does not lock a user's account at the server when they attempt to log in too many times with an invalid password. *The maxInvalidLoginSessionAttempts* variable does not appear to be updated in a manner that triggers account lockouts at the server as it is only tracked client-side.

**Figure 55: REDACTED's login function does not lock a user's account at the server.**

### Recommendations

Ensure that all failed login attempts are tracked within the database or a persistent form of storage that cannot be modified by an attacker. The session variable should not be used to track this value, as an attacker can disassociate himself from this value and continue to launch attacks without locking accounts out.

### Additional Information

OWASP Authentication Cheat Sheet

[https://www.owasp.org/index.php/Authentication_Cheat_Sheet](https://www.owasp.org/index.php/Authentication_Cheat_Sheet)

# 4. RISK ASSESSMENT

The purpose of this risk assessment is to document the risks to the applications resulting from the identified threats and vulnerabilities and the efforts designed to reduce those risks through the use of security controls.

The methodology used is based on a qualitative approach to assessing risk; thus, no numerical values are calculated. Rather, a rating of high, medium, or low was assigned based on established definitions, analysis of the system and provided information, and the expertise of the risk assessment team. TNCG developed the methodology used to perform the risk assessment for the REDACTED applications through use of the guidelines outlined in the NIST SP 800-30, which provides a foundation for an effective risk management program for federal organizations that process sensitive information.

The risk assessment enables management to make informed risk-based business decisions without the use of complex mathematical formulas..

The level of risk is determined by evaluating the following factors:

- All collected risk-related attributes related to threats, vulnerabilities, assets and resources, and current controls;
- The associated likelihood that a vulnerability could be exploited by a potential threat; and
- The impact if a vulnerability was exploited (e.g., magnitude of loss resulting from such exploitation).

The results of the risk assessment are included in the table below along with the risk assessment methodology that was used.

**Table 31: Risk Assessment**

| Risk Assessment Results |
|---|
| Extensive risk assessment matrix. Please see embedded file “REDACTED Risk Assessment Matrix.doc and Risk Assessment Methodology.” |

# 5. MAJOR FINDINGS AND RECOMMENDATIONS

This section contains an overview of selected recommendations that are suggested to mitigate the findings that were identified throughout this exercise. Each recommendation is assigned a severity level that describes what the risk level would be if the recommendation was not implemented. The severity level is based on the following definitions:

- **HIGH**: If exploited, this vulnerability would yield complete control of the subject system or access to extremely sensitive data to attackers, severely disrupting system operations and integrity.
- **MEDIUM**: While not directly leading to a system security breach, if exploited, this vulnerability may play a significant role in combination with other vulnerabilities or pertinent system information available to an attacker.
- **LOW**: A vulnerability that is unlikely in itself to lead directly to a compromise of a system, but can in some way aid an attacker indirectly in mounting attacks against the subject system.

The recommendations are also assigned a level of effort that describes how difficult or expensive it would be to implement the recommendation. The level of effort is based on the following definitions:

- **HIGH**: In order to implement the recommendation, it will take a very high-level of effort, in terms of both people and cost. This would involve outside assistance and/or third-party products. In order to implement this effectively, it would also involve a large amount of research and testing. This would be considered a long-term or major project. The estimated cost in order to implement this recommendation is greater than $100,000.00.
- **MEDIUM**: In order to implement the recommendation, it will take a MEDIUM level of effort, in terms of both people and cost. This could involve outside assistance and/or third-party products, but most likely could be completed with in-house resources. This would be considered a medium length project. The estimated cost in order to implement this recommendation is between $20,000.00 and $100,000.00.
- **LOW**: In order to implement the recommendation, it will take a very low-level of effort, in terms of both people and cost. This is something that can be implemented very quickly at very little cost. This would be considered a short-term or simple project. The estimated cost in order to implement this recommendation is less than $20,000.

For specific and complete listings of all recommendations, please see the specific Vulnerability Summary Matrix located in the respective appendix.

- Review all findings (i.e. SQLi, XSS) that are a result of data not being validated and filtered correctly and implement code changes to mitigate these vulnerabilities.

  Severity-Level: **HIGH**

  Level of Effort: **MEDIUM**

- Review all open ports that are listed in the Nmap scans and verify that they are needed for a legitimate business purpose. Insecure protocols such as File Transfer Protocol (FTP) should be replaced with a secure alternative similar to SSH.

  Severity-Level: **MEDIUM**
  Level of Effort: **LOW**

- Apply the security patches and hot-fixes that are identified in the Vulnerability Matrix on all servers.

  Severity-Level: **HIGH**
  Level of Effort: **LOW**

- Provide security coding training to developers on a quarterly basis.

  Severity-Level: **MEDIUM**
  Level of Effort: **MEDIUM**

- Implement a Web Application Firewall (WAF) in order to provide an additional layer of protection at the web application level.

  Severity-Level: **MEDIUM**
  Level of Effort: **MEDIUM**

- Mitigate all findings in the application code and take steps to develop and implement a secure coding standard process to be followed by REDACTED developers.

  Severity-Level: **HIGH**
  Level of Effort: **MEDIUM**

- Implement a mechanism for REDACTED to monitor and review IDS and other logs for those systems and application being hosted at REDACTED. This can be done by transferring the current logs into REDACTED's internal SIEM or by placing a REDACTED managed and controlled IDS/IPS solution at the facility.

  Severity-Level: **MEDIUM**
  Level of Effort: **MEDIUM**

- Consider implementing a database specific IDS, such as dbProtect, to provide an additional layer of protection at the database level.

  Severity-Level: **MEDIUM**
  Level of Effort: **MEDIUM**

- Implement a data leakage prevention (DLP) solution to help prevent the exfiltration of sensitive data maintained on the systems.

Severity-Level: **MEDIUM**
Level of Effort: **MEDIUM**

# 6. GUIDE TO VULNERABILITY MATRIXES

Appendices A through E contain vulnerability matrices. Each of the vulnerability matrices summarizes the vulnerabilities from this application risk assessment and SeNet's recommendations to REDACTED for mitigating identified risks. Each vulnerability is assigned a severity level based on the following definitions:

- **HIGH**: If exploited, this vulnerability would yield complete control of the subject system or access to extremely sensitive data to attackers, severely disrupting system operations and integrity.
- **MEDIUM**: While not directly leading to system security breach, if exploited, this vulnerability may play a significant role in combination with other vulnerabilities or pertinent system information available to an attacker.
- **LOW**: A vulnerability that is unlikely in itself to lead directly to a compromise of a system, but can in some way aid an attacker indirectly in mounting attacks against the subject system.
- **Not Applicable (N/A)**: Does not necessarily indicate a vulnerability. It is used when a risk level cannot be assigned. Most often it is used when a service is detected. For example, if port scans identify port 25 (SMTP) open, it is not necessarily a vulnerability because the service may be needed for a business purpose. However, unnecessary services are often enabled by default and are not needed.

The risk level to which a system is exposed is determined by a number of factors, as indicated in the following subsections.

## 5.1 THREAT(S) AGAINST THE SYSTEM

A threat-source is defined as any circumstance or event with the potential to cause harm to an information system. Common threat sources include

- **Natural Threats**: Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other events.
- **Human Threats**: Events that are either enabled by or caused by human beings such as unintentional acts (inadvertent data entry) or deliberate actions (network based attacks, malicious software upload, unauthorized access to confidential information).
- **Environmental Threats**: Long-term power failure, pollution, chemicals, liquid leakage.

## 5.2 TECHNICAL AND OPERATIONAL VULNERABILITIES

A flaw or weakness in system security procedures, design, implementation, internal controls, etc., that could be exercised and could result in a violation of the system's security policy. Vulnerabilities can be accidentally triggered or intentionally exploited. Some proactive methods used to identify vulnerabilities include:

- Automated vulnerability scanning
- Network mapping
- Security testing and evaluation
- Penetration testing.

## 5.3 MITIGATING SECURITY CONTROLS (TECHNICAL, PROCEDURAL)

Technical controls are those safeguards incorporated in computer hardware, software, or firmware (e.g., anti-virus software, firewalls, and intrusion detection). Operational controls are those operational procedures and personnel and physical security measures established to provide an acceptable level of protection for computing resources, including acceptable usage policy, disaster recovery (DR), and security awareness training.

## 5.4 LIKELIHOOD OF SUCCESSFUL EXPLOITATION

Factors that govern the threat likelihood include threat-source motivation and capability, the nature of the vulnerability, and the effectiveness of current countermeasures.

## 5.5 IMPACT ON MISSION

The impact of a security event can be described in terms of mission impacts attributed to loss or degradation of the five security goals: integrity, availability, confidentiality, accountability, and assurance.

Under this task, the TNCG Team concentrated on identifying technical vulnerabilities associated with the perimeter security. As such, the other factors discussed above were outside the scope of this task.

Within the limited scope of technical vulnerabilities, TNCG attempted to categorize their severity based on the direct impact on the system itself (without regard to its possible mission impact). For example, we ranked the severity of a Web server vulnerability (e.g., susceptibility to remote command line execution) the same regardless if the Web server was sitting directly on the Internet, in a firewalled DMZ, on an internal segment, or was a stand-alone system. The severity level is intended to provide a prioritization scale for addressing all technical vulnerabilities found during the vulnerability assessment.

**Note:** The vulnerabilities listed in the Vulnerability Summary Matrix are the vulnerabilities that TNCG believes may cause the greatest risk. Not all vulnerabilities that were discovered by the various scanners are reported in the matrix. TNCG made decisions based on past experiences and industry knowledge to not report low-level or incorrect vulnerabilities.

**Note**: The recommendations provided in the vulnerability matrix should first be evaluated to determine if they are appropriate for REDACTED’s environment. TNCG suggests that all recommendations be applied to test or non-production systems to verify that the changes do not cause any adverse effects to the production system or network.

# APPENDIX A: SERVICES MATRIX

**Table 32: Services Matrix**

| Port Number | Host |
|---|---|
| Please see embedded file “REDACTED Services Matrix.docx.” | |

# APPENDIX B: WEB APPLICATION VULNERABILITIES MATRIX

**Table 33: Web Application Vulnerabilities Matrix**

| Finding Number | Description | Implication | Recommendation | Host |
|---|---|---|---|---|
| Extensive web application vulnerability matrix. Please see embedded file "REDACTED Web TVA Table.docx." | | | | |

# APPENDIX C: CODE REVIEW VULNERABILITY MATRIX

**Table 34: Code Review Vulnerability Matrix**

<table>
<tr><th>Finding Number</th><th>Description</th><th>Implication</th><th>Recommendation</th><th>Host</th></tr>
<tr><td colspan="5">Extensive code review vulnerability matrix. Please see embedded file “REDACTED Application Level TVA Table.docx.”</td></tr>
</table>

# APPENDIX D: SERVER VULNERABILITY MATRIX

**Table 35: Server Vulnerability Matrix**

| Finding Number | Description | Implication | Recommendation | Host |
|---|---|---|---|---|
| Extensive server vulnerability matrix. Please see embedded file "REDACTED Server TVA.doc." | | | | |

# APPENDIX E: DATABASE VULNERABILITY MATRIX

**Table 36: Database Vulnerability Matrix**

| Finding Number | Description | Implication | Recommendation | Host |
|---|---|---|---|---|
| Extensive database vulnerability matrix. Please see embedded file “REDACTED Database TVA.docx.” | | | | |

# APPENDIX F: PLANS OF ACTION AND MILESTONES

Table 37: REDACTED POA&MS

| Port Number | Host |
|---|---|
| Extensive code review matrix. Please see embedded file “REDACTED POAM.doc.” | |

# APPENDIX G: SCREEN CAPTURES

Due to size this was delivered separately.

Table 38: Screen Capture Document

| Screenshots |
|---|
| Extensive screen shot document. Please see embedded file “REDACTED Screenshots.docx.” |

# APPENDIX H: RAW DATA RESULTS

All test results are included separately on a CD-ROM disk along with the final report.  These include, but are not limited to:

- Nessus Scans Results
- Burp Suite Reports
- Burp Session Data
- AppScan Reports
- AppScan Session Data
- Fortify Scan Results
- Nmap Scan Results
- AppDetective Scan Results