Statement of Work

Security Services

Lake County, Illinois

October, 2018

GSA Contract: GS-35F-511T

MTM Technologies

www.mtm.com

Submitted by:

Kristin Johnson,
Cybersecurity Solutions Advisor

Matt Wilson, Account Manager

Statement of Confidentiality

The information in this document is confidential and proprietary. It has been made available to this MTM Security Client exclusively. No portion of this document should be disclosed or disseminated without the expressed written consent of Client.

---

1. Security Services

1.1 Overview

MTM Technologies ("MTM") will deliver the selected projects, with the added benefit of a Client Team, to Lake County IL ("Client") and ensure successful delivery and customer satisfaction. All Security Services include an assigned vCISO, Client Lead and Security Program Manager to proactively plan and strategize, and to ensure the success of the engagement.

1.2 Objectives

The objectives of this service are as follows:

- Delivery a suite of services as a single continuous effort
- Address unplanned issues in a quick and effective manner
- Solve problems using the virtual cybersecurity team
- Provide an assigned team to help ensure successful service delivery

1.3 Deliverables

MTM will deliver the planned services in a managed and organized manner. MTM will provide the following:

- A security roadmap (or project plan)
- An assigned vCISO
- A Client Team consisting of an assigned Client Lead and Security Program Manager, and other supporting members
- Consulting and advisory services via access to the virtual cybersecurity team, including industry experts, subject matter experts and virtual CISOs
- A Client Relationship Manager
- Quarterly service reviews
- Periodic status reports
- Retained Incident Response Team

1.4 Options

All Managed Services include a minimum amount of Consulting to ensure unplanned work and business-critical business issues can be resolved in a timely and effective manner. In some cases, additional consulting effort may be anticipated due to complexity or other factors.

2. Executive Summary

2.1 Overview

This Statement of Work will provide Client with the following service(s):

1. Penetration Testing
2. Vulnerability Assessment (Elections and Scada systems)
3. Risk Assessment
4. Data Classification
5. Policy Development
6. Consulting

2.2 Engagement

Unless otherwise specified here, services will be delivered as a Managed Security Service (MSS).

☒ Deliver Services as a Managed Security Service over __12__ Months

☐ Deliver Services as a Co-Managed Security Service Over _____ Months

☐ Deliver Services as a Project

2.3 Genesis

The intent of this proposal is two-fold. The high-priority focus is for MTM to perform Internal and External Vulnerability Assessments, as well as Penetration Testing on each of Lake County, Illinois' Election and Scada Systems. The second objective is for MTM to partner with Lake County, Illinois in executing their cybersecurity strategy and objectives to build out a long-term, sustainable and defensible program.

3. Penetration Testing

3.1 Service Overview

A Penetration Test, often called "red teaming" or a "red team exercise" is the practice of simulating as closely as possible the effect that cyber threats could have on your business. It is a simulation of a real-world attack on targeted assets using the same tools and techniques that modern cybercriminals use.

During the Penetration Test, MTM will attempt to partially or entirely exploit Client's critical assets, including:

- Personnel, via phishing and other social engineering attacks;
- Privileged system accounts, including administrators;
- Bank accounts and other financial accounts;
- Regulated data, including PII, PHI and credit card information;
- Intellectual property, including corporate secrets, plans, reports, blueprints and other valuable assets;
- Facilities, including data centers, protected areas, offices and other secure areas.

In the event that Client is considered a "high value target", MTM offers a longer-term and more intensive test, called an Advanced Persistent Penetration Test (APPT). The Advanced Persistent Penetration Test addresses offers the following benefits:

1. Testing is choreographed over longer periods of time, allowing for different attack methods, more successful exploits and lower attack signatures;
2. Testing may leverage zero-days, vulnerabilities and exploits that are identified and existent over a longer period of time;
3. Testing occurs over longer periods of time, allowing fingerprint data to age and ripen and thus become more valuable.

Additionally, MTM offers a Web Application Penetration Test designed to identify weaknesses, vulnerabilities and exploits in web applications, based on the globally recognized Open Web Application Security Project (OWASP) Testing Guide.

3.2 Objectives

The objectives of this initiative are as follows:

- Assess how Client's security controls and protective measures will withstand a real-world attack
- Identify exploitable vulnerabilities in Client's environment
- Assess Client's incident detection, reporting and response capabilities
- Ensure the protection of critical assets
- Ensure compliance with regulatory requirements
- Develop a prioritized, actionable plan for risk mitigation

3.3 Methodology

This Penetration Test is based on the following regulations and standards:

- NIST SP 800-115 Guide to Information Security Testing and Assessment
- The Penetration Testing Execution Standard (PTES)
- Payment Card Industry Data Security Standards (PCI-DSS) 3.x
- ISO 27002:2013

This Penetration Test consists of the following phases:

1. *Planning* – Preparation necessary to conduct an effective test, including:
   a. *Scope Definition* – Identifying the assets that will be the focus of the test, including people, process and technology;
   b. *Schedule Development* – Scheduling, project plan creation and resource identification.
   c. *Rules of Engagement Definition* – Determination of primary contacts, data handling requirements and mandatory communications for events that may arise during testing.
2. *Testing* – Active discovery and exploitation of Client assets.
3. *Documentation* – Documentation of all deliverables, including summary and detailed findings.
4. *Reporting* – Presentation of findings to Client.

Attack Vectors

The following are attack vectors typically included in MTM penetration tests. Depending on the goals of the test, attack vectors are chosen and the scope of the engagement directed to target only specified assets and/or known vulnerabilities.

- External Network - Attacks are made against externally accessible resources (public web servers, Internet hosted systems, cloud services, remote access systems, etc.)
- Internal Network - Attacks are made against internal network resources; servers, network infrastructure, workstations, etc. Access may be provided to the Internal network or access may be obtained through other attack vectors.
- Wireless Network – Attacks are performed against wireless networks and wireless clients. This may provide credentials to target wireless networks, or compromise wireless clients.
- Social Engineering – The manipulation of company personnel to perform inappropriate actions such as divulging confidential or sensitive information, providing access to restricted areas, or running malicious software. Some common attack vectors include emails sent in an attempt to fraudulently obtain confidential information (such as usernames and passwords), phone calls made to individuals in an attempt to obtain confidential information, and malicious software loaded onto USB or other removable media and placed in high traffic areas with the goal of obtaining remote access to targeted devices.
- Physical - Attempts are made to gain physical access to sensitive or restricted areas - server rooms, executive/employee offices, data closets, etc. - simulating the methods of a malicious intruder. This may involve the manipulation of personnel depending on target environments, and/or malicious devices may be planted to provide remote access to target systems.

3.4 Scope

The scope of this Penetration Test is bounded by the people, process and technology that are legally owned by Client.

During the Planning phase, detailed Rules of Engagement and methodology will be established describing:

- The extent of the authority of the MTM penetration testing team to perform the actions prescribed herein;
- The procedures that are to be followed for the care and handling of any data that is compromised as the result of the actions prescribed herein.
- Coordination of attack teams: Red Team / Blue Team
- Analysis and preparation: Black box / White Box / Grey box
- Scenario Planning: External Attacker, Hacktivist, Insider Threat, Competitor, and others

3.5 Deliverables

MTM will produce the following deliverables:

1. *Kickoff Meeting* – MTM will host a kickoff meeting to conduct introductions and familiarize Client with the initiative. This meeting will be no longer than sixty (60) minutes and it is intended to review the objectives, methodology, scope and deliverables in the Statement of Work.
2. *Project Plan* – MTM will deliver a project plan that describes the tasks, milestones, resources, and project start and end dates of each major deliverable.
3. *Findings and Recommendations* – MTM will deliver a report clearly identifying all findings, weaknesses and vulnerabilities related to the initiative and the relevant details of each, as well as illustrating risk mitigation recommendations related to the initiative.
4. *Artifacts* – MTM will deliver examples of evidence generated by the test, including harvested credentials, screenshots, images and videos.
5. *Findings Review* – MTM will schedule a meeting, onsite or virtual, to review the results of the initiative.
6. *Transition Meeting* – MTM will host a transition meeting to assist Client with next steps.

3.6 Options

MTM provides comprehensive penetration testing solutions designed to meet the most common requirements as well as more specialized requests.

Standard Penetration Test - Includes three of the following attack vectors. More than three attack vectors may be selected, which results in additional attack time.

- ☒ External Network – Year 1
- ☒ Social Engineering, Remote (Phishing, Vishing, Smishing*)
- ☒ Internal Network, remote – Year 1
- ☐ Social Engineering, on-site
- ☐ Wireless Network, on-site
- ☐ Physical, on-site

*Smishing requires the cellular or land line to be owned by the business (cannot be a personal line).

The following is a sampling of tools used during the Penetration Test:

- Google – Google hacking, target research and reconnaissance
- NMAP – Network mapping, custom packet configuration, vulnerability discovery
- PeepingTom - Webserver screenshot utility
- Alpha - Proprietary backdoor and remote administration tool
- theHarvester – Recon and intelligence gathering tool
- Nessus – Vulnerability scanning
- FIERCE – DNS mapping and mapping
- Foca – Metadata extraction tool
- Maltego – Data mining
- MetaSploit – Target scanning, IPS obfuscator, exploit engine
- The Social Engineering Toolkit (SET) – Penetration testing and Social-Engineering tool

4. Vulnerability Assessment

4.1 Service Overview

A Vulnerability Assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in systems. Systems may consist of applications, networks, operating systems, devices and hardware, and other assets or more complex groupings of all of these.

Vulnerabilities exist in all technology assets. By taking an inventory of technology assets in question and identifying their vulnerabilities, we can create actionable plans to reduce overall vulnerability based on rankings and other decisions.

4.2 Objectives

The objectives of this initiative are as follows:

- Identify technical vulnerabilities in Client's environment
- Implement the Vulnerability Management process
- Ensure the protection of critical assets
- Ensure compliance with regulatory requirements
- Develop a prioritized, actionable plan for risk mitigation

4.3 Methodology

This Vulnerability Assessment is based on the following regulations and standards:

- NIST SP 800-40 Guide to Enterprise Patch Management Technologies
- Payment Card Industry Data Security Standards (PCI-DSS) 3.x
- NIST SP 800-53 Security and Privacy Controls for Federal Information Systems
- ISO 27002:2013

This Vulnerability Assessment consists of the following phases:

1. *Planning* – Preparation necessary to conduct an effective test, including:
   a. *Scope Definition* – Identifying the assets that will be the focus of the test, including people, process and technology;
   b. *Schedule Development* – Scheduling, project plan creation and resource identification.

2. *Assessment* – Identification, analysis and prioritization of technical vulnerabilities by performing the following:
   a. *Configuration Assessment* – Analysis of configuration settings in devices, applications, networks, operating systems and other technology assets.
   b. *Vulnerability Scanning* – Scanning of assets for known vulnerabilities. This can usually be performed onsite or offsite.
   c. *Analysis* – Identification of false-positives, false-negatives and prioritization of vulnerabilities.
3. *Documentation* – Documentation of all deliverables, including summary and detailed findings.
4. *Presentation* – Presentation of findings to Client.

4.4 Scope

The scope of this Vulnerability Assessment is bounded by the technology assets that are legally owned by Client.

During the Planning phase, detailed Rules of Engagement will be established describing:

- The extent of the authority of the MTM team to perform the actions prescribed herein;
- The procedures that are to be followed for the care and handling of any issues resulting from the actions prescribed herein.

During the Planning phase, Client should identify any technology assets that should be explicitly included or excluded in the assessment.

Any of all of the following activities may be included in the Vulnerability Assessment:

- *External Vulnerability Assessment* – The external vulnerability assessment identifies technical vulnerabilities accessible via the Internet, including:
  - Port and service identification
  - Application vulnerabilities
  - Configuration issues
  - Outdated services and software
  - SNMP vulnerabilities
  - Web server vulnerabilities
  - Root-level exploits

- *Internal Vulnerability Assessment* – The internal vulnerability assessment identifies technical vulnerabilities accessible only to the organization (not accessible via the Internet), including:
  - Patch levels for operating systems
  - Patch levels for third-party software
  - Registry and file-related security vulnerabilities
  - Configuration-related security vulnerabilities
- *Network Security Assessment* – The network security assessment identifies network security weaknesses in the following areas:
  - Physical security
  - Layer 2 security
  - Layer 3 segmentation and VLANs
  - Firewall and router security
  - Secure DMZ configuration
  - WAN and remote office connectivity
  - Business partner connectivity
  - Remote Access
  - Wireless

4.5 Deliverables

MTM will produce the following deliverables:

1. *Kickoff Meeting* – MTM will host a kickoff meeting to conduct introductions and familiarize Client with the initiative. This meeting will be no longer than sixty (60) minutes and it is intended to review the objectives, methodology, scope and deliverables in the Statement of Work.
2. *Project Plan* – MTM will deliver a project plan that describes the tasks, milestones, resources, and project start and end dates of each major deliverable.
3. *Detailed Findings* – MTM will deliver a report clearly identifying all technical vulnerabilities related to the initiative and the relevant details of each.
4. *Detailed Recommendations* – MTM will deliver a report clearly illustrating risk mitigation recommendations related to the initiative.
5. *Findings Presentation* – MTM will deliver an onsite, in-person presentation to review the results of the initiative.
6. *Transition Meeting* – MTM will host a transition meeting to assist Client with next steps.

4.6 Options

Scanning Options

☒ __2__ External Vulnerability Assessment(s) – Year 1, Elections and Scada

☒ __2__ Internal Vulnerability Assessment(s) – Year 1, Elections and Scada

Assessment Options

☒ __1__ Network Security Assessment(s) – Year 1

For the purposes of this proposal:

- Year 1 Vulnerability Assessments will focus on the Elections and Scada systems, each being assessed separately.

The External Vulnerability Assessment includes a penetration test on the respective findings.

5. Risk Assessment

5.1 Service Overview

All businesses face cybersecurity risks. Risks to critical assets may be intentional or negligent, they may come from determined criminals or careless employees, they may cause minor inconveniences or significant damages and they may result in severe financial penalties, loss of public trust and damage to corporate reputation.

A Risk Assessment is the single-most important step a business can take to ensure the security of critical assets, including money, regulated data, intellectual property and reputation. It is also an important component for achieving regulatory compliance.

This Risk Assessment will provide a comprehensive evaluation of Client's cybersecurity risks and a plan for effectively mitigating those risks.

5.2 Objectives

The objectives of this initiative are as follows:

- Identify cybersecurity risks in accordance with NIST SP 800-30 standard for Risk Assessment
- Ensure the protection of critical assets
- Ensure compliance with regulatory requirements
- Develop a prioritized, actionable plan for risk mitigation
- Initiate the Risk Management process

5.3 Methodology

This Risk Assessment is based on the following regulations and standards:

- NIST SP 800-30 Risk Management Guide
- NIST SP 800-37 Applying the Risk Management Framework
- NIST SP 800-53 Security and Privacy Controls for Federal Information Systems

This Risk Assessment consists of the following phases:

1. *Planning* – Preparation necessary to conduct an effective assessment, including:

a. *Asset Inventory Development* – The identification of assets (people, process and technology) that are directly or indirectly related to the creation, storage, processing or transmission of classified or otherwise important data;
b. *Scope Definition* – Identifying the assets that will be the focus of the assessment, including people, process and technology;
c. *Schedule Development* – Scheduling, project plan creation and resource identification.

2. *Assessment* – Evaluation of cybersecurity controls applied to the assets defined in the Planning phase, including:
   a. *Interviews* – Interviews with Subject Matter Experts, business leaders and other parties with knowledge of Client's cybersecurity controls;
   b. *Artifact Analysis* – Evaluation of policies, procedures, plans, reports, logs and other artifacts;
   c. *Risk Analysis* – Prioritization of identified risks.
      i. Identify threats and vulnerabilities
      ii. Assess current security measures
      iii. Determine the likelihood of threat occurrence
      iv. Determine the potential impact of threat occurrence
      v. Determine the level of risk
3. *Documentation* – Documentation of all deliverables, including summary and detailed assessment findings.
4. *Presentation* – Presentation of findings to Client.

5.4 Scope

The scope of this Risk Assessment is bounded by the people, process and technology that create, process, store or transmit digital assets.

The scope of the cybersecurity controls that will be evaluated during the Risk Assessment are derived from the global NIST SP 800-53 standard for security. These security controls include the following domains:

NIST SP 800-53

1. Access Control
2. Awareness and Training
3. Audit and Accountability
4. Certification, Accreditation, and Security Assessments

5. Configuration Management
6. Contingency Planning
7. Identification and Authentication
8. Incident Response
9. Maintenance
10. Media Protection
11. Physical and Environmental Protection
12. Planning
13. Personnel Security
14. Risk Assessment
15. System and Services Acquisition
16. System and Communications Protection
17. System and Information Integrity
18. Program Management

5.5 Deliverables

MTM will produce the following deliverables:

1. *Kickoff Meeting* – MTM will host a kickoff meeting to conduct introductions and familiarize Client with the initiative. This meeting will be no longer than sixty (60) minutes and it is intended to review the objectives, methodology, scope and deliverables in the Statement of Work.
2. *Project Plan* – MTM will deliver a project plan that describes the tasks, milestones, resources, and project start and end dates of each major deliverable.
3. *Summary Findings* – MTM will deliver a report summarizing the findings of the initiative.
4. *Detailed Findings* – MTM will deliver a report clearly identifying all findings, weaknesses and vulnerabilities related to the initiative and the relevant details of each.
5. *Detailed Recommendations* – MTM will deliver a report clearly illustrating risk mitigation recommendations related to the initiative.
6. *Findings Presentation* – MTM will deliver an onsite, in-person presentation to review the results of the initiative.
7. *Transition Meeting* – MTM will host a transition meeting to assist Client with next steps.

5.6 Options

Service Delivery Options

☒ Executive

Assessment Options

☐ Third-Party Risk Assessment Evaluation
☐ Asset Inventory Development
☒ __1__ MTM Risk Assessments
☒ __1__ MTM Risk Assessment Updates (Year 3, PO Pending)
☒ __1__ Interview Location(s)
☒ __1__ Findings Presentation(s)

Other Options (Please Describe)

6. Data Classification

6.1 Service Overview

In its purest form, cybersecurity is about protection of information assets. Creating and maintaining an accurate inventory of data is a critical step in the implementation of reasonable and effective cybersecurity controls and enablement of risk management.

This process of data classification enables effective risk management in many scenarios, including vendor management and contract review, and control design and implementation. It also enables prioritization of investment, creation of internal audit controls, ownership and responsibilities for information and vendor relationship, and helps to support decision making around people, process and technology.

The Data Classification project will provide an asset inventory, policies and procedures necessary to set the foundation for a successful cybersecurity program and a corrective action plan to remediate gaps discovered as part of the process.

6.2 Objectives

The objectives of this initiative are as follows:

- Identify and inventory business information and confidentiality, integrity and availability requirements;
- Identify ownership (departmental level);
- Where information is stored, processed and handled;
- Identify business partners or 3rd parties that have access to information;
- Prepare for information security control implementation.

6.3 Methodology

The Data Classification Project is based on the following regulations and standards:

- FIPS 199 Standards for Security Categorization of Federal Information and Information Systems
- NIST SP 800-53 Security and Privacy Controls for Federal Information Systems

This Data Classification Project consists of the following phases:

5. *Planning* – Preparation necessary to conduct an effective data classification effort, including:
    a. *Interview Schedule* – The identification of departments and business partners that are directly or indirectly related to the creation, storage, processing or transmission of data;
    b. *Scope Definition* – Identifying the resources that will be the focus of the project, and those that may be excluded.
    c. *Schedule Development* – Scheduling, project plan creation and resource identification.
6. *Discovery* – Identification of data assets, as discovered via departmental interviews defined in the planning phase, including:
    a. *Interviews* – Interviews with Subject Matter Experts, business leaders and other parties with knowledge of Client's cybersecurity controls;
    b. *Artifact Analysis* – Evaluation of policies, procedures, plans, reports, logs and other artifacts;
    c. *Risk Analysis* – Prioritization of identified risks.
        i. Identify threats and vulnerabilities
        ii. Assess current security measures
        iii. Determine the likelihood of threat occurrence
        iv. Determine the potential impact of threat occurrence
        v. Determine the level of risk
7. *Documentation* – Documentation of all deliverables, including summary and detailed assessment findings.
8. *Presentation* – Presentation of findings to Client.

6.4 Scope

The scope of the Data Classification Project includes all data sets owned or handled by the Organization.

6.5 Deliverables

MTM will produce the following deliverables:

8. *Kickoff Meeting* – MTM will host a kickoff meeting to conduct introductions and familiarize Client with the initiative. This meeting will be no longer than sixty (60) minutes and it is intended to review the objectives, methodology, scope and deliverables in the Statement of Work.

9. *Project Plan* – MTM will deliver a project plan that describes the tasks, milestones, resources, and project start and end dates of each major deliverable.
10. *Discovery* – MTM will conduct a discovery via departmental interviews to identify and capture data assets and work toward creation of an asset inventory
11. *Data Classification Policies* – MTM will provide a Data Classification and Acceptable Use policy, using the information gained from the discovery and organization-specific information to customize.
12. *Data Classification Procedure* - MTM will provide a Client-specific Data Classification Procedure, using the information gained from the discovery and organization-specific information to customize.
13. *Summary Findings* – MTM will deliver a report summarizing the findings of the initiative.
14. *Asset Inventory* – MTM will deliver an asset inventory clearly identifying all discovered data sets, with classifications.
15. *Detailed Recommendations* – MTM will deliver a report clearly illustrating recommendations related to the initiative.
16. *Findings Presentation* – MTM will deliver an onsite, in-person presentation to review the results of the initiative.
17. *Transition Meeting* – MTM will host a transition meeting to assist Client with next steps and to introduce the Managed Security Services engagement.

7. Policy Development

7.1 Service Overview

A security policy is the primary governance structure for a cybersecurity program. Security policies protect people and information, define expected personnel behaviors, define the organization's position on security, minimize risk and track compliance with regulations and legislation. Information security policies also provide a framework for best practices.

Security policy defines the organization's attitude towards information, and declares internally and externally that information is an asset, the property of the organization, and is to be protected from unauthorized access, modification, disclosure and destruction.

7.2 Objectives

The objectives of this initiative are as follows:

- Develop, document and optionally implement organizational cybersecurity policy
- Establish security expectations for people, process and technology
- Ensure compliance with regulatory requirements
- Define consequences of policy violations
- Establish the Policy Management process

7.3 Methodology

All policies are based on one or more of the following regulations and standards:

- National Institute of Standards in Technology (NIST)
- International Organization for Standardization (ISO:IEC)
- Health Insurance Portability and Accountability Act (HIPAA)
- Family Educational Rights and Privacy Act (FERPA)
- Federal Information Security Management Act (FISMA)
- Federal Information Processing Standards (FIPS)
- North American Electric Reliability Corporate Critical Infrastructure Protection (NERC CIP)
- Payment Card Industry Data Security Standards (PCI-DSS)
- Center for Internet Security Critical Security Controls (SANS)

- United States Computer Emergency Readiness Team (US-CERT)
- Information Technology Infrastructure Library (ITIL)

This Policy Development service consists of the following phases:

1. *Policy Development*
    a. *Policy Format Development* – Organizational style guides and requirements will be reviewed and considered for new policies.
    b. *Policy Review* – Existing information security policies will be reviewed to assess weaknesses and to determine if they can be used as part of the new suite of policy documents.
    c. *Business Objective Incorporation* – Organizational objectives, strategies and principles will be collected, prioritized and prepared for integration into policies. Communications with Subject Matter Experts, organizational leaders and vested parties will be held to ensure accuracy and completeness.
    d. *Security Standards Incorporation* – Appropriate standards, including SANS, NIST and others will be considered as baselines for policy statements.
    e. *Compliance Requirement Incorporation* – Appropriate legal and regulatory language will be considered as baselines for policy statements.
2. *Policy Review* – Draft policies will be presented to the organization's Client policy review committee for initial feedback.
3. *Policy Presentation* – Feedback will be integrated into draft policies and final policies will be presented to Client policy review committee.
4. *Implementation Strategy Development* – A schedule and mechanism for communication of new policies will be developed and prepared for implementation.
5. *Policy Implementation* – New policies will be published, per the strategy developed above.

7.4 Scope

The scope of this Policy Development service is bounded by the people, process and technology that create, process, store or transmit digital assets. Security policy may address any or all of the following security domains:

- Risk Assessment – Processes and procedures for determine Client's risks, risk tolerance and security priorities

- Security Policy and Procedures – Development or maintenance of written security policies, and processes for continuous review and revision of policies
- Organization of Information Security – Oversight of infrastructure supporting information security, security issues concerning access by third parties, and security issues created by outsourcing
- Asset Management – Processes and procedures for classifying assets into different classes or types that have appropriate security controls associated with them
- Human Resources Security – Human security issues such as training and the steps taken when hiring or terminating employees
- Physical and Environmental Security – The security of physical assets, including data centers and other controlled areas, and controls for securing assets and equipment
- Communications and Operations Management – Processes and controls in areas such as system planning and acceptance; malware protection, backup and recovery, network management and media management
- Access Control – Controls for user access to information and physical assets, including servers, applications, networks, data centers and data
- Information Systems Acquisition, Development and Maintenance – Application development, cryptography, filesystems, and development and support processes
- Information Security Incident Management – Detecting, responding to and managing security events
- Business Continuity Management – Prevention of disruptions to core business processes due to failures or disasters
- Compliance – Compliance with legal, regulatory, and business requirements

7.5 Deliverables

MTM will produce the following deliverables:

1. *Kickoff Meeting* – MTM will host a kickoff meeting to conduct introductions and familiarize Client with the initiative. This meeting will be no longer than sixty (60) minutes and it is intended to review the objectives, methodology, scope and deliverables in the Statement of Work.
2. *Project Plan* – MTM will deliver a project plan that describes the tasks, milestones, resources, and project start and end dates of each major deliverable.

3. *Security Policy* – MTM will deliver all policies, procedures and plans requested in the Options section of this Statement of Work.
4. *Transition Meeting* – MTM will host a transition meeting to assist Client with next steps.

7.6 Options

Development Options

- ☒ Policy Framework
- ☐ Program (ISMS)
- ☐ _____ Plan(s)
- ☒ _See note below_ Policy(ies)
- ☐ _____ Procedure(s)

Implementation Options

- ☒ Policy Implementation

Other Options (Please Describe)

MTM's Policy Framework Development Option includes these Policies: Information Security Policy and Data Classification Policy.

8. Consulting

8.1 Service Overview

In the event that a standard MTM service does not address the specific and unique needs of Client, a Consulting engagement may be utilized. Consulting engagements can address any cybersecurity function not expressly satisfied by standard engagements. Consulting is also included, by default, with all Managed Solutions. Common work efforts include:

- Addressing business partner and client requests
- providing presentations to stakeholders, prospects or clients
- Assessing impact and risk associated with mergers and acquisitions or contract requirements

8.2 Objectives

The objectives of this initiative are as follows:

- Address specific, unique cybersecurity tasks utilizing industry standards and highly-certified experts

8.3 Methodology

All Consulting efforts leverage industry standards where possible, including:

- National Institute of Standards in Technology (NIST)
- International Organization for Standardization (ISO:IEC)
- Health Insurance Portability and Accountability Act (HIPAA)
- Family Educational Rights and Privacy Act (FERPA)
- Federal Information Security Management Act (FISMA)
- Federal Information Processing Standards (FIPS)
- North American Electric Reliability Corporate Critical Infrastructure Protection (NERC CIP)
- Payment Card Industry Data Security Standards (PCI-DSS)
- Center for Internet Security Critical Security Controls (SANS)
- United States Computer Emergency Readiness Team (US-CERT)
- Information Technology Infrastructure Library (ITIL)

8.4 Scope

The scope of this Consulting engagement is determined by Client needs.

8.5 Consulting Hours

The following apply to all Consulting hours:

1. Available Consulting hours shall accumulate monthly, per the total purchased hours and contract duration in months;
2. Consulting hours are intended to be consumed equally throughout each month of the contract period;
3. Additional Consulting hours may be purchased through a corresponding Change Order;
4. Accumulated but unused Consulting hours may be applied towards other MTM services at the end of the contract period;
5. Accumulated but unused Consulting hours shall expire six months following the end date of the contract.

8.6 Deliverables

MTM will produce the following deliverables:

1. *Kickoff Meeting* – MTM will host a kickoff meeting to conduct introductions and familiarize Client with the initiative. This meeting will be no longer than sixty (60) minutes and it is intended to review the objectives, methodology, scope and deliverables in the Statement of Work.
2. *Project Plan* – MTM will deliver a project plan that describes the tasks, milestones, resources, and project start and end dates of each major deliverable.
3. *Artifacts* – MTM will deliver all reports, analysis, findings and other documentation resulting from the initiative.
4. *Detailed Recommendations* – MTM will deliver a report clearly illustrating risk mitigation recommendations related to the initiative.
5. *Transition Meeting* – MTM will host a transition meeting to assist Client with next steps.

8.7 Options

Consulting Options

☒ _108__ Consulting Hours

Other Options (Please Describe)

Consulting hours may be applied (but not limited) to:

- Remediation services
- Reactive requests (i.e. Election and Scada Vulnerability Assessment Report)
- Customization of Procedures,
- Awareness Program guidance

9. Phase 1 Pricing: 1-Year vCISO Engagement

Service	Price
Year 1: November 2018-October 2019	
Penetration Testing	$16,000
Vulnerability Assessment	$35,000
Risk Assessment	$20,000
Data Classification	$20,000
Policy Development (Partial)	$12,000
Consulting	$27,000
vCISO Managed Services Program Management*	$40,000
Year 1 Total Pricing	**$170,000**

Travel and Expenses Consulting hours will be delivered onsite and offsite, based on minimization of travel expenses and maximization of presence, availability and execution of deliverables.	Billed to Client Per Client Travel and Expense Policy

*vCISO Program Management and Managed Services includes:

- Assigned vCISO
- Managed Program
- A Highly Certified and Experienced Client Team consisting of an assigned Client Lead and Security Program Manager, and other supporting members
- A Security Roadmap (SRM)
- Consulting and Advisory services
- A Client Relationship Manager
- Quarterly Service Reviews
- Periodic status reports
- Retained Incident Response Team

For the purposes of this proposal, the following is an initial Program Schedule.

Service	Year 1	Year 2	Year 3	Year 4
Gap Assessment	☐	☐	☐	☐
Internal Audit	☐	☐	☐	☐
Risk Assessment	☒	☐	☐	☐
HIPAA Risk Assessment	☐	☐	☐	☐
Vendor Risk Assessment	☐	☐	☐	☐
PCI Risk Assessment	☐	☐	☐	☐
Policy Development	☒	☐	☐	☐
Awareness Training	☐	☐	☐	☐
Incident Response Development	☐	☐	☐	☐
Incident Response	☐	☐	☐	☐
Penetration Testing*	☒	☐	☐	☐
Vulnerability Assessment*	☒	☐	☐	☐
Consulting	☒	☐	☐	☐
Data Classification	☒	☐	☐	☐
ISO 27001 Solution	☐	☐	☐	☐
GDPR Solution	☐	☐	☐	☐

*Priority Projects: The priorities of this engagement are MTM performing, separate Internal and External Vulnerability Assessments and Penetration Testing on each of Lake County, Illinois' Election System and Scada System.

10. Acceptance

10.1 Overview

The signatures below indicate agreement between MTM and Client to proceed with cybersecurity services as defined in this Statement of Work. MTM cannot proceed without an executed Statement of Work and compliance with payment terms.

10.2 MTM Signature

MTM, by way of its Authorized Representative, agrees to this Statement of Work.

Name: Pete Madsen
Title: VP Innovation Services
Date: _____

Signature: _____

10.3 Client Signature

Client, by way of its Authorized Representative, approves this Statement of Work.

Authorized Representative of "Client"

Name: _____

Title: _____

Date: _____

Signature: _____

11. Terms and Conditions

11.1 Assumptions

The service(s) described in this Statement of Work will be delivered by MTM under the following basic assumptions, which will govern the work and form the basis for changes that will apply throughout term of the engagement:

1. All work not specifically described in this Statement of Work will be subject to a Change Order, in these cases additional fees may apply;
2. All scheduled work will be performed during MTM normal business hours, which are Monday-Friday from 8:00am to 5:00pm, Eastern Time. Any work that must be performed outside of MTM normal business hours may be subject to a Change Order;
3. All unscheduled work, including Incident Response, may not be performed outside normal business hours without a Change Order;
4. Delivery delays caused by circumstances beyond the direct control of MTM are not covered under this Statement of Work and may be subject to a Change Order.

11.2 Limitations of Service

The scope of the MTM Services does not include time and expenses that are directly related to any damage or failure caused by: failure or functional limitations of any software or product impacting systems receiving MTM Services; improper use, site preparation, or site or environmental conditions or other non-compliance as determined by the software or product vendor; modifications or improper system maintenance or calibration not performed by MTM or authorized by MTM; abuse, neglect, accident, fire or water damage, electrical disturbances, transportation by anyone other than MTM; or other causes beyond MTM's control; or malware (e.g. virus, worm, etc.) not introduced by MTM.

11.3 MTM Responsibilities

As the provider of services herein, MTM will have the following basic responsibilities before, during, and after the engagement:

1. Completing this Statement of Work and providing all deliverables;
2. Providing a primary point of contact for all services;

3. Conducting appropriate communications to ensure the successful delivery of all services;
4. Timely billing for all services and applicable expenses.

11.4 Client Responsibilities

As the consumer of services herein, Client will have the following responsibilities before, during, and after the engagement:

1. Providing access to all assets necessary to complete the services described in this Statement of Work;
2. Providing a primary point of contact for all services;
3. Timely payment for all services and applicable expenses.

11.5 Cancellation Policy

MTM requires a minimum of twenty-four (24) hour notice for all activities cancelled by Client. Cancellations made with less than 24-hour notification may be subject to a cancellation fee, at the discretion of MTM. Cancellation penalties will be based on the opportunity cost for lost time.

11.6 Travel

Travel time will be billed to Client per the following schedule:

Travel Description	Hourly Rate
Un-retained Incident Response Travel	$400.00
All Other Travel	$190.00

1. All travel expenses related to the engagement, including hotel, transportation and meals will be billable to Client. Allowable travel expenses will be governed by Client Travel and Expense Policy, at Client's request;
2. For engagements with extensive travel requirements, MTM may require a travel retainer in advance, billable to Client.

11.7 Payment Terms

Unless other written arrangements have been made with MTM that supersede the terms of this section, the following payment terms will apply:

1. All invoices shall be Net 30, unless otherwise agreed to in advance and codified in writing;
2. Services will be billed 25% of the total every ninety (90) days starting the date of signature with the first invoice to be sent to Client immediately on signature;
3. Late fees and interest charges will be assessed for payments not received according to the payment schedule specified above.

11.8 Hourly Rates

Rate Description	Hourly Rate
All Services, Normal Business Hours (M-F, 8am-5pm)	$300.00
Un-retained Incident Response, Normal Business Hours (M-F, 8am - 5pm)	$350.00
Un-retained Incident Response, Off-Hours	$475.00

11.9 Privacy

By executing the Statement of Work, Client agrees to receive marketing materials from MTM. Client may unsubscribe to these communications at any time. Information regarding Client preferences is considered *classified* data and is protected as such. MTM will, under no circumstances sell or share Client information.