STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget
525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **2**

to

Contract Number **210000000301**

CONTRACTOR	
	Dewpoint, Inc.
	300 S. Washington Sq. Suite 200
	Lansing, MI 48933
	Kelly Schafka
	517-230-1519
	kschafka@dewpoint.com
	CV0040100

STATE			
	Program Manager	Various	MULTI
	Contract Administrator	Courtney Powell	DTMB
		(517) 249-0452	
		powellc11@michigan.gov	

CONTRACT SUMMARY			
INDEPENDENT CYBER ASSESSMENT SERVICES FOR LOCAL ENTITIES			
INITIAL EFFECTIVE DATE	**INITIAL EXPIRATION DATE**	**INITIAL AVAILABLE OPTIONS**	**EXPIRATION DATE BEFORE**
January 25, 2021	January 24, 2026	5 - 1 Year	January 10, 2026
PAYMENT TERMS		**DELIVERY TIMEFRAME**	
Net 45		N/A	
ALTERNATE PAYMENT OPTIONS			**EXTENDED PURCHASING**
☐ P-Card	☐ PRC	☐ Other	☒ Yes ☐ No
MINIMUM DELIVERY REQUIREMENTS			
N/A			

DESCRIPTION OF CHANGE NOTICE				
OPTION	**LENGTH OF OPTION**	**EXTENSION**	**LENGTH OF EXTENSION**	**REVISED EXP. DATE**
☐		☐		January 10, 2026
CURRENT VALUE	**VALUE OF CHANGE NOTICE**		**ESTIMATED AGGREGATE CONTRACT VALUE**	
$1.00	$0.00		$1.00	

DESCRIPTION

Effective December 7, 2021 the following Schedule A - SOW and associated attachments are added to this Contract for use by DHHS. The State PM on this project is Mark Shook.

The Contractor's Contract Administrator has changed to Kelly Schafka (kschafka@dewpoint.com, 517-230-1519).

All other terms, conditions, specifications and pricing remain the same. Per contractor and agency agreement, and DTMB Central Procurement approval.

Program Managers
for
Multi-Agency and Statewide Contracts

AGENCY	NAME	PHONE	EMAIL
DTMB	Jayson Cavendish	517-241-1624	CavendishJ@Michigan.gov
DTMB	Mark Shook	313-600-1515	shookm1@michigan.gov

SCHEDULE A – STATEMENT OF WORK CONTRACT ACTIVITIES

CN 2 - 210000002458

Cybersecurity Assessment and Advisory Services for "County Managed" Friend of Court and Prosecuting Attorney Offices in Michigan

BACKGROUND

Background on Certification Requirement and 2019 assessment cycle

- Michigan Office of Child Support (OCS) is required by the federal Office of Child Support Enforcement (OCSE) to certify the safeguard and security of Title IV-D child support confidential data including Federal Parent Locator Service data as attested to in the Annual Security Agreement between OCSE and OCS. Every three years, an independent security assessment is to be conducted involving child support program information and the computer systems storing and processing that information.
- To complete this requirement in 2019, OCS required county managed Friend of the Court (FOC) and Prosecuting Attorney (PA) offices to conduct an independent third-party assessment of compliance with the OCSE Security Agreement. Counties were reimbursed 66 percent of the incurred costs to meet this requirement.
- OCS received the third-party audit results and corrective action plans or Plan of Action and Milestones (POAM), when necessary, from the county-managed agencies.

SCOPE

OCS, in partnership with DTMB Agency Services (AS) and Michigan Cyber Security (MCS), will engage a pre-qualified Contractor from the Michigan Cyber Partners MiDEAL Independent Cyber Assessment and Advisory Services contract to assess each county managed office's technical security controls that are required to maintain OCS' OCSE Annual Security Certification over a 3-year period.

1. Requirements

OCS, in partnership with DTMB and Michigan Cyber Security will coordinate Contractor acquisition through the Michigan Cyber Partners MiDEAL independent cyber assessment and advisory service contract to assess the information technology (IT) environment and controls at each of the county managed offices that impacts the safeguard of Title IV-D child support data. More about Michigan Cyber Partners at www.michgan.gov/cyberpartners.

OCS is seeking one (1) Contractor (or a prime with sub- contractors) to provide services outlined and required for this project who will provide:

- Consistent county level reports on the findings of their county managed IT systems and environment.
- Comprehensive statewide summary report.

- Remediation advisory services through the remainder of the contract period.

All county assessments and initial reporting **MUST** be completed by September 30, 2022. Statewide summary report must be completed by November 30, 2022.

Monitoring and remediation advisory services are to be provided through the remainder of the contract period.

The Center for Internet Security (CIS) Controls are to be used for the county assessment and reporting. OCS has identified specific CIS controls and subcontrols that map to the OCSE security certification requirements.

Work closely with county FOC, PA, and IT staff to ensure a smooth process that focuses on assessing, reporting on, and improving the information security processes of individual offices and the statewide system by identifying risks and monitoring remediation with follow up reporting on remediation activities to OCS.

1.1. Individual County Assessments

Conduct individual assessments for each county managed FOC and PA office – see Attachment A - Michigan County Offices for list of counties and locations. Assessment will follow MiDEAL contract specifications including Core Service Offering Deliverables and Optional Services as detailed below.

A. Core Service Offering Deliverables

1. On-site or virtual cybersecurity assessment jointly completed by an independent assessor and local entity staff using the CIS Controls Self-Assessment Tool (CSAT).
2. Current-state report (based on CSAT) the overall assessment results including most important vulnerabilities and recommended next steps for remediation.
3. Annual Cybersecurity Improvement Plan (POAM) that identifies priority actions to complete in the coming 12 months and other lesser priority activities that have a longer time horizon.
4. Ensure that county has an effective basic cyber incident response plan. A sample incident response plan is on the Cyber Partners website: www.michigan.gov/cyberpartners.
5. Monthly one-hour telephone/online or in-person consultation to provide ongoing coaching and consulting regarding understanding of and implementation of cybersecurity improvements for each county assessed.
6. End of contract assessment update using CSAT which identifies progress made towards improving priority items identified in initial assessment and items remaining to be addressed.

B. MiDEAL Optional Deliverables - ***REQUIRED*** for this engagement as part of each county/office assessment

MiDEAL Optional Deliverable #2: Assessment and planning for CIS Controls/Sub Controls in Implementation Groups (IG) 2 and 3.

1. Requirement: Assess each county office using IG 1 controls as identified in Core Services Offerings #1 and additional controls in IG 2 and 3

identified in Attachment B - Controls Required for OCS County Level Assessments.

MiDEAL Optional Deliverable #4 Conduct Penetration Test

2. Requirement: Penetration testing including internal vulnerability scanning - based on Internal Revenue Service (IRS) SCSEM and County IT Infrastructure Architecture. Include these findings and remediation steps in overall assessment results and Annual Cybersecurity Improvement Plan and coaching activities. The IRS Safeguards links can be found at the following IRS sites:

    a. https://www.irs.gov/privacy-disclosure/computer-security-compliance-references-and-related-topics

    b. https://www.irs.gov/privacy-disclosure/nessus-audit-files

MiDEAL Optional Deliverable #3: Assistance with audits or compliance requirements that are present at the local entity based on business practices. (CJIS, PCI, HIPAA, IRS-1075, FERPA, etc…)

3. Requirement: County assessment results, improvement plans, and planning documents and activities must include all CIS subcontrols identified in Attachment B and results of Penetration Testing and Plan of Action and Milestones (POAM).

1.2. Statewide Reporting of Assessment Results

The reporting requirements described below are listed as Deliverables 1, 2, and 3 under **B. Optional Service Offerings** in the MiDEAL contracts are required under this SOW:

- *#1 – General Advisory Services on a time and materials basis.*
- *#2 – Assessment and planning for CIS Controls/SubControls in Implementation Groups 2 and 3.*
- *#3 – Assistance with audits or compliance requirements that are present at the local entity based on business practices. (CJIS, PCI, HIPAA, IRS-1075, FERPA, etc…)*

A. Requirement: Statewide summary of county-by-county results for both CIS Controls and Penetration Testing identifying counties in high, medium, and low risk categories and number of outstanding findings. POAMs are to be updated twice per year in years 2 and 3 (see section 1.3 Schedule of Deliverables, below).

B. Requirement: Statewide summary of results that will create a common understanding of the state of child support data related to cybersecurity at county managed offices and anonymized results that can be used to inform policy at county, State of Michigan, and OCS levels.

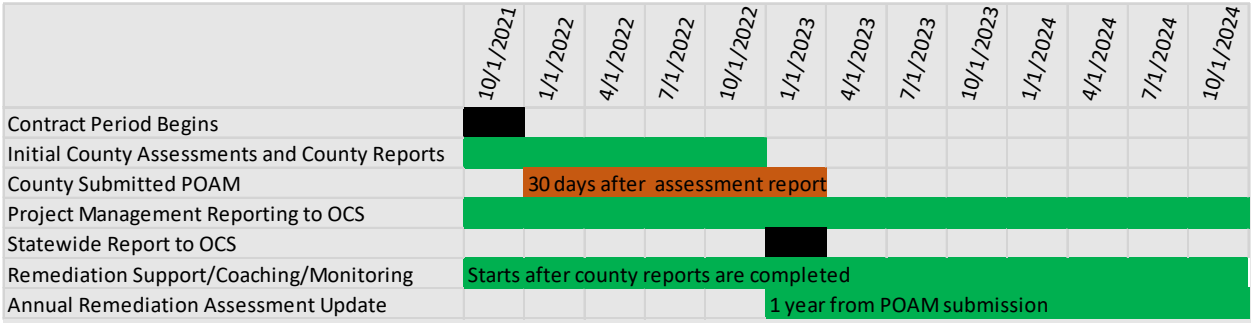
C. Requirement: Project Management, planning, and project reporting including scheduling of assessments and regular updates.

The Contractor will manage this program under the guidance of OCS and DTMB using an industry standard Program/Project Management methodology.

1. The Contractor will conduct a Program Kickoff with the OCS and DTMB concerning the overall program and state-wide project plan. Additionally, the vendor will conduct kick-off meetings with each county that will be assessed to outline the individual assessment.
2. The Contractor will present the state-wide Project Management Plan (PMP) to the OCS and DTMB within 10 business days of the program start date. The Contractor will use the State Unified Information Technology Environment (SUITE) PMM 102 Template (see Attachment D - Project Management Plan PMM-0102) to document the PMP.
3. Contractor will adhere to the standard Communication and Change Management processes outlined in the PMP.
4. Quarterly progress reports must be submitted to the OCS and DTMB Project Managers throughout the life of this contract. This report may be submitted with the billing invoice. Each Quarterly progress report must contain the following:

    a. Overall Program status using the Green/Yellow/Red format including percentage complete, any risks, and issues.
    b. Accomplishments: Indicate what was worked on and what was completed during the current reporting period.
    c. Next steps and/or activities that are expected to be completed in the next reporting period

1.3. Schedule of Deliverables:



This contract is for assessment, remediation oversight, and coaching only. Selected Contractor is expected to assist with remediation support but is precluded from selling additional products or services related to this contract to counties during the life of this agreement. Contract deliverables must be completed within three (3) years or not later than October 1, 2024.

2. Service Requirements

2.1. Timeframes

All Contract Activities must be delivered within the timeframe set forth in section 1.3 above and must be completed by October 1, 2024. The receipt of order date is pursuant to the **Notices** section of the *Standard Contract Terms*.

3. Acceptance

Acceptance will be in accordance with section 16. Acceptance in the Standard Contract Terms.

4. Staffing

4.1. Contractor Representative

The Contractor must appoint an Account Executive/Engagement Manager, Cybersecurity Expert and Technical Testing Lead individuals specifically assigned to State of Michigan accounts, who will respond to State inquiries regarding the Contract Activities, answer questions related to ordering and delivery, etc. (the "Contractor Representative"). Refer to Attachment C for qualifications and forms.

4.2. Work Hours

The Contractor must provide Contract Activities during the State's normal working hours outlined on the main contract.

4.3. Key Personnel

The Contractor must appoint a Project Manager, an Account Executive/Engagement Manager and Cybersecurity Expert individuals who will be directly responsible for the day-to-day operations of the Contract ("Key Personnel"). Key Personnel must be specifically assigned to the State account, be knowledgeable on the contractual requirements, and respond to State inquiries within 24 hours.

The State has the right to recommend and approve in writing the initial assignment, as well as any proposed reassignment or replacement, of any Key Personnel. Before assigning an individual to any Key Personnel position, Contractor will notify the State of the proposed assignment, introduce the individual to the State's Project Manager, and provide the State with a resume and any other information about the individual reasonably requested by the State. The State reserves the right to interview the individual before granting written approval. In the event the State finds a proposed individual unacceptable, the State will provide a written explanation including reasonable detail outlining the reasons for the rejection. The State may require a 30-calendar day training period for replacement personnel.

Contractor will not remove any Key Personnel from their assigned roles on this Contract without the prior written consent of the State. The Contractor's removal of Key Personnel without the prior written consent of the State is an unauthorized removal ("Unauthorized Removal"). An Unauthorized Removal does not include replacing Key Personnel for reasons beyond the reasonable control of Contractor, including illness, disability, leave of absence, personal emergency circumstances, resignation, or for cause termination of the Key Personnel's employment. Any Unauthorized Removal may be considered by the State to be a material breach of this Contract, in respect of which the State may elect to terminate this Contract for cause under the **Termination for Cause** section of the Standard Contract Terms. It is further acknowledged that an Unauthorized Removal will interfere with the timely and proper completion of this Contract, to the loss and damage of the State, and that it would be impracticable and extremely difficult to fix the actual damage sustained by the State as a result of any Unauthorized Removal. Therefore, Contractor and the State agree that in the case of any Unauthorized Removal in respect of which the State does not elect to exercise its rights under Termination for Cause, Contractor will issue to the State the corresponding credits set forth below (each, an "Unauthorized Removal Credit"):

i. For the Unauthorized Removal of any Key Personnel designated in the applicable Statement of Work, the credit amount will be $25,000.00 per individual if Contractor identifies a replacement approved by the State and assigns the replacement to shadow the Key Personnel who is leaving for a period of at least 30-calendar days before the Key Personnel's removal.

ii. If Contractor fails to assign a replacement to shadow the removed Key Personnel for at least 30-calendar days, in addition to the $25,000.00 credit specified above, Contractor will credit the State $833.33per calendar day for each day of the 30-calendar day shadow period that the replacement Key Personnel does not shadow the removed Key Personnel, up to $25,000.00maximum per individual. The total Unauthorized Removal Credits that may be assessed per Unauthorized Removal and failure to provide 30-calendar days of shadowing will not exceed $50,000.00per individual.

Contractor acknowledges and agrees that each of the Unauthorized Removal Credits assessed above: (i) is a reasonable estimate of and compensation for the anticipated or actual harm to the State that may arise from the Unauthorized Removal, which would be impossible or very difficult to accurately estimate; and (ii) may, at the State's option, be credited or set off against any fees or other charges payable to Contractor under this Contract.

The Contractor must identify the Key Personnel, indicate where they will be physically located, describe the functions they will perform, and provide current chronological résumés.

4.4. Organizational Chart

The Contractor must provide an overall organizational chart that details staff members, by name and title, and subcontractors.

4.5. Disclosure of Subcontractors

If the Contractor intends to utilize subcontractors, the Contractor must disclose the following:

- The legal business name; address; telephone number; a description of subcontractor's organization and the services it will provide; and information concerning subcontractor's ability to provide the Contract Activities.
- The relationship of the subcontractor to the Contractor.
- Whether the Contractor has a previous working experience with the subcontractor. If yes, provide the details of that previous relationship.
- A complete description of the Contract Activities that will be performed or provided by the subcontractor.

5. Project Management

5.1. Project Plan

Per the original pre-qualification contracts, within 10 business day of the award of this SOW, the Contractor must submit, for final approval, a detailed project plan to the Contracting Entity.

The final Project Plan must be in agreement with the Contractor's SOW proposal and accepted by the State. Detailed requirements will include steps required to plan and conduct onsite assessment, deliver draft and final assessment reports and plan and schedule monthly check in meetings; and individuals responsible for receiving/reacting to the requested information, including names and titles of personnel assigned to the project, both from the Contractor and State.

The Contractor will carry out this project under the direction and control of the State Program Manager. Within 45 calendar days of the Effective Date, the Contractor must submit a mutually agreed upon project plan to the Program Manager for approval. The

plan must include: (a) the Contractor's organizational chart with names and title of personnel assigned to the project, which must align with the staffing stated in accepted proposals; and (b) the project breakdown showing sub-projects, tasks, timeline, and resources required.

5.2. Meetings

The Contractor must attend the Kick-off meeting within five (5) business days of the Effective Date.

Ongoing update meetings will be mutually agreed upon.

The State may request other meetings, as it deems appropriate.

5.3. Reporting

The Contractor must submit, to the Program Manager or designee, periodic (weekly or bi-weekly) and ongoing status and progress reports.

6. Invoice and Payment

6.1. Invoice Requirements

All invoices submitted to the State must include: (a) date; (b) purchase order; (c) quantity; (d) description of the Contract Activities; (e) unit price; (f) shipping cost (if any); (g) vendor-generated invoice number; and (h) total price. Overtime, holiday pay, and travel expenses will not be paid.

6.2. Payment Methods

The State will make payment for Contract Activities via EFT.

7. Liquidated Damages

Late or improper completion of the Contract Activities will cause loss and damage to the State and it would be impracticable and extremely difficult to fix the actual damage sustained by the State. Therefore, if there is late or improper completion of the Contract Activities the State is entitled to collect liquidated damages in the amount of $10,000 and an additional $1,000 per day for each day Contractor fails to remedy the late or improper completion of the Work.

Schedule B - Pricing for 3 Years

MIDEAL Core Services	**Small Entity** *>50 End Points*	**Medium Entity** *50-500 End Points*	**Large Entity** *500-1500 End Points*	**X-Large Entity** *1500+ End Points*	
Fixed Price for MIDEAL Core Services:					
1. Cybersecurity Assessment Workshop using CIS Controls and CSAT Tool					
2. Assessment Report & Recommendations	$ 7,681.00	$ 13,216.00	$ 15,600.00	$ 20,762.00	
3. Cybersecurity Improvements Plan					
4. Baseline Incident Response Plan					
5. Monthly Advisory Sessions (1 hour)					
6. End of Engagement Assessment					
Number of Entities	11	23	16	8	
Total	$ 84,491	$ 303,968	$ 249,600	$ 166,096	**$ 804,155**

Required Optional Service Offerings from Schedule B in MIDEAL Contract	**Small Entity** *>50 End Points*	**Medium Entity** *50-500 End Points*	**Large Entity** *500-1500 End Points*	**X-Large Entity** *1500+ End Points*	
County Level:	Fixed Price	Fixed Price	Fixed Price	Fixed Price	
Additional 8 CIS Controls in IG 2 and 3 from Attachment B	$ 1,092.00	$ 1,877.00	$ 2,216.00	$ 2,936.00	
Penetration Test	$ 4,268.00	$ 5,978.00	$ 9,750.00	$ 13,164.00	
Subtotal	$ 5,360.00	$ 7,855.00	$ 11,966.00	$ 16,100.00	
Number of Entities	11	23	16	8	
Total	$ 58,960	$ 180,665	$ 191,456	$ 128,800	**$ 559,881**

Statewide Reporting:		
County by County Summary	$ 58,000	
Statewide Summary of Results	$ 24,860	
Project Management	$ 366,050	
Total	$ 448,910	**$ 448,910**

Grand Total	**$ 1,812,946**

Additional Cost Considerations

Anything else to offer to the State or miscelaneous cost values here.

Monthly coaching beyond initial 12 months

ATTACHMENT A - MICHIGAN COUNTY OFFICES

List of County Offices to be reviewed			County Office		
County	**County Population**	**Child Support System Users (Approx.)**	**Prosecuting Attorney**	**Friend of the Court**	**Combined Circuit with**
Alcona County	10,364	26	x		
Allegan County	115,250	31	x	x	
Alpena County	28,612	17		x	Montmorency FOC
Antrim County	23,177	38	x	x	
Barry County	60,057	35	x	x	
Bay County	104,786	41	x	x	
Benzie County	17,552	22	x	x	
Berrien County	154,807	75	x	x	
Branch County	43,584	18	x	x	
Calhoun County	134,473	83	x	x	
Cass County	51,460	23	x	x	
Cheboygan County	25,458	31	x	x	
Clare County	30,616	8	x	x	
Clinton County	77,896	38	x	x	
Eaton County	109,155	37	x	x	
Emmet County	33,039	27	x	x	
Genesee County	409,361	125	x	x	
Gladwin County	25,289	27	x	x	
Grand Traverse County	91,746	39		x	Antrim FOC & Leelanau FOC
Gratiot County	41,067	24	x	x	
Ingham County	289,564	106	x	x	
Ionia County	64,176	33	x		
Iosco County	25,247	41	x	x	
Isabella County	70,775	25	x	x	
Jackson County	158,913	72	x	x	
Kalamazoo County	261,573	88	x	x	
Kalkaska County	17,463	24	x	x	
Kent County	643,140	152	x	x	
Lapeer County	88,202	31	x	x	
Leelanau County	21,639	35	x	x	
Lenawee County	98,474	32		x	
Livingston County	188,482	45	x	x	
Macomb County	868,704	147	x	x	
Manistee County	24,444	25	x	x	Benzie FOC
Marquette County	66,939	33	x	x	
Mason County	28,884	13	x	x	
Menominee County	23,234	20	x	x	
Midland County	83,389	49	x	x	
Monroe County	149,699	52	x	x	
Montcalm County	63,209	33	x	x	
Muskegon County	173,043	109	x	x	

Newaygo County	48,142	28	x	x
Oakland County	1,250,843	236	x	x
Oceana County	26,417	18	x	
Oscoda County	8,277	30	x	x
Otsego County	24,397	37	x	x
Ottawa County	284,034	77	x	x
Presque Isle County	12,797	21	x	
Roscommon County	23,877	18	x	x
Saginaw County	192,778	55	x	x
Sanilac County	41,376	21		x
Shiawassee County	68,493	30	x	x
St. Clair County	159,566	71	x	x
St. Joseph County	60,897	37	x	x
Tuscola County	53,250	21	x	x
Van Buren County	75,272	36	x	x
Washtenaw County	365,961	90	x	x
Wayne County	1,761,382	435	x	x
		3191	**54**	**54**

Note: Counties with a combined circuit may have more than one county IT network to review and assess.

Attachment B - Controls Required for OCS County Level Assessment

Summary:
Controls Required for OCS County Level Assessments
56 Safeguards/Subcontrols from Controls V8 plus 8 controls added from OCSE requirements

CIS Controls v8	CIS Safeguards	Asset Type	Title	Description	IG 1	IG 2	IG 3	OCSE	IG1 and/or OCS
1	1.1	Devices	Establish and Maintain Detailed Enterprise Asset Inventory	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices,MDM type tools can support this process, where appropriate. This inventory includes assetsconnected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	1	1	1	1	1
2	1.2	Devices	Address Unauthorized Assets	Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	1	1	1		1
6	2.1	Applications	Establish and Maintain a Software Inventory	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	1	1	1		1
7	2.2	Applications	Ensure Authorized Software is Currently Supported	Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	1	1	1		1

8	2.3	Applications	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	1	1	1		1
13	3.1	Data	Establish and Maintain a Data Management Process	Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	1	1	1	1	1
14	3.2	Data	Establish and Maintain a Data Inventory	Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.	1	1	1		1
15	3.3	Data	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	1	1	1	1	1
16	3.4	Data	Enforce Data Retention	Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.	1	1	1		1
17	3.5	Data	Securely Dispose of Data	Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.	1	1	1	1	1
18	3.6	Devices	Encrypt Data on End-User Devices	Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker, Apple FileVault, Linux dm-crypt.	1	1	1	1	1
22	3.1	Data	**Encrypt Sensitive Data in Transit**	Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		1	1	1	1
23	3.11	Data	**Encrypt Sensitive Data at Rest**	Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		1	1	1	1
26	3.14	Data	**Log Sensitive Data Access**	Log sensitive data access, including modification and disposal.			1	1	1

27	4.1	Applications	Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile; non-computing/IoT devices; and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	1	1	1	1	1
28	4.2	Network	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	1	1	1		1
29	4.3	Users	Configure Automatic Session Locking on Enterprise Assets	Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	1	1	1	1	1
30	4.4	Devices	Implement and Manage a Firewall on Servers	Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	1	1	1		1
31	4.5	Devices	Implement and Manage a Firewall on End-User Devices	Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	1	1	1		1
32	4.6	Network	Securely Manage Enterprise Assets and Software	Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	1	1	1		1
33	4.7	Users	Manage Default Accounts on Enterprise Assets and Software	Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	1	1	1		1
39	5.1	Users	Establish and Maintain an Inventory of Accounts	Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	1	1	1	1	1

40	5.2	Users	Use Unique Passwords	Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	1	1	1		1
41	5.3	Users	Disable Dormant Accounts	Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	1	1	1		1
42	5.4	Users	Restrict Administrator Privileges to Dedicated Administrator Accounts	Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	1	1	1		1
45	6.1	Users	Establish an Access Granting Process	Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	1	1	1	1	1
46	6.2	Users	Establish an Access Revoking Process	Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	1	1	1	1	1
47	6.3	Users	Require MFA for Externally-Exposed Applications	Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.	1	1	1		1
48	6.4	Users	Require MFA for Remote Network Access	Require MFA for remote network access.	1	1	1	1	1
49	6.5	Users	Require MFA for Administrative Access	Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	1	1	1		1
53	7.1	Applications	Establish and Maintain a Vulnerability Management Process	Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	1	1	1		1
54	7.2	Applications	Establish and Maintain a Remediation Process	Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.	1	1	1		1
55	7.3	Applications	Perform Automated Operating System Patch Management	Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	1	1	1		1
56	7.4	Applications	Perform Automated Application Patch Management	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	1	1	1		1

60	8.1	Network	Establish and Maintain an Audit Log Management Process	Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	1	1	1		1
61	8.2	Network	Collect Audit Logs	Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	1	1	1		1
62	8.3	Network	Ensure Adequate Audit Log Storage	Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	1	1	1		1
72	9.1	Applications	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	1	1	1		1
73	9.2	Network	Use DNS Filtering Services	Use DNS filtering services on all enterprise assets to block access to known malicious domains.	1	1	1		1
79	10.1	Devices	Deploy and Maintain Anti-Malware Software	Deploy and maintain anti-malware software on all enterprise assets.	1	1	1		1
80	10.2	Devices	Configure Automatic Anti-Malware Signature Updates	Configure automatic updates for anti-malware signature files on all enterprise assets.	1	1	1		1
81	10.3	Devices	Disable Autorun and Autoplay for Removable Media	Disable autorun and autoplay auto-execute functionality for removable media.	1	1	1		1
86	11.1	Data	Establish and Maintain a Data Recovery Process	Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	1	1	1		1
87	11.2	Data	Perform Automated Backups	Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.	1	1	1		1
88	11.3	Data	Protect Recovery Data	Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	1	1	1		1
89	11.4	Data	Establish and Maintain an Isolated Instance of Recovery Data	Establish and maintain an isolated instance of recovery data. Example implementations include version controlling backup destinations through offline, cloud, or off-site systems or services.	1	1	1		1
91	12.1	Network	Ensure Network Infrastructure is Up-to-Date	Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.	1	1	1		1

97	12.7	Devices	**Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure**	Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.		1	1	1	1
103	13.5	Devices	**Manage Access Control for Remote Assets**	Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed; configuration compliance with the enterprise's secure configuration process; and ensuring the operating system and applications are up-to-date.		1	1	1	1
107	13.9	Devices	**Deploy Port-Level Access Control**	Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.			1	1	1
110	14.1	N/A	Establish and Maintain a Security Awareness Program	Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.	1	1	1	1	1
111	14.2	N/A	Train Workforce Members to Recognize Social Engineering Attacks	Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.	1	1	1	1	1
112	14.3	N/A	Train Workforce Members on Authentication Best Practices	Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.	1	1	1	1	1
113	14.4	N/A	Train Workforce on Data Handling Best Practices	Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.	1	1	1	1	1
114	14.5	N/A	Train Workforce Members on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.	1	1	1	1	1
115	14.6	N/A	Train Workforce Members on Recognizing and Reporting Security Incidents,Train workforce members to be able to recognize a potential incident and be able to report such an incident.	x	1	1		1	1

116	14.7	N/A	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.	1	1	1	1	1
117	14.8	N/A	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.	1	1	1	1	1
118	14.9	N/A	**Conduct Role-Specific Security Awareness and Skills Training**	Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, (OWASP's Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles.		1	1	1	1
119	15.1	N/A	Establish and Maintain an Inventory of Service Providers	Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.	1	1	1		1
140	17.1	N/A	Designate Personnel to Manage Incident Handling	Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	1	1	1	1	1
141	17.2	N/A	Establish and Maintain Contact Information for Reporting Security Incidents	Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.	1	1	1	1	1

142	17.3	N/A	Establish and Maintain an Enterprise Process for Reporting Incidents	Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	1	1	1	1	1
143	17.4	N/A	**Establish and Maintain an Incident Response Process**	Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		1	1	1	1

OCSE Mapped to CIS Controls 8

CIS Controls Version 8 Sub Controls for this audit.

Will be an Excel export from CIS Controls Navigator with identified subcontrols.
https://www.cisecurity.org/controls/cis-controls-navigator/

Attachment C – Bidder Staffing Qualifications and Resumes

Detailed resumes and completed forms for the following positions who will be considered Key Personnel:

1. **Account Executive / Engagement Manger**
2. **Cybersecurity Expert**
3. **Technical Testing Lead**

Proposed Classification:	**1. Account Executive / Engagement Manager**
Proposed Resource Name:	
Key Personnel (YES/NO):	**YES**
If resource is associated with a subcontractor provide name of company:	

Describe the skills and experience of the proposed classification by completing the following table:

	Required Skills	Does resource have this required skill	Description of skills and experience Name of project(s) and year(s) experience was obtained
1.	10 years of experience managing and implementation projects of similar size and scope of this project		
2.	3 years of experience managing cybersecurity engagements.		
3.	Education: Bachelor of Science in Information Technology, Computer Science, Engineering, Business or related degree.		
4.	5 years of experience as an Account Executive or Engagement Manager (or similar role)		
5.	3 years of experience as an Account Executive or Engagement Manager in the Cybersecurity or Risk Management field		

6.	(Optional Requirement) 3 years of experience managing engagements for Federal, State, Local Government, or education entities		
7.	List all other relevant Certifications:		

Proposed Classification:	**2. Cybersecurity Expert**
Proposed Resource Name:	
Key Personnel (YES/NO):	**YES**
If resource is associated with a subcontractor provide name of company:	

Describe the skills and experience of the proposed classification by completing the following table:

	Required Skills	Does resource have this required skill	Description of skills and experience Name of project(s) and year(s) experience was obtained
1.	10 years of experience in information technology		
2.	5 years of experience implementing cybersecurity best practices at an organizational level.		
3.	5 years of experience conducting assessments with nationally recognized cybersecurity frameworks. (e.g. NIST, CIS Controls, ISO, PCI, CJIS, etc.)		
4.	Education: Bachelor of Science in Information Technology, Computer Science, Engineering, Business or related degree.		
5.	3 years of experience performing Cyber Security Risk Assessments		
6.	5 years of experience as a server or network administrator		

7.	3 years of experience as a security analyst or security operations engineer		
8.	Certification: current CISSP or similar cybersecurity certification		
9.	(Optional Requirement) 3 years of experience with specific focus on vulnerability and asset management		
10.	List all other relevant Certifications:		

Proposed Classification:	**3. Technical Testing Lead**
Proposed Resource Name:	
Key Personnel (YES/NO):	**YES**
If resource is associated with a subcontractor provide name of company:	

Describe the skills and experience of the proposed classification by completing the following table:

	Required Skills	Does resource have this required skill	Description of skills and experience Name of project(s) and year(s) experience was obtained
1.	5 years of experience in information technology with broad knowledge of Application Lifecycle Management		
2.	3 years of experience developing scripts and/or programming languages such as java/type script, java, c#, etc.		
3.	3 years of experience as a server operating system or network administrator		
4.	3 years of experience conducting Penetration Testing for a medium to large organization with nationally recognized cybersecurity frameworks. (e.g., NIST, CIS Controls, IRS, PCI, CJIS, etc.)		
5.	3 years of experience performing Cyber Security Risk Assessments		
6.	3 years of experience with specific focus on		

	vulnerability remediation at the server OS and network tiers		
7.	Education: Bachelor of Science in Information Technology, Computer Science, Engineering, Business or related degree.		
8.	List Relevant Certifications		

Attachment D - Project Management Plan PMM-0102 (Word document)

State approved Project Management Plan (PMP) (the State Unified Information Technology Environment (SUITE)).

STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
Department of Technology, Management, and Budget
525 W. ALLEGAN ST., LANSING, MICHIGAN 48913
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number **1**

to

Contract Number **210000000301**

CONTRACTOR	
	Dewpoint, Inc.
	300 S. Washington Sq. Suite 200
	Lansing, MI 48933
	Michelle Massey
	517-258-2750
	mmassey@dewpoint.com
	CV0040100

STATE			
	Program Manager	Jayson Cavendish	DTMB
		517-243-8692	
		CavendishJ@Michigan.gov	
	Contract Administrator	Courtney Powell	DTMB
		(517) 249-0452	
		powellc11@michigan.gov	

CONTRACT SUMMARY

INDEPENDENT CYBER ASSESSMENT SERVICES FOR LOCAL ENTITIES

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
January 25, 2021	January 24, 2026	5 - 1 Year	January 10, 2026

PAYMENT TERMS	DELIVERY TIMEFRAME

ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING	
☐ P-Card	☐ PRC	☐ Other	☒ Yes	☐ No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
☐		☐		January 10, 2026

CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE
$1.00	$0.00	$1.00

DESCRIPTION

Please note the Program Manager has been changed to Jayson Cavendish.

All other terms, conditions, specifications and pricing remain the same. Per Contractor and Agency agreement, and DTMB Procurement approval.

STATE OF MICHIGAN PROCUREMENT

Department of Technology Management and Budget
525 W. Allegan 1st Floor, Lansing, MI 48913
P.O. BOX 30026 Lansing, MI 48909

NOTICE OF CONTRACT

NOTICE OF CONTRACT NO. **210000000301**
between
THE STATE OF MICHIGAN
and

CONTRACTOR	
	Dewpoint Inc.
	300 S. Washington Sq. Suite 200
	Lansing, MI 48933
	Michelle Massey
	517.258.2750
	mmassey@dewpoint.com
	CV0040100

STATE			
	Program Manager	Derek Larson	DTMB
		517-241-6606	
		LarsonD4@michigan.gov	
	Contract Administrator	Steven Motz	DTMB
		517-331-6086	
		Motzs1@michigan.gov	

CONTRACT SUMMARY			
DESCRIPTION: Independent Cyber Assessment Services for Local Entities			
INITIAL EFFECTIVE DATE	**INITIAL EXPIRATION DATE**	**INITIAL AVAILABLE OPTIONS**	**EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW**
1/25/2021	1/24/2026	5 - 1 Year	N/A
PAYMENT TERMS		**DELIVERY TIMEFRAME**	
Net 45		N/A	
ALTERNATE PAYMENT OPTIONS			**EXTENDED PURCHASING**
☐ P-card ☐ Payment Request (PRC) ☐ Other			☒ Yes ☐ No
MINIMUM DELIVERY REQUIREMENTS			
N/A			
MISCELLANEOUS INFORMATION			
THIS IS NOT AN ORDER. This Contract Agreement is awarded on the basis of our inquiring RFP No. 200000001673. Orders for delivery will be issued directly by Departments through the issuance of a Delivery Order Form.			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION			**$1.00**

STATE OF MICHIGAN

STANDARD CONTRACT TERMS

This STANDARD CONTRACT ("**Contract**") is agreed to between the State of Michigan (the "**State**") and **Dewpoint Inc** ("**Contractor**"), a Michigan corporation. This Contract is effective on **January 25, 2021** ("**Effective Date**"), and unless terminated, expires on **January 24, 2026**.

This Contract may be renewed for up to **five (5)** additional **one (1) year** period(s). Renewal is at the sole discretion of the State and will automatically extend the Term of this Contract. The State will document its exercise of renewal options via Contract Change Notice.

The parties agree as follows:

1. **Duties of Contractor.** Contractor must perform the services and provide the deliverables described in **Schedule A – Statement of Work** (the "**Contract Activities**"). An obligation to provide delivery of any commodity is considered a service and is a Contract Activity.

   Contractor must furnish all labor, equipment, materials, and supplies necessary for the performance of the Contract Activities, and meet operational standards, unless otherwise specified in Schedule A.

   Contractor must: (a) perform the Contract Activities in a timely, professional, safe, and workmanlike manner consistent with standards in the trade, profession, or industry; (b) meet or exceed the performance and operational standards, and specifications of the Contract; (c) provide all Contract Activities in good quality, with no material defects; (d) not interfere with the State's operations; (e) obtain and maintain all necessary licenses, permits or other authorizations necessary for the performance of the Contract; (f) cooperate with the State, including the State's quality assurance personnel, and any third party to achieve the objectives of the Contract; (g) return to the State any State-furnished equipment or other resources in the same condition as when provided when no longer required for the Contract; (h) not make any media releases without prior written authorization from the State; (i) assign to the State any claims resulting from state or federal antitrust violations to the extent that those violations concern materials or services supplied by third parties toward fulfillment of the Contract; (j) comply with all State physical and IT security policies and standards which will be made available upon request; and (k) provide the State priority in performance of the Contract except as mandated by federal disaster response requirements. Any breach under this paragraph is considered a material breach.

   Contractor must also be clearly identifiable while on State property by wearing identification issued by the State, and clearly identify themselves whenever making contact with the State.

2. **Notices.** All notices and other communications required or permitted under this Contract must be in writing and will be considered given and received: (a) when verified by written receipt if sent by courier; (b) when actually received if sent by mail without verification of receipt; or (c) when verified by automated receipt or electronic logs if sent by facsimile or email.

If to State:	If to Contractor:
Steve Motz 525 W. Allegan St., 1ST FLR. NE Lansing, MI 48909 Motzs1@michigan.gov 517-331-6086	Michelle Massey 300 S Washington, Suite 200 Lansing, MI 48933 mmassey@dewpoint.com 517-258-2750

3. **Contract Administrator.** The Contract Administrator for each party is the only person authorized to modify any terms of this Contract, and approve and execute any change under this Contract (each a "**Contract Administrator**"):

If to State:	If to Contractor:
Steve Motz 525 W. Allegan St., 1ST FLR. NE Lansing, MI 48909 Motzs1@michigan.gov 517-331-6086	Michelle Massey 300 S Washington, Suite 200 Lansing, MI 48933 mmassey@dewpoint.com 517-258-2750

4. **Program Manager.** The Program Manager for each party will monitor and coordinate the day-to-day activities of the Contract (each a "**Program Manager**"):

State:	Contractor:
Derek Larson 7119 S Canal Rd, Lansing, MI 48917 LarsonD4@michigan.gov 517-241-6606	Joe Old 300 S Washington, Suite 200 Lansing, MI 48933 jold@dewpoint.com 810-625-6873

5. **Performance Guarantee.** Contractor must at all times have financial resources sufficient, in the opinion of the State, to ensure performance of the Contract and must provide proof upon request. The State may require a performance bond (as specified in Schedule A) if, in the opinion of the State, it will ensure performance of the Contract.

6. **Insurance Requirements.** Contractor must maintain the insurances identified below and is responsible for all deductibles. All required insurance must: (a) protect the State from claims that may arise out of, are alleged to arise out of, or result from Contractor's or a subcontractor's performance; (b) be primary and non-contributing to any comparable liability insurance (including self-insurance) carried by the State; and (c) be provided by a company with an A.M. Best rating of "A-" or better, and a financial size of VII or better.

Required Limits	Additional Requirements
Commercial General Liability Insurance	
Minimum Limits: $1,000,000 Each Occurrence Limit $1,000,000 Personal & Advertising Injury Limit $2,000,000 General Aggregate Limit $2,000,000 Products/Completed Operations	Contractor must have their policy endorsed to add "the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents" as additional insureds using endorsement CG 20 10 11 85, or both CG 2010 07 04 and CG 2037 07 04.
Automobile Liability Insurance	
If a motor vehicle is used in the performance of the Contract, Contractor must maintain motor vehicle liability coverage for bodily injury and property damage, as required by law, for the term of the Contract.	
Workers' Compensation Insurance	
Minimum Limits: Coverage according to applicable laws governing work activities.	Waiver of subrogation, except where waiver is prohibited by law.
Employers Liability Insurance	
Minimum Limits: $500,000 Each Accident $500,000 Each Employee by Disease $500,000 Aggregate Disease.	
Privacy and Security Liability (Cyber Liability) Insurance	

Minimum Limits: $1,000,000 Each Occurrence $1,000,000 Annual Aggregate	Contractor must have their policy cover information security and privacy liability, privacy notification costs, regulatory defense and penalties, and website media content liability.
Professional Liability (Errors and Omissions) Insurance	
Minimum Limits: $1,000,000 Each Occurrence $1,000,000 Annual Aggregate	

If any of the required policies provide **claims-made** coverage, the Contractor must: (a) provide coverage with a retroactive date before the effective date of the contract or the beginning of Contract Activities; (b) maintain coverage and provide evidence of coverage for at least three (3) years after completion of the Contract Activities; and (c) if coverage is cancelled or not renewed, and not replaced with another claims-made policy form with a retroactive date prior to the contract effective date, Contractor must purchase extended reporting coverage for a minimum of three (3) years after completion of work.

Contractor must: (a) provide insurance certificates to the Contract Administrator, containing the agreement or delivery order number, at Contract formation and within 20 calendar days of the expiration date of the applicable policies; (b) require that subcontractors maintain the required insurances contained in this Section; (c) notify the Contract Administrator within 5 business days if any insurance is cancelled; and (d) waive all rights against the State for damages covered by insurance. Failure to maintain the required insurance does not limit this waiver.

This Section is not intended to and is not to be construed in any manner as waiving, restricting or limiting the liability of either party for any obligations under this Contract (including any provisions hereof requiring Contractor to indemnify, defend and hold harmless the State).

7. **Administrative Fee and Reporting.** Contractor must pay an **administrative fee of 1%** on all payments made to Contractor under the Contract including transactions with the State (including its departments, divisions, agencies, offices, and commissions), MiDEAL members, and other states (including governmental subdivisions and authorized entities). Administrative fee payments must be made online by check or credit card:

   State of MI Admin Fees: https://www.thepayplace.com/mi/dtmb/adminfee
   State of Mi MiDEAL Fees: https://www.thepayplace.com/mi/dtmb/midealfee
   Contractor must submit an itemized purchasing activity report, which includes at a minimum, the name of the purchasing entity and the total dollar volume in sales. Reports should be mailed to MiDeal@michigan.gov.

   The administrative fee and purchasing activity report are due within 30 calendar days from the last day of each calendar quarter.

8. **Extended Purchasing Program.** This contract is extended to MiDEAL members. MiDEAL members include local units of government, school districts, universities, community colleges, and nonprofit hospitals. A current list of MiDEAL members is available at www.michigan.gov/mideal.

   Upon written agreement between the State and Contractor, this contract may also be extended to: (a) other states (including governmental subdivisions and authorized entities) and (b) State of Michigan employees.

   If extended, Contractor must supply all Contract Activities at the established Contract prices and terms. The State reserves the right to impose an administrative fee and negotiate additional discounts based on any increased volume generated by such extensions.

   Contractor must submit invoices to, and receive payment from, extended purchasing program members on a direct and individual basis.

9. **Independent Contractor.** Contractor is an independent contractor and assumes all rights, obligations and liabilities set forth in this Contract. Contractor, its employees, and agents will not be considered employees of the State. No partnership or joint venture relationship is created by virtue of this Contract. Contractor, and not the State, is responsible for the payment of wages, benefits and taxes of Contractor's employees and any subcontractors. Prior performance does not modify Contractor's status as an independent contractor. Contractor hereby acknowledges that the State is and will be the sole and exclusive owner of all right, title, and interest in the Contract Activities and all associated intellectual property rights, if any. Such Contract Activities are works made for hire as defined in Section 101 of the Copyright Act of 1976. To the extent any Contract Activities and related intellectual property do not qualify as works made for hire under the Copyright Act, Contractor will, and hereby does, immediately on its creation, assign, transfer and otherwise convey to the State, irrevocably and in perpetuity, throughout the universe, all right, title and interest in and to the Contract Activities, including all intellectual property rights therein.

10. **Subcontracting.** Contractor may not delegate any of its obligations under the Contract without the prior written approval of the State. Contractor must notify the State at least 90 calendar days before the proposed delegation and provide the State any information it requests to determine whether the delegation is in its best interest. If approved, Contractor must: (a) be the sole point of contact regarding all contractual matters, including payment and charges for all Contract Activities; (b) make all payments to the subcontractor; and (c) incorporate the terms and conditions contained in this Contract in any subcontract with a subcontractor. Contractor remains responsible for the completion of the Contract Activities, compliance with the terms of this Contract, and the acts and omissions of the subcontractor. The State, in its sole discretion, may require the replacement of any subcontractor.

11. **Staffing.** The State's Contract Administrator may require Contractor to remove or reassign personnel by providing a notice to Contractor.

12. **Background Checks.** Pursuant to Michigan law, all agencies subject to IRS Pub. 1075 are required to ask the Michigan State Police to perform fingerprint background checks on all employees, including Contractor and Subcontractor employees, who may have access to any database of information maintained by the federal government that contains confidential or personal information, including, but not limited to, federal tax information. Further, pursuant to Michigan law, any agency described above is prohibited from providing Contractors or Subcontractors with the result of such background check. For more information, please see Michigan Public Act 427 of 2018. Upon request, or as may be specified in Schedule A, Contractor must perform background checks on all employees and subcontractors and its employees prior to their assignment. The scope is at the discretion of the State and documentation must be provided as requested. Contractor is responsible for all costs associated with the requested background checks. The State, in its sole discretion, may also perform background checks.

13. **Assignment.** Contractor may not assign this Contract to any other party without the prior approval of the State. Upon notice to Contractor, the State, in its sole discretion, may assign in whole or in part, its rights or responsibilities under this Contract to any other party. If the State determines that a novation of the Contract to a third party is necessary, Contractor will agree to the novation and provide all necessary documentation and signatures.

14. **Change of Control.** Contractor will notify within 30 days of any public announcement or otherwise once legally permitted to do so, the State of a change in Contractor's organizational structure or ownership. For purposes of this Contract, a change in control means any of the following: (a) a sale of more than 50% of Contractor's stock; (b) a sale of substantially all of Contractor's assets; (c) a change in a majority of Contractor's board members; (d) consummation of a merger or consolidation of Contractor with any other entity; (e) a change in ownership through a transaction or series of transactions; (f) or the board (or the stockholders) approves a plan of complete liquidation. A change of control does not include any consolidation or merger effected exclusively to change the domicile of Contractor, or any transaction or series of transactions principally for bona fide equity financing purposes.

    In the event of a change of control, Contractor must require the successor to assume this Contract and all of its obligations under this Contract.

15. **Ordering.** Contractor is not authorized to begin performance until receipt of authorization as identified in Schedule A.

16. **Acceptance.** Contract Activities are subject to inspection and testing by the State within 30 calendar days of the State's receipt of them ("**State Review Period**"), unless otherwise provided in Schedule A. If the Contract Activities are not fully accepted by the State, the State will notify Contractor by the end of the State Review Period that either: (a) the Contract Activities are accepted but noted deficiencies must be corrected; or (b) the Contract Activities are rejected. If the State finds material deficiencies, it may: (i) reject the Contract Activities without performing any further inspections; (ii) demand performance at no additional cost; or (iii) terminate this Contract in accordance with Section 23, Termination for Cause.

    Within 10 business days from the date of Contractor's receipt of notification of acceptance with deficiencies or rejection of any Contract Activities, Contractor must cure, at no additional cost, the deficiency and deliver unequivocally acceptable Contract Activities to the State. If acceptance with deficiencies or rejection of the Contract Activities impacts the content or delivery of other non-completed Contract Activities, the parties' respective Program Managers must determine an agreed to number of days for re-submission that minimizes the overall impact to the Contract. However, nothing herein affects, alters, or relieves Contractor of its obligations to correct deficiencies in accordance with the time response standards set forth in this Contract.

    If Contractor is unable or refuses to correct the deficiency within the time response standards set forth in this Contract, the State may cancel the order in whole or in part. The State, or a third party identified by the State, may perform the Contract Activities and recover the difference between the cost to cure and the Contract price plus an additional 10% administrative fee.

17. **RESERVED**

18. **RESERVED**

19. **RESERVED**

20. **Terms of Payment.** Invoices must conform to the requirements communicated from time-to-time by the State. All undisputed amounts are payable within 45 days of the State's receipt. Contractor may only charge for Contract Activities performed as specified in Schedule A. Invoices must include an itemized statement of all charges. The State is exempt from State sales tax for direct purchases and may be exempt from federal excise tax, if Services purchased under this Agreement are for the State's exclusive use. All prices are exclusive of taxes, and Contractor is responsible for all sales, use and excise taxes, and any other similar taxes, duties and charges of any kind imposed by any federal, state, or local governmental entity on any amounts payable by the State under this Contract.

    The State has the right to withhold payment of any disputed amounts until the parties agree as to the validity of the disputed amount. The State will notify Contractor of any dispute within a reasonable time. Payment by the State will not constitute a waiver of any rights as to Contractor's continuing obligations, including claims for deficiencies or substandard Contract Activities. Contractor's acceptance of final payment by the State constitutes a waiver of all claims by Contractor against the State for payment under this Contract, other than those claims previously filed in writing on a timely basis and still disputed.

    The State will only disburse payments under this Contract through Electronic Funds Transfer (EFT). Contractor must register with the State at http://www.michigan.gov/SIGMAVSS to receive electronic fund transfer payments. If Contractor does not register, the State is not liable for failure to provide payment. Without prejudice to any other right or remedy it may have, the State reserves the right to set off at any time any amount then due and owing to it by Contractor against any amount payable by the State to Contractor under this Contract.

21. **Liquidated Damages.** Liquidated damages, if applicable, will be assessed as described in Schedule A. Late or improper completion of the Contract Activities will cause loss and damage to the State and it would be impracticable and extremely difficult to fix the actual damage sustained by the State. Therefore, if there is late or improper completion of the Contract Activities the State is entitled to collect liquidated damages in the amount of $500 and an additional $1,000 per day for each day Contractor fails to remedy the late or improper completion of the Work in Exhibit A and SOW requirements.

22. **Stop Work Order.** The State may suspend any or all activities under the Contract at any time. The State will provide Contractor a written stop work order detailing the suspension. Contractor must comply with the stop work order upon receipt. Within 90 calendar days, or any longer period agreed to by Contractor, the State will either: (a) issue a notice authorizing Contractor to resume work, or (b) terminate the Contract

or delivery order. The State will not pay for Contract Activities, Contractor's lost profits, or any additional compensation during a stop work period.

23. Termination for Cause. The State may terminate this Contract for cause, in whole or in part, if Contractor, as determined by the State: (a) endangers the value, integrity, or security of any location, data, or personnel; (b) becomes insolvent, petitions for bankruptcy court proceedings, or has an involuntary bankruptcy proceeding filed against it by any creditor; (c) engages in any conduct that may expose the State to liability; (d) breaches any of its material duties or obligations; or (e) fails to cure a breach within the time stated in a notice of breach. Any reference to specific breaches being material breaches within this Contract will not be construed to mean that other breaches are not material.

If the State terminates this Contract under this Section, the State will issue a termination notice specifying whether Contractor must: (a) cease performance immediately, or (b) continue to perform for a specified period. If it is later determined that Contractor was not in breach of the Contract, the termination will be deemed to have been a Termination for Convenience, effective as of the same date, and the rights and obligations of the parties will be limited to those provided in Section 24, Termination for Convenience.

The State will only pay for amounts due to Contractor for Contract Activities accepted by the State on or before the date of termination, subject to the State's right to set off any amounts owed by the Contractor for the State's reasonable costs in terminating this Contract. The Contractor must pay all reasonable costs incurred by the State in terminating this Contract for cause, including administrative costs, attorneys' fees, court costs, transition costs, and any costs the State incurs to procure the Contract Activities from other sources.

24. Termination for Convenience. The State may immediately terminate this Contract in whole or in part without penalty and for any reason, including but not limited to, appropriation or budget shortfalls. The termination notice will specify whether Contractor must: (a) cease performance of the Contract Activities immediately, or (b) continue to perform the Contract Activities in accordance with Section 25, Transition Responsibilities. If the State terminates this Contract for convenience, the State will pay all reasonable costs, as determined by the State, for State approved Transition Responsibilities.

25. Transition Responsibilities. Upon termination or expiration of this Contract for any reason, Contractor must, for a period of time specified by the State (not to exceed 180 calendar days), provide all reasonable transition assistance requested by the State, to allow for the expired or terminated portion of the Contract Activities to continue without interruption or adverse effect, and to facilitate the orderly transfer of such Contract Activities to the State or its designees. Such transition assistance may include, but is not limited to: (a) continuing to perform the Contract Activities at the established Contract rates; (b) taking all reasonable and necessary measures to transition performance of the work, including all applicable Contract Activities, training, equipment, software, leases, reports and other documentation, to the State or the State's designee; (c) taking all necessary and appropriate steps, or such other action as the State may direct, to preserve, maintain, protect, or return to the State all materials, data, property, and confidential information provided directly or indirectly to Contractor by any entity, agent, vendor, or employee of the State; (d) transferring title in and delivering to the State, at the State's discretion, all completed or partially completed deliverables prepared under this Contract as of the Contract termination date; and (e) preparing an accurate accounting from which the State and Contractor may reconcile all outstanding accounts (collectively, "**Transition Responsibilities**"). This Contract will automatically be extended through the end of the transition period.

26. General Indemnification. Contractor must defend, indemnify and hold the State, its departments, divisions, agencies, offices, commissions, officers, and employees harmless, without limitation, from and against any and all actions, claims, losses, liabilities, damages, costs, attorney fees, and expenses (including those required to establish the right to indemnification), arising out of or relating to: (a) any breach by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable) of any of the promises, agreements, representations, warranties, or insurance requirements contained in this Contract; (b) any infringement, misappropriation, or other violation of any intellectual property right or other right of any third party; (c) any bodily injury, death, or damage to real or tangible personal property occurring wholly or in part due to action or inaction by Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable); and (d) any acts or omissions of Contractor (or any of Contractor's employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable).

The State will notify Contractor in writing if indemnification is sought; however, failure to do so will not relieve Contractor, except to the extent that Contractor is materially prejudiced. Contractor must, to the satisfaction of the State, demonstrate its financial ability to carry out these obligations.

The State is entitled to: (i) regular updates on proceeding status; (ii) participate in the defense of the proceeding; (iii) employ its own counsel; and to (iv) retain control of the defense if the State deems necessary. Contractor will not, without the State's written consent (not to be unreasonably withheld), settle, compromise, or consent to the entry of any judgment in or otherwise seek to terminate any claim, action, or proceeding. To the extent that any State employee, official, or law may be involved or challenged, the State may, at its own expense, control the defense of that portion of the claim.

Any litigation activity on behalf of the State, or any of its subdivisions under this Section, must be coordinated with the Department of Attorney General. An attorney designated to represent the State may not do so until approved by the Michigan Attorney General and appointed as a Special Assistant Attorney General.

27. Infringement Remedies. If, in either party's opinion, any piece of equipment, software, commodity, or service supplied by Contractor or its subcontractors, or its operation, use or reproduction, is likely to become the subject of a copyright, patent, trademark, or trade secret infringement claim, Contractor must, at its expense: (a) procure for the State the right to continue using the equipment, software, commodity, or service, or if this option is not reasonably available to Contractor, (b) replace or modify the same so that it becomes non-infringing; or (c) accept its return by the State with appropriate credits to the State against Contractor's charges and reimburse the State for any losses or costs incurred as a consequence of the State ceasing its use and returning it.

28. Limitation of Liability and Disclaimer of Damages. IN NO EVENT WILL THE STATE'S AGGREGATE LIABILITY TO CONTRACTOR UNDER THIS CONTRACT, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT, EXCEED THE MAXIMUM AMOUNT OF FEES PAYABLE UNDER THIS CONTRACT. The State is not liable for consequential, incidental, indirect, or special damages, regardless of the nature of the action.

29. Disclosure of Litigation, or Other Proceeding. Contractor must notify the State within 14 calendar days of receiving notice of any litigation, investigation, arbitration, or other proceeding (collectively, "**Proceeding**") involving Contractor, a subcontractor, or an officer or director of Contractor or subcontractor, that arises during the term of the Contract, including: (a) a criminal Proceeding; (b) a parole or probation Proceeding; (c) a Proceeding under the Sarbanes-Oxley Act; (d) a civil Proceeding involving: (1) a claim that might reasonably be expected to adversely affect Contractor's viability or financial stability; or (2) a governmental or public entity's claim or written allegation of fraud; or (e) a Proceeding involving any license that Contractor is required to possess in order to perform under this Contract.

30. RESERVED.

31. State Data.

a. Ownership. The State's data ("**State Data**," which will be treated by Contractor as Confidential Information) includes: (a) the State's data collected, used, processed, stored, or generated as the result of the Contract Activities; (b) personally identifiable information ("**PII**") collected, used, processed, stored, or generated as the result of the Contract Activities, including, without limitation, any information that identifies an individual, such as an individual's social security number or other government-issued identification number, date of birth, address, telephone number, biometric data, mother's maiden name, email address, credit card information, or an individual's name in combination with any other of the elements here listed; and, (c) personal health information ("**PHI**") collected, used, processed, stored, or generated as the result of the Contract Activities, which is defined under the Health Insurance Portability and Accountability Act (HIPAA) and its related rules and regulations. State Data is and will remain the sole and exclusive property of the State and all right, title, and interest in the same is reserved by the State. This Section survives the termination of this Contract.

b. Contractor Use of State Data. Contractor is provided a limited license to State Data for the sole and exclusive purpose of providing the Contract Activities, including a license to collect, process, store, generate, and display State Data only to the extent necessary in the provision of the Contract

Activities. Contractor must: (a) keep and maintain State Data in strict confidence, using such degree of care as is appropriate and consistent with its obligations as further described in this Contract and applicable law to avoid unauthorized access, use, disclosure, or loss; (b) use and disclose State Data solely and exclusively for the purpose of providing the Contract Activities, such use and disclosure being in accordance with this Contract, any applicable Statement of Work, and applicable law; and (c) not use, sell, rent, transfer, distribute, or otherwise disclose or make available State Data for Contractor's own purposes or for the benefit of anyone other than the State without the State's prior written consent. This Section survives the termination of this Contract.

c. Extraction of State Data. Contractor must, within five (5) business days of the State's request, provide the State, without charge and without any conditions or contingencies whatsoever (including but not limited to the payment of any fees due to Contractor), an extract of the State Data in the format specified by the State.

d. Backup and Recovery of State Data. Unless otherwise specified in Schedule A, Contractor is responsible for maintaining a backup of State Data and for an orderly and timely recovery of such data. Unless otherwise described in Schedule A, Contractor must maintain a contemporaneous backup of State Data that can be recovered within two (2) hours at any point in time.

e. Loss or Compromise of Data. In the event of any act, error or omission, negligence, misconduct, or breach on the part of Contractor that compromises or is suspected to compromise the security, confidentiality, or integrity of State Data or the physical, technical, administrative, or organizational safeguards put in place by Contractor that relate to the protection of the security, confidentiality, or integrity of State Data, Contractor must, as applicable: (a) notify the State as soon as practicable but no later than twenty-four (24) hours of becoming aware of such occurrence; (b) cooperate with the State in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by the State; (c) in the case of PII or PHI, at the State's sole election, (i) with approval and assistance from the State, notify the affected individuals who comprise the PII or PHI as soon as practicable but no later than is required to comply with applicable law, or, in the absence of any legally required notification period, within five (5) calendar days of the occurrence; or (ii) reimburse the State for any costs in notifying the affected individuals; (d) in the case of PII, provide third-party credit and identity monitoring services to each of the affected individuals who comprise the PII for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for no less than twenty-four (24) months following the date of notification to such individuals; (e) perform or take any other actions required to comply with applicable law as a result of the occurrence; (f) pay for any costs associated with the occurrence, including but not limited to any costs incurred by the State in investigating and resolving the occurrence, including reasonable attorney's fees associated with such investigation and resolution; (g) without limiting Contractor's obligations of indemnification as further described in this Contract, indemnify, defend, and hold harmless the State for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the State in connection with the occurrence; (h) be responsible for recreating lost State Data in the manner and on the schedule set by the State without charge to the State; and (i) provide to the State a detailed plan within ten (10) calendar days of the occurrence describing the measures Contractor will undertake to prevent a future occurrence. Notification to affected individuals, as described above, must comply with applicable law, be written in plain language, not be tangentially used for any solicitation purposes, and contain, at a minimum: name and contact information of Contractor's representative; a description of the nature of the loss; a list of the types of data involved; the known or approximate date of the loss; how such loss may affect the affected individual; what steps Contractor has taken to protect the affected individual; what steps the affected individual can take to protect himself or herself; contact information for major credit card reporting agencies; and, information regarding the credit and identity monitoring services to be provided by Contractor. The State will have the option to review and approve any notification sent to affected individuals prior to its delivery. Notification to any other party, including but not limited to public media outlets, must be reviewed and approved by the State in writing prior to its dissemination. The parties agree that any damages relating to a breach of this **Section 31** are to be considered direct damages and not consequential damages. This section survives termination or expiration of this Contract.

f. State's Governance, Risk and Compliance (GRC) platform. Contractor is required to assist the State with its security accreditation process through the development, completion and ongoing updating of

a system security plan using the State's automated GRC platform and implement any required safeguards or remediate any security vulnerabilities as identified by the results of the security accreditation process.

32. Non-Disclosure of Confidential Information. The parties acknowledge that each party may be exposed to or acquire communication or data of the other party that is confidential, privileged communication not intended to be disclosed to third parties. The provisions of this Section survive the termination of this Contract.

a. Meaning of Confidential Information. For the purposes of this Contract, the term "**Confidential Information**" means all information and documentation of a party that: (a) has been marked "confidential" or with words of similar meaning, at the time of disclosure by such party; (b) if disclosed orally or not marked "confidential" or with words of similar meaning, was subsequently summarized in writing by the disclosing party and marked "confidential" or with words of similar meaning; and, (c) should reasonably be recognized as confidential information of the disclosing party. The term "Confidential Information" does not include any information or documentation that was: (a) subject to disclosure under the Michigan Freedom of Information Act (FOIA); (b) already in the possession of the receiving party without an obligation of confidentiality; (c) developed independently by the receiving party, as demonstrated by the receiving party, without violating the disclosing party's proprietary rights; (d) obtained from a source other than the disclosing party without an obligation of confidentiality; or, (e) publicly available when received, or thereafter became publicly available (other than through any unauthorized disclosure by, through, or on behalf of, the receiving party). For purposes of this Contract, in all cases and for all matters, State Data is deemed to be Confidential Information.

b. Obligation of Confidentiality. The parties agree to hold all Confidential Information in strict confidence and not to copy, reproduce, sell, transfer, or otherwise dispose of, give or disclose such Confidential Information to third parties other than employees, agents, or subcontractors of a party who have a need to know in connection with this Contract or to use such Confidential Information for any purposes whatsoever other than the performance of this Contract. The parties agree to advise and require their respective employees, agents, and subcontractors of their obligations to keep all Confidential Information confidential. Disclosure to a subcontractor is permissible where: (a) use of a subcontractor is authorized under this Contract; (b) the disclosure is necessary or otherwise naturally occurs in connection with work that is within the subcontractor's responsibilities; and (c) Contractor obligates the subcontractor in a written contract to maintain the State's Confidential Information in confidence. At the State's request, any employee of Contractor or any subcontractor may be required to execute a separate agreement to be bound by the provisions of this Section.

c. Cooperation to Prevent Disclosure of Confidential Information. Each party must use its best efforts to assist the other party in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the foregoing, each party must advise the other party immediately in the event either party learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Contract and each party will cooperate with the other party in seeking injunctive or other equitable relief against any such person.

d. Remedies for Breach of Obligation of Confidentiality. Each party acknowledges that breach of its obligation of confidentiality may give rise to irreparable injury to the other party, which damage may be inadequately compensable in the form of monetary damages. Accordingly, a party may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies which may be available, to include, in the case of the State, at the sole election of the State, the immediate termination, without liability to the State, of this Contract or any Statement of Work corresponding to the breach or threatened breach.

e. Surrender of Confidential Information upon Termination. Upon termination of this Contract or a Statement of Work, in whole or in part, each party must, within 5 calendar days from the date of termination, return to the other party any and all Confidential Information received from the other party, or created or received by a party on behalf of the other party, which are in such party's possession, custody, or control; provided, however, that Contractor must return State Data to the State following the timeframe and procedure described further in this Contract. Should Contractor or the State determine that the return of any Confidential Information is not feasible, such party must destroy the Confidential Information and must certify the same in writing within 5 calendar days from

the date of termination to the other party. However, the State's legal ability to destroy Contractor data may be restricted by its retention and disposal schedule, in which case Contractor's Confidential Information will be destroyed after the retention period expires.

33. Data Privacy and Information Security.

a. Undertaking by Contractor. Without limiting Contractor's obligation of confidentiality as further described, Contractor is responsible for establishing and maintaining a data privacy and information security program, including physical, technical, administrative, and organizational safeguards, that is designed to: (a) ensure the security and confidentiality of the State Data; (b) protect against any anticipated threats or hazards to the security or integrity of the State Data; (c) protect against unauthorized disclosure, access to, or use of the State Data; (d) ensure the proper disposal of State Data; and (e) ensure that all employees, agents, and subcontractors of Contractor, if any, comply with all of the foregoing. In no case will the safeguards of Contractor's data privacy and information security program be less stringent than the safeguards used by the State, and Contractor must at all times comply with all applicable State IT policies and standards, which are available to Contractor upon request.

b. Audit by Contractor. No less than annually, Contractor must conduct a comprehensive independent third-party audit of its data privacy and information security program and provide such audit findings to the State.

c. Right of Audit by the State. Without limiting any other audit rights of the State, the State has the right to review Contractor's data privacy and information security program prior to the commencement of Contract Activities and from time to time during the term of this Contract. During the providing of the Contract Activities, on an ongoing basis from time to time and without notice, the State, at its own expense, is entitled to perform, or to have performed, an on-site audit of Contractor's data privacy and information security program. In lieu of an on-site audit, upon request by the State, Contractor agrees to complete, within 45 calendar days of receipt, an audit questionnaire provided by the State regarding Contractor's data privacy and information security program.

d. Audit Findings. Contractor must implement any required safeguards as identified by the State or by any audit of Contractor's data privacy and information security program.

e. State's Right to Termination for Deficiencies. The State reserves the right, at its sole election, to immediately terminate this Contract or a Statement of Work without limitation and without liability if the State determines that Contractor fails or has failed to meet its obligations under this Section.

34. RESERVED

35. RESERVED

36. Records Maintenance, Inspection, Examination, and Audit. The State or its designee may audit Contractor to verify compliance with this Contract. Contractor must retain and provide to the State or its designee and the auditor general upon request, all financial and accounting records related to the Contract through the term of the Contract and for 4 years after the latter of termination, expiration, or final payment under this Contract or any extension ("**Audit Period**"). If an audit, litigation, or other action involving the records is initiated before the end of the Audit Period, Contractor must retain the records until all issues are resolved.

Within 10 calendar days of providing notice, the State and its authorized representatives or designees have the right to enter and inspect Contractor's premises or any other places where Contract Activities are being performed, and examine, copy, and audit all records related to this Contract. Contractor must cooperate and provide reasonable assistance. If any financial errors are revealed, the amount in error must be reflected as a credit or debit on subsequent invoices until the amount is paid or refunded. Any remaining balance at the end of the Contract must be paid or refunded within 45 calendar days.

This Section applies to Contractor, any parent, affiliate, or subsidiary organization of Contractor, and any subcontractor that performs Contract Activities in connection with this Contract.

37. Warranties and Representations. Contractor represents and warrants: (a) Contractor is the owner or licensee of any Contract Activities that it licenses, sells, or develops and Contractor has the rights

necessary to convey title, ownership rights, or licensed use; (b) all Contract Activities are delivered free from any security interest, lien, or encumbrance and will continue in that respect; (c) the Contract Activities will not infringe the patent, trademark, copyright, trade secret, or other proprietary rights of any third party; (d) Contractor must assign or otherwise transfer to the State or its designee any manufacturer's warranty for the Contract Activities; (e) the Contract Activities are merchantable and fit for the specific purposes identified in the Contract; (f) the Contract signatory has the authority to enter into this Contract; (g) all information furnished by Contractor in connection with the Contract fairly and accurately represents Contractor's business, properties, finances, and operations as of the dates covered by the information, and Contractor will inform the State of any material adverse changes;(h) all information furnished and representations made in connection with the award of this Contract is true, accurate, and complete, and contains no false statements or omits any fact that would make the information misleading; and that (i) Contractor is neither currently engaged in nor will engage in the boycott of a person based in or doing business with a strategic partner as described in 22 USC 8601 to 8606. A breach of this Section is considered a material breach of this Contract, which entitles the State to terminate this Contract under Section 23, Termination for Cause.

38. **Conflicts and Ethics.** Contractor will uphold high ethical standards and is prohibited from: (a) holding or acquiring an interest that would conflict with this Contract; (b) doing anything that creates an appearance of impropriety with respect to the award or performance of the Contract; (c) attempting to influence or appearing to influence any State employee by the direct or indirect offer of anything of value; or (d) paying or agreeing to pay any person, other than employees and consultants working for Contractor, any consideration contingent upon the award of the Contract. Contractor must immediately notify the State of any violation or potential violation of these standards. This Section applies to Contractor, any parent, affiliate, or subsidiary organization of Contractor, and any subcontractor that performs Contract Activities in connection with this Contract.

39. **Compliance with Laws.** Contractor must comply with all federal, state and local laws, rules and regulations.

40. **RESERVED.**

41. **RESERVED.**

42. **Nondiscrimination.** Under the Elliott-Larsen Civil Rights Act, 1976 PA 453, MCL 37.2101, *et seq*., the Persons with Disabilities Civil Rights Act, 1976 PA 220, MCL 37.1101, *et seq*., and Executive Directive 2019-09. Contractor and its subcontractors agree not to discriminate against an employee or applicant for employment with respect to hire, tenure, terms, conditions, or privileges of employment, or a matter directly or indirectly related to employment, because of race, color, religion, national origin, age, sex (as defined in Executive Directive 2019-09), height, weight, marital status, partisan considerations, any mental or physical disability, or genetic information that is unrelated to the person's ability to perform the duties of a particular job or position. Breach of this covenant is a material breach of this Contract.

43. **Unfair Labor Practice.** Under MCL 423.324, the State may void any Contract with a Contractor or subcontractor who appears on the Unfair Labor Practice register compiled under MCL 423.322.

44. **Governing Law.** This Contract is governed, construed, and enforced in accordance with Michigan law, excluding choice-of-law principles, and all claims relating to or arising out of this Contract are governed by Michigan law, excluding choice-of-law principles. Any dispute arising from this Contract must be resolved in Michigan Court of Claims. Contractor consents to venue in Ingham County, and waives any objections, such as lack of personal jurisdiction or *forum non conveniens*. Contractor must appoint agents in Michigan to receive service of process.

45. **Non-Exclusivity.** Nothing contained in this Contract is intended nor will be construed as creating any requirements contract with Contractor. This Contract does not restrict the State or its agencies from acquiring similar, equal, or like Contract Activities from other sources.

46. **Force Majeure.** Neither party will be in breach of this Contract because of any failure arising from any disaster or acts of god that are beyond their control and without their fault or negligence. Each party will use commercially reasonable efforts to resume performance. Contractor will not be relieved of a breach or delay caused by its subcontractors. If immediate performance is necessary to ensure public health and safety, the State may immediately contract with a third party.

47. **Dispute Resolution.** The parties will endeavor to resolve any Contract dispute in accordance with this provision. The dispute will be referred to the parties' respective Contract Administrators or Program Managers. Such referral must include a description of the issues and all supporting documentation. The parties must submit the dispute to a senior executive if unable to resolve the dispute within 15 business days. The parties will continue performing while a dispute is being resolved, unless the dispute precludes performance. A dispute involving payment does not preclude performance.

    Litigation to resolve the dispute will not be instituted until after the dispute has been elevated to the parties' senior executive and either concludes that resolution is unlikely or fails to respond within 15 business days. The parties are not prohibited from instituting formal proceedings: (a) to avoid the expiration of statute of limitations period; (b) to preserve a superior position with respect to creditors; or (c) where a party makes a determination that a temporary restraining order or other injunctive relief is the only adequate remedy. This Section does not limit the State's right to terminate the Contract.

48. **Media Releases.** News releases (including promotional literature and commercial advertisements) pertaining to the Contract or project to which it relates must not be made without prior written State approval, and then only in accordance with the explicit written instructions of the State.

49. **Website Incorporation.** The State is not bound by any content on Contractor's website unless expressly incorporated directly into this Contract.

50. **Schedules.** All Schedules and Exhibits that are referenced herein and attached hereto are hereby incorporated by reference. The following Schedules are attached hereto and incorporated herein:

Schedule A	Statement of Work
Schedule B	Pricing
Exhibit 1	Request for Cyber Assessment Service Request for Quote (RFQ)
Exhibit 2	Document Samples/Attachments

51. **Entire Agreement and Order of Precedence.** This Contract, which includes Schedule A – Statement of Work, and schedules and exhibits which are hereby expressly incorporated, is the entire agreement of the parties related to the Contract Activities. This Contract supersedes and replaces all previous understandings and agreements between the parties for the Contract Activities. If there is a conflict between documents, the order of precedence is: (a) first, this Contract, excluding its schedules, exhibits, and Schedule A – Statement of Work; (b) second, Schedule A – Statement of Work as of the Effective Date; and (c) third, schedules expressly incorporated into this Contract as of the Effective Date. NO TERMS ON CONTRACTOR'S INVOICES, ORDERING DOCUMENTS, WEBSITE, BROWSE-WRAP, SHRINK-WRAP, CLICK-WRAP, CLICK-THROUGH OR OTHER NON-NEGOTIATED TERMS AND CONDITIONS PROVIDED WITH ANY OF THE CONTRACT ACTIVITIES WILL CONSTITUTE A PART OR AMENDMENT OF THIS CONTRACT OR IS BINDING ON THE STATE FOR ANY PURPOSE. ALL SUCH OTHER TERMS AND CONDITIONS HAVE NO FORCE AND EFFECT AND ARE DEEMED REJECTED BY THE STATE, EVEN IF ACCESS TO OR USE OF THE CONTRACT ACTIVITIES REQUIRES AFFIRMATIVE ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

52. **Severability.** If any part of this Contract is held invalid or unenforceable, by any court of competent jurisdiction, that part will be deemed deleted from this Contract and the severed part will be replaced by agreed upon language that achieves the same or similar objectives. The remaining Contract will continue in full force and effect.

53. **Waiver.** Failure to enforce any provision of this Contract will not constitute a waiver.

54. **Survival.** The provisions of this Contract that impose continuing obligations, including warranties and representations, termination, transition, insurance coverage, indemnification, and confidentiality, will survive the expiration or termination of this Contract.

55. **Contract Modification.** This Contract may not be amended except by signed agreement between the parties (a "**Contract Change Notice**"). Notwithstanding the foregoing, no subsequent Statement of Work or Contract Change Notice executed after the Effective Date will be construed to amend this Contract unless it specifically states its intent to do so and cites the section or sections amended.

Federal Provisions Addendum

The provisions in this addendum may apply if the purchase will be paid for in whole or in part with funds obtained from the federal government. If any provision below is not required by federal law for this Contract, then it does not apply and must be disregarded. If any provision below is required to be included in this Contract by federal law, then the applicable provision applies, and the language is not negotiable. If any provision below conflicts with the State's terms and conditions, including any attachments, schedules, or exhibits to the State's Contract, the provisions below take priority to the extent a provision is required by federal law; otherwise, the order of precedence set forth in the Contract applies. Hyperlinks are provided for convenience only; broken hyperlinks will not relieve Contractor from compliance with the law.

1. **Federally Assisted Construction Contracts.** If this contract is a "**federally assisted construction contract**" as defined in 41 CRF Part 60-1.3, and except as otherwise may be provided under 41 CRF Part 60, then during performance of this Contract, the Contractor agrees as follows:

   (1) The Contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, sexual orientation, gender identity, or national origin. The Contractor will take affirmative action to ensure that applicants are employed, and that employees are treated during employment without regard to their race, color, religion, sex, sexual orientation, gender identity, or national origin. Such action shall include, but not be limited to the following:

   Employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided setting forth the provisions of this nondiscrimination clause.

   (2) The Contractor will, in all solicitations or advertisements for employees placed by or on behalf of the Contractor, state that all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, or national origin.

   (3) The Contractor will not discharge or in any other manner discriminate against any employee or applicant for employment because such employee or applicant has inquired about, discussed, or disclosed the compensation of the employee or applicant or another employee or applicant. This provision shall not apply to instances in which an employee who has access to the compensation information of other employees or applicants as a part of such employee's essential job functions discloses the compensation of such other employees or applicants to individuals who do not otherwise have access to such information, unless such disclosure is in response to a formal complaint or charge, in furtherance of an investigation, proceeding, hearing, or action, including an investigation conducted by the employer, or is consistent with the Contractor's legal duty to furnish information.

   (4) The Contractor will send to each labor union or representative of workers with which he has a collective bargaining agreement or other contract or understanding, a notice to be provided advising the said labor union or workers' representatives of the Contractor's commitments under this section, and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

   (5) The Contractor will comply with all provisions of Executive Order 11246 of September 24, 1965, and of the rules, regulations, and relevant orders of the Secretary of Labor.

   (6) The Contractor will furnish all information and reports required by Executive Order 11246 of September 24, 1965, and by rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to his books, records, and accounts by the administering agency and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules, regulations, and orders.

   (7) In the event of the Contractor's noncompliance with the nondiscrimination clauses of this contract or with any of the said rules, regulations, or orders, this Contract may be canceled, terminated, or suspended in whole or in part and the Contractor may be declared ineligible for further Government contracts or federally assisted construction contracts in accordance with procedures authorized in Executive Order 11246 of September 24, 1965, and such other sanctions may be imposed and remedies invoked as provided in Executive Order 11246 of September 24, 1965, or by rule, regulation, or order of the Secretary of Labor, or as otherwise provided by law.

(8) The Contractor will include the portion of the sentence immediately preceding paragraph (1) and the provisions of paragraphs (1) through (8) in every subcontract or purchase order unless exempted by rules, regulations, or orders of the Secretary of Labor issued pursuant to section 204 of Executive Order 11246 of September 24, 1965, so that such provisions will be binding upon each subcontractor or vendor. The Contractor will take such action with respect to any subcontract or purchase order as the administering agency may direct as a means of enforcing such provisions, including sanctions for noncompliance:

Provided, however, that in the event a Contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such direction by the administering agency, the Contractor may request the United States to enter into such litigation to protect the interests of the United States.

2. **Davis-Bacon Act (Prevailing Wage)**

   a. If applicable, the Contractor (and its Subcontractors) for **prime construction contracts** in excess of $2,000 must comply with the Davis-Bacon Act (40 USC 3141-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction").

   b. The Contractor (and its Subcontractors) shall pay all mechanics and laborers employed directly on the site of the work, unconditionally and at least once a week, and without subsequent deduction or rebate on any account, the full amounts accrued at time of payment, computed at wage rates not less than those stated in the advertised specifications, regardless of any contractual relationship which may be alleged to exist between the Contractor or subcontractor and the laborers and mechanics;

   c. The Contractor will post the scale of wages to be paid in a prominent and easily accessible place at the site of the work;

   d. There may be withheld from the Contractor so much of accrued payments as the contracting officer considers necessary to pay to laborers and mechanics employed by the Contractor or any Subcontractor on the work the difference between the rates of wages required by the Contract to be paid laborers and mechanics on the work and the rates of wages received by the laborers and mechanics and not refunded to the Contractor or Subcontractors or their agents.

3. **Copeland "Anti-Kickback" Act.** If applicable, the Contractor must comply with the Copeland "Anti-Kickback" Act (40 USC 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"), which prohibits the Contractor and subrecipients from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled.

4. **Contract Work Hours and Safety Standards Act.** If the Contract is **in excess of $100,000** and **involves the employment of mechanics or laborers**, the Contractor must comply with 40 USC 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5), as applicable.

5. **Rights to Inventions Made Under a Contract or Agreement.** If the Contract is funded by a federal "funding agreement" as defined under 37 CFR §401.2 (a) and the recipient or subrecipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that "funding agreement," the recipient or subrecipient must comply with 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

6. **Clean Air Act.** If this Contract is **in excess of $150,000,** the Contractor must comply with all applicable standards, orders, and regulations issued under the Clean Air Act (42 USC 7401-7671q) and the Federal Water Pollution Control Act (33 USC 1251-1387). Violations must be reported to the federal awarding agency and the regional office of the Environmental Protection Agency.

7. **Debarment and Suspension.** A "contract award" (see 2 CFR 180.220) must not be made to parties listed on the government-wide exclusions in the System for Award Management (SAM), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR part 1986 Comp., p. 189) and 12689 (3 CFR part 1989 Comp., p. 235), "Debarment and Suspension." SAM Exclusions contains the names of parties debarred,

suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549.

8. **Byrd Anti-Lobbying Amendment.** If this Contract **exceeds $100,000**, bidders and the Contractor must file the certification required under 31 USC 1352.

9. **Procurement of Recovered Materials.** Under 2 CFR 200.322, a non-Federal entity that is a state agency or agency of a political subdivision of a state **and its contractors** must comply with section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act. The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds $10,000 or the value of the quantity acquired during the preceding fiscal year exceeded $10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery; and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

Byrd Anti-Lobbying Certification

The following certification and disclosure regarding payments to influence certain federal transactions are made under FAR 52.203-11 and 52.203-12 and 31 USC 1352, the "Byrd Anti-Lobbying Amendment." Hyperlinks are provided for convenience only; broken hyperlinks will not relieve Contractor from compliance with the law.

1. FAR 52.203-12, "Limitation on Payments to Influence Certain Federal Transactions" is hereby incorporated by reference into this certification.

2. The Contractor, hereby certifies to the best of his or her knowledge and belief that:

   a. No federal **appropriated** funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress on his or her behalf in connection with the awarding of any federal contract, the making of any federal grant, the making of any federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment or modification of any federal contract, grant, loan, or cooperative agreement;

   b. If any funds **other than federal appropriated funds** (including profit or fee received under a covered federal transaction) have been paid, or will be paid, to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress on his or her behalf **in connection with this solicitation**, the Contractor must complete and submit, with its proposal, OMB standard form LLL, Disclosure of Lobbying Activities, to the Solicitation Manager; and

   c. He or she will include the language of this certification in all subcontract awards at any tier and require that all recipients of subcontract awards in excess of $150,000 must certify and disclose accordingly.

3. This certification is a material representation of fact upon which reliance is placed at the time of Contract award. Submission of this certification and disclosure is a prerequisite for making or entering into this Contract under 31 USC 1352. Any person making an expenditure prohibited under this provision or who fails to file or amend the disclosure form to be filed or amended by this provision is subject to a civil penalty of not less than $10,000, and not more than $100,000, for each such failure.

Signed by:

_____

Date: _____

STATE OF MICHIGAN

Contract No. 210000000301

Independent Cyber Assessment for Local Entities in Michigan

SCHEDULE A
STATEMENT OF WORK
CONTRACT ACTIVITIES

BACKGROUND

This is a Contract for Independent Cyber Assessment Services for local public entities in Michigan. This Contract is available to local public entities through the State of Michigan's MiDEAL program which will fast-track their ability to get needed cybersecurity assessment services. This is one of multiple optional use Cyber Assessment Services contracts that are available to MiDEAL members throughout the State.

Through this Contract, the State of Michigan and local partners seek to improve the cybersecurity posture of local public entities in Michigan by using a common cybersecurity framework. This includes cities, townships, villages, counties, school districts, universities, community colleges and nonprofit hospitals. The CIS Controls will be the selected nationally recognized framework for the purposes of this Contract. The State of Michigan has pre-qualified multiple vendors through a competitive RFP process and each awarded contract is available through the MIDEAL program. A local public entity can contract with any of the vendors selected through the competitive RFP to provide assessment, planning, and coaching services using the CIS Controls.

For additional information on these contracts, please see www.michigan.gov/cyberpartners.

The goals of this statewide initiative include:

- Guide the improvement of cyber posture of local entities across Michigan through risk-based assessment and planning.
- Provide standard assessment methodology and outputs in order to:
  - Create a common language about cybersecurity
  - Create opportunities for ongoing collaboration
- Provide local entities a choice in selecting an appropriate assessor.
- Through this work, we will continue to build public private collaboration in cybersecurity.

Contracts with local entities are expected to be an annual agreement with the option to renew. The assessors will conduct an initial assessment and engage with the local entity throughout the year to guide the improvement of the local entity's cybersecurity posture.

The State reserves the right to recompete at its sole discretion to add additional vendors to this prequalification program. Existing contractors will not be required to submit new proposals during recompete until all option years of this Contract have been exhausted.

SCOPE AND REQUIREMENTS

Independent Assessors

Vendors conducting cybersecurity assessments under this agreement shall act as independent assessors:

- Provide an independent lens on the contracting entity's cyber posture using the CIS Controls Implementation Group 1.
- Make recommendations on implementation or improvement of cyber posture that are in the best interest of the contracting entity.

Common Cybersecurity Framework – CIS Controls

The cybersecurity assessment shall be conducted using the CIS 20 Controls, which are developed and maintained by the Center for Internet Security. The assessment will use the Controls Self-Assessment (CSAT) tool and focus initially on the Controls Implementation Group 1 which focuses on cyber hygiene.

- CIS Controls: https://www.cisecurity.org/controls
- Controls Self-Assessment Tool (CSAT): https://www.cisecurity.org/blog/cis-csat-free-tool-assessing-implementation-of-cis-controls/
- Contracting Entity will register themselves and add Contractor to their assessment account. https://csat.cisecurity.org/accounts/signup/

1. General Requirements

A. Core Service Offering Deliverables (Price in Schedule B)

The Contractor shall perform all Core Service Offering Deliverables as part of the engagement:

	Core Service Offering Deliverables	References and Sample Documents
1	On-site cybersecurity assessment jointly completed by an independent assessor and local entity staff using the CIS Controls Self-Assessment Tool (CSAT).	Contracting Entity will register themselves and add Contractor to their assessment account. https://www.cisecurity.org/blog/cis-csat-free-tool-assessing-implementation-of-cis-controls/
2	Current-state report (based on CSAT) to the local public entity's leadership identifying the overall assessment results including most important vulnerabilities and recommended next steps.	Vendor will use sample attachment or equivalent format/template. See **Exhibit 2, Attachment 3** – SAMPLE CIS Controls IG 1 Assessment and Plan and **Exhibit 2, Attachment 1** – SAMPLE CSAT Assessment Report.
3	Annual Cybersecurity Improvement Plan that identifies priority actions to complete in the coming 12 months and other priority activities that have a longer time horizon.	Vendor will use sample attachment or equivalent format/template. See **Exhibit 2, Attachment 3** – SAMPLE CIS Controls IG 1 Assessment and Plan and **Exhibit 2, Attachment 1** – SAMPLE CSAT Assessment Report.
4	Ensure that local entity has an effective basic cyber incident response plan. A sample incident response plan is included as part of this RFP	Vendor will use sample attachment or equivalent format/template. (See **Exhibit 2, Attachment 2** – SAMPLE Cyber Incident Response Plan).
5	Monthly one-hour telephone/online or in-person consultation to provide ongoing coaching and consulting regarding understanding of and implementation of cybersecurity improvements.	Teleconference tools by mutual agreement of vendor and Contracting Entity.
6	End of year assessment update using CSAT which identifies progress made towards improving priority items identified in initial assessment and items remaining to be addressed.	Provide updated versions of reports provided in items 1, 2, and 3 noting improvements made in the preceding 12 months.

Exhibit 1 - Request for Cyber Assessment Service Request for Quote (RFQ)
The Request for Quote (RFQ) form will be used by the local public entity to request services from one or more qualitied contractor(s). Contractors who receive this RFQ will required to respond to the RFQ. The State Program Manager may approve updates to the RFQ template at any point and will provide this updated RFQ template to MiDEAL members and contractors. The latest RFQ template will be available on www.michigan.gov/cyberpartners.

Exhibit 2 - Document Samples/Attachments
The following sample documents have been provided for reference. The idea is for the Contractor to use these as-is, as starting points, or improve for use. The State will use feedback on these templates to make future improvements in and will republish best practice templates periodically on www.michigan.gov/cyberpartners. The intent of providing these samples is to create common formats and common language around cybersecurity controls to further promote partnerships and collaboration between local public entities.

- Center for Internet Security Controls Self-Assessment Tool
  Free online platform that organizations can use to conduct, track and assess their implementation of the CIS Controls.
- **Attachment 1 - SAMPLE CSAT Assessment Report**
  Sample Microsoft Word format report and annual plan to a local public entity that highlights current state of implementation of applicable CIS Controls and recommended next steps.
- **Attachment 2 – SAMPLE Cyber Incident Response Plan**
  Sample Microsoft Word format cyber incident response plan that can be modified for use by a local public entity.
- **Attachment 3 - SAMPLE CIS Controls IG 1 Assessment and Plan**
  Sample Microsoft Excel spreadsheet with CIS Controls with modifications to allow capture of Controls in Place, Controls Recommended/Planned, and Notes. Intended as a note-taking companion to the CSAT.

B. Optional Service Offerings (Priced separately in Schedule B)

These additional services are available through the Contract.

	Optional Deliverables
1	General Advisory Services on a time and materials basis.
2	Assessment and planning for CIS Controls/Sub Controls in Implementation Groups 2 and 3.
3	Assistance with audits or compliance requirements that are present at the local entity based on business practices. (CJIS, PCI, HIPAA, IRS-1075, FERPA, etc…)
4	Conduct Penetration Test
5	Conduct Infrastructure Vulnerability Scan
6	Conduct Security Tool Evaluation
7	Conduct Security Tool Assessment and Rationalization
8	Conduct Physical Security Assessment
9	Implement a Security information and event management (SIEM) Platform
10	Implement a Vulnerability Scanning Platform
11	Implement a Data Loss Prevention (DLP) Platform
12	Implement an Endpoint Detection & Response (EDR) Platform
13	Implement Intrusion Protection (IDS/IPS) Solution
14	Implement Web Content Filtering
15	Implement Next Generation Firewall(s)

C. Service Area – Districts

The Contractor must be able to provide On-Site Security in Michigan. Indicate regions you will serve in the table below. See attached map of regions. https://www.michigan.gov/msp/0,4643,7-123-1878_63868_63877---,00.html

All work must be performed within the USA and the State prefers that remote work be performed in Michigan

	District 1	District 2	District 3	District 4	District 5	District 6	District 7	District 8
Onsite Offered	X	X	X	X	X	X	X	X
Remote Offered	X	X	X	X	X	X	X	X

D. Local Government Responsibilities

Prior to engaging in an assessment, each local entity will need to provide information to vendors and agree to make key staff available to participate in the Cybersecurity assessment Workshop. Local public entity will use the Request for Cybersecurity Assessment form. See (**Exhibit 1**- Request for Cyber Assessment Service RFQ)

1. RESERVED

2. Services Levels

2.1. Request for Quote Response Time

The Contractor must be able to respond to a Request for Quote (RFQ) within 14 calendar days.

2.2. Resource Deployment Time Frame

The Contractor must deploy resources after award recommendation by the Contracting Entity within 30 calendar days of order date.

3. Acceptance

3.1. Acceptance Criteria
See Section 16, Acceptance, of the Standard Contract Terms.

4. Staffing
4.1. Contractor Representative
The Contract shall appoint a representative (may be one of the two positions listed identified in Section 4.3 below) who will be responsible for responding to State inquiries regarding the Contract Activities, answering questions related to ordering and delivery, etc. (the "Contractor Representative").

The Contractor must notify the Contract Administrator at least 30 calendar days before removing or assigning a new Contractor Representative.

4.2. Work Hours
The Contractor must provide Contract Activities during the normal working hours of the Contracting Entity. These are anticipated to occur Monday – Friday, 7:00 a.m. to 6:00 p.m. EST, with some variation by each location.

4.3. Key Personnel
The Contractor must appoint the following individuals who will be directly responsible for the day-to-day operations of the Contract ("Key Personnel"). The key resources will be assigned for each Contracting Entity who submits a Request for Quote (RFQ).

The following staffing is identified as Key Personnel:

Dewpoint Inc.	Name
1. Account Executive / Engagement Manger	Mike Coyne
2. Cyber Security Expert	Don Cornish Scott Adema

The Account Executive / Engagement Manager must be specifically assigned to the State account, be knowledgeable on the contractual requirements, and respond to State inquires within 2 business days.

The Contractor must identify and introduce Key Personnel to the Contracting Entity, describe the functions they will perform, and provide current chronological resumes.

The Contracting Entity has the right to recommend and approve in writing the initial assignment, as well as any proposed reassignment or replacement, of any Key Personnel. Before assigning an individual to any Key Personnel position, Contractor will notify the Contracting Entity of the proposed assignment, introduce the individual to the Contracting Entity's Point of Contact, and provide the Contracting Entity with a resume and any other information about the individual reasonably requested by the Contracting Entity. The Contracting Entity reserves the right to interview the individual before granting written approval. In the event the Contracting Entity finds a proposed individual unacceptable, the Contracting Entity will provide a written explanation including reasonable detail outlining the reasons for the rejection.

Contractor will not remove any Key Personnel from their assigned roles on this Contract without the prior written consent of the Contracting Entity. The Contractor's removal of Key Personnel without the prior written consent of the State is an unauthorized removal ("Unauthorized Removal"). An Unauthorized Removal does not include replacing Key Personnel for reasons beyond the reasonable control of Contractor, including illness, disability, leave of absence, personal emergency circumstances, resignation, or for cause termination of the Key Personnel's employment. Any Unauthorized Removal may be considered by the State to be a material breach of this Contract, in respect of which the State may elect to terminate this Contract for cause under Termination for Cause in the Standard Terms.

4.4. Disclosure of Subcontractors
The Contractor shall notify and obtain approval from the Program Manager prior to utilizing a subcontractor.

4.5. Security
The Contractor will be subject security procedures that will vary by location and be identified by the contracting local public entity. This may include the following:

- Background checks (See Section 12 of Contract Terms) for individuals working on site or with access to sensitive information.
- Other, to be determined by local public entity

5. Project Management

5.1. Project Plan
Within five business day of the award of any SOW, the Contractor must submit, for final approval, a detailed project plan to the Contracting Entity.

The final Project Plan must be in agreement with the Contractor's SOW proposal and accepted by the Local Public Entity. Detailed requirements will include steps required to plan and conduct onsite assessment, deliver draft and final assessment reports and plan and schedule monthly check in meetings; and individuals responsible for receiving/reacting to the requested information, including names and titles of personnel assigned to the project, both from the Vendor and Local Public Entity.

5.2. Meetings
As part of this agreement, there will be monthly scheduled meetings between the Contractor and the Contracting Entity. The Contracting entity may request other meetings as needed to manage the contract or schedule. The Contractor will meet with the State Program Manager as required to coordinate the state-wide the Independent Cyber Assessment Program.

5.3. Reporting

I. Within 30 calendar days of the Engagement commencement date, with the local public entity, the Contractor shall provide the State Program Manager with the following information:

   a. Contracting Local Public Entity Name
   b. Contact Name for Local Public Entity
   c. Contact E-mail for Local Public Entity
   d. Optional Services Selected by Contracting Entity
   e. Start Date of engagement

II. Additional reporting requirements may be identified in the future Request for Quote.

6. Pricing

6.1. Price Term
Pricing is firm for the entire length of the Contract. Contractor pricing, for any SOW, must not exceed rates provided in **Schedule B**. Contractor's out-of-pocket expenses are not separately reimbursable unless, on a case-by-case basis for unusual expenses, the Contracting Entity has agreed in advance and in writing to reimburse Contractor for the expense at the State's current travel reimbursement rates. See http://www.michigan.gov/dtmb/0,5552,7-150- 9141_13132---,00.html for current rates.

7. Ordering
7.1. Authorizing Document
The appropriate authorizing document for the Contract will be the Purchase Order from the Contracting Entity.

8. Invoice and Payment
8.1. Invoice Requirements
All invoices submitted to the Contracting Entity must include: (a) date; (b) purchase order; (c) quantity; (d) description of the Contract Activities; (e) unit price and (f) total price. Overtime and holiday pay will not be paid.

8.2. Payment Methods
Payment methods will vary by Contracting Entity.

8.3. Procedure
Final pricing will be submitted per the SOW/RFP requirements.

STATE OF MICHIGAN

Contract No. 210000000301

Independent Cyber Assessment for Local Entities in Michigan

SCHEDULE B
PRICING

Prices include all costs, including but not limited to, any one-time or set-up charges, fees, and potential costs that Contractor may charge the Local Public Entity.

The Contractor has provided not to exceed pricing and an estimate of hours for delivering the Core Service Offerings.

Core Service Offerings	***Estimated Hours**	**Small Entity** *Less than 50 End Points*	**Medium Entity** *50-500 End Points*	**Large Entity** *500-1500 End Points*	**X-Large Entity** *1500+ End Points*	**Includes Travel Yes/No****
a. Cybersecurity Assessment Workshop using CIS Controls and CSAT Tool	S: 21 M: 39 L: 70 XL:103	Fixed Price $ 11,060.49	Fixed Price $ 19,030.56	Range: Low End – High End $ 19030.56- $ 29,896.87	Range: Low End – High End $ 29,896.87- $ 39,968.68	No
b. Assessment Report & Recommendations	S: 21 M: 45 L: 70 XL:95					
c. Cybersecurity Improvements Plan	S: 7 M: 11 L: 17 XL:25					
d. Baseline Incident Response Plan	S: 9 M: 15 L: 29 XL:29					
e. 12 Monthly Advisory Sessions (1 hour)	S: 21 M: 24 L: 24 XL:24					
f. End of Year Assessment	S: 6.5 M: 12.5 L: 19 XL:30					

* Estimated hours, provided for fixed price activities are for estimation purposes only.

Definition of Endpoints for Core Services:
Pricing tiers by endpoint shall be determined exclusively based on the number of end user computers (desktops/ laptops).

Centrally-managed student devices in a school/university environment such Chromebooks and iPads count as a single device managed by a single device management platform to determine pricing tier for Core Services.

An example of the way we count those devises as “end points” would be: if a school environment has forty (40) end points (end points as defined by this RFP clarification) and two-hundred (200) student devices (i.e. Chromebooks/iPads), the two-hundred (200) student devices will be treated as one (1) endpoint giving the entity forty-one (41) end points and thus keeping the entity in the “Small Entity” pricing tier

Optional Services Offering	**Service Available?** (Y/N)	***Estimated Hours**	**Small Entity** *Less than 50 End Points*	**Medium Entity** *50-500 End Points*	**Large Entity** *500-1500 End Points*	**X-Large Entity** *1500+ End Points*	**Includes Travel Yes/No****
a. General Advisory Services on a time and materials basis.	Yes	See rate table below	N/A	N/A	N/A	N/A	No
b. Assessment and planning for CIS Controls/Sub Controls in Implementation Groups 2 and 3.	Yes	See rate table below	N/A	N/A	N/A	N/A	No
c. Assistance with audits or compliance requirements that are present at the local entity based on business practices. (CJIS, PCI, HIPAA, IRS-1075, FERPA, etc…)	Yes	See rate table below	N/A	N/A	N/A	N/A	No
d. Conduct Penetration Test	Yes	S: M: L: XL:	Low End – High End $ _____	Low End – High End $ _____	Low End – High End $ _____- $ _____	Low End – High End $ _____- $ _____	No
e. Conduct Infrastructure Vulnerability Scan	Yes	S: M: L: XL:	Low End – High End $ _____	Low End – High End $ _____	Low End – High End $ _____- $ _____	Low End – High End $ _____- $ _____	No
f. Conduct Security Tool Evaluation	Yes	S: M: L: XL:	Low End – High End $ _____	Low End – High End $ _____	Low End – High End $ _____- $ _____	Low End – High End $ _____- $ _____	No
g. Conduct Security Tool Assessment and Rationalization	Yes	S: M: L: XL:	Low End – High End $ _____	Low End – High End $ _____	Low End – High End $ _____- $ _____	Low End – High End $ _____- $ _____	No
h. Conduct Physical Security Assessment	Yes	S: M: L: XL:	Low End – High End $ _____	Low End – High End $ _____	Low End – High End $ _____- $ _____	Low End – High End $ _____- $ _____	No
i. Implement a SIEM Platform	Yes	S: M: L: XL:	Low End – High End $ _____	Low End – High End $ _____	Low End – High End $ _____- $ _____	Low End – High End $ _____- $ _____	No

Optional Services Offering	**Service Available?** (Y/N)	***Estimated Hours**	**Small Entity** *Less than 50 End Points*	**Medium Entity** *50-500 End Points*	**Large Entity** *500-1500 End Points*	**X-Large Entity** *1500+ End Points*	**Includes Travel Yes/No****
j. Implement a Vulnerability Scanning Platform	Yes	S: M: L: XL:	Low End – High End $ _____	Low End – High End $ _____	Low End – High End $ _____- $ _____	Low End – High End $ _____- $ _____	No
k. Implement a DLP Platform	Yes	S: M: L: XL:	Low End – High End $ _____	Low End – High End $ _____	Low End – High End $ _____- $ _____	Low End – High End $ _____- $ _____	No
l. Implement an Endpoint Detection & Response (EDR) Platform	Yes	S: M: L: XL:	Low End – High End $ _____	Low End – High End $ _____	Low End – High End $ _____- $ _____	Low End – High End $ _____- $ _____	No
m. Implement Intrusion Protection (IDS/IPS) Solution	Yes	S: M: L: XL:	Low End – High End $ _____	Low End – High End $ _____	Low End – High End $ _____- $ _____	Low End – High End $ _____- $ _____	No
n. Implement Web Content Filtering	Yes	S: M: L: XL:	Low End – High End $ _____	Low End – High End $ _____	Low End – High End $ _____- $ _____	Low End – High End $ _____- $ _____	No
o. Implement Next Gen Firewall(s)	Yes	S: M: L: XL:	Low End – High End $ _____	Low End – High End $ _____	Low End – High End $ _____- $ _____	Low End – High End $ _____- $ _____	No

* Estimated hours, provided for fixed price activities are for estimation purposes only.

Optional Services Rates (Labor/Hour)	**Hourly Rate**
1. Executive Level Security Consulting	$200
2. Security Technical Architect	$168.35
3. Security Specialist	$127.40
4. Sr Program Manager	$118.30
5. Sr Business/Technical Analyst	$104.65
Note – Rates are not to exceed and do not include cost of travel outside of the greater Lansing area.	

****Travel Description (Time and Expenses)**
Travel is not included in the rates listed. Dewpoint will not charge for travel within the greater Lansing area. If work is quoted to locations outside of the greater Lansing area, Dewpoint will invoice for travel at cost to the entity receiving our services and ensure that we follow the State of Michigan or local entity not to exceed travel guidelines. Whichever are appropriate.

DEWPOINT SOLUTION ASSUMPTIONS

- All pricing provided is "not to exceed".
- CSAT registration will require a Contracting Entity's email address with valid domain name.
- Dewpoint will deliver these services with a combination of onsite and off-site resources.
- Any changes in scope will be agreed upon by Dewpoint and Contracting Entity. A signed change notice will accompany any changes. Changes to the scope may impact the price and/or duration of the project.
- The project will not start until a purchase order is received by Dewpoint.
- The consultants assigned by Dewpoint to perform the services for the Contracting Entity are not to be solicited for permanent employment.

STATE OF MICHIGAN

Contract No. 210000000301
Independent Cyber Assessment for Local Entities in Michigan

EXHIBIT 1
Cyber Assessment Service Request for Quote (RFQ)

Request for Cyber Assessment Service

Local Public Entity shall use this format to request a quote cybersecurity assessment and planning services from pre-qualified vendors using contract ####.

Provide this information to pre-qualified vendors of your choice so that they may provide you with an accurate proposal. It is sufficient for the Local Public Entity cut and paste this format into an email and send it to the contact(s) identified by the vendor.

Overview of Local Entity

- Name of Entity:
- Type of Entity:
- Population:
- Location of Offices:
- Number of Staff (overall):
- Number of IT staff:
- Number of Computers:
- Number of Physical Servers:
- Number of Virtual Servers:
- Other Devices (specify):
- Cloud-based services in use:
- Size of local IT staff:
- Name and title of main point of contact for this engagement:
  - Main point of contact is responsible for coordinating access to all resources and individuals at the local public entity required to support this engagement.

Services Requested

✓ Core Service Offerings
- Cybersecurity Assessment Workshop using CIS Controls and CSAT Tool
- Assessment Report & Recommendations
- Cybersecurity Improvements Plan
- Baseline Incident Response Plan
- 12 Monthly Advisory Sessions (1 hour)

Optional Service Offerings

Check all that you would like quoted:

- ☐ General Advisory Services
- ☐ Conduct Penetration Test
- ☐ Conduct Infrastructure Vulnerability Scan
- ☐ Conduct Security Tool Evaluation
- ☐ Conduct Security Tool Assessment and Rationalization
- ☐ Conduct Physical Security Assessment
- ☐ Implement a SIEM Platform
- ☐ Implement a Vulnerability Scanning Platform
- ☐ Implement a DLP Platform
- ☐ Implement an Endpoint Detection & Response (EDR) Platform
- ☐ Implement Intrusion Protection (IDS/IPS) Solution
- ☐ Implement Web Content Filtering
- ☐ Implement Next Gen Firewall(s)

List Additional Optional Services provide in Vendor Contract (if available)

- ☐ _____

Vendor Response

At a minimum, the Contractor shall include the following in their proposal:

1. Pricing (must not exceed the rates in State of Michigan Contract ####
2. Identify Proposed Staffing (Qualifications shall match or exceed those in State of Michigan Contract ####.

STATE OF MICHIGAN

Contract No. 210000000301

Independent Cyber Assessment for Local Entities in Michigan

EXHIBIT 2
Document Samples/Attachments

The Attachments provided in Exhibit 2 are Samples that can be used in carrying out the activities of this contract. The Contractor shall use these sample documents, an equivalent/improved version of their own creation, or an updated version published by the State at a future date on www.michigan.gov/cyberpartners.

Attachment 1
Sample CSAT Assessment Report

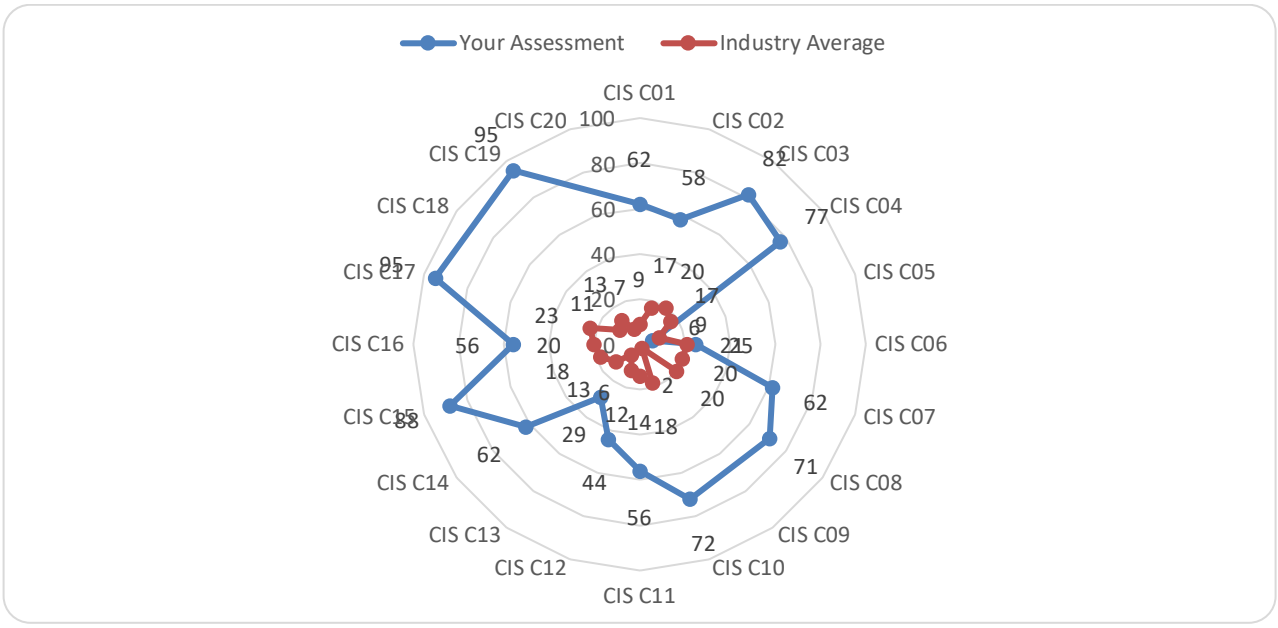
NOTE: The Attachments provided in Exhibit 2 are Samples that can be used in carrying out the activities of this contract. The Contractor shall use these sample documents, an equivalent/improved version of their own creation, or an updated version published by the State at a future date on www.michigan.gov/cyberpartners.

Executive Summary

On [date] [assessor/names] performed an onsite survey of [local entity name] cyber security posture using the Critical Controls from the Center for Internet Security (CIS). Team members used the Controls Self-Assessment Tool (CSAT), an online assessment that catalogs maturity based on the 20 Critical Controls. The CIS Critical Security Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. A principal benefit of the Controls is that they prioritize and focus a smaller number of actions with high pay-off results*. The team focused only on Implementation Group (IG) 1, this survey was conducted using the sub controls identified in Implementation Group 1, which covers the most important “cyber hygiene” activities. We recommend a follow up to examine maturity on Implementation Groups 2 and 3.

The purpose of this survey was twofold: 1) provide a snapshot of [entity name] cyber assessment posture; and 2) develop an annual plan for cybersecurity improvements.

Based on the survey results for CIS Controls, Implementation Group 1, [entity name] is [adjectives of comparison to] benchmarks in the CSAT database in most control areas. (see Figure 1) and has a few priority items to tackle in order to improve their cyber security posture.


Your Assessment
Industry Average
CIS C01
CIS C02
CIS C03
CIS C04
CIS C05
CIS C06
CIS C07
CIS C08
CIS C09
CIS C10
CIS C11
CIS C12
CIS C13
CIS C14
CIS C15
CIS C16
CIS C17
CIS C18
CIS C19
CIS C20

Survey Results

Each control area has an at-a-glance color code to indicate maturity. The basic color code: green = good | red = needs improvement

Note: summary is based on consideration of the 43 sub controls in Implementation Group 1. For a complete picture, additional follow up on Implementation Groups 2 and 3 is recommended.

Findings and Action Plan

Priority areas of potential improvement were noted:

- CC [control.subcontrol] **[control name]** *[Control description for CIS Controls].*
  - Report: [Describe controls in place, status of controls].
  - Recommendation: [Describe recommendations for improvement in this area.]

- CC [control.subcontrol] **[control name]** *[Control description for CIS Controls].*
  - Report: [Describe controls in place, status of controls].
  - Recommendation: [Describe recommendations for improvement in this area.]

- CC [control.subcontrol] **[control name]** *[Control description for CIS Controls].*
  - Report: [Describe controls in place, status of controls].
  - Recommendation: [Describe recommendations for improvement in this area.]

- CC [control.subcontrol] **[control name]** *[Control description for CIS Controls].*
  - Report: [Describe controls in place, status of controls].
  - Recommendation: [Describe recommendations for improvement in this area.]

Complete Survey Results

Control	Question	Question Title	Policy Defined	Control Implemented	Control Automated	Control Reported
CIS C01	1.4	Maintain Detailed Asset Inventory	Informal Policy	Implemented on All Systems	Automated on Most Systems	Reported on Most Systems
CIS C01	1.6	Address Unauthorized Assets	Informal Policy	Implemented on Most Systems	Automated on Some Systems	Reported on Most Systems
CIS C02	2.1	Maintain Inventory of Authorized Software	Approved Written Policy	Implemented on All Systems	Automated on All Systems	Reported on Most Systems
CIS C02	2.2	Ensure Software is Supported by Vendor	Informal Policy	Implemented on Some Systems	Automated on Most Systems	Reported on Some Systems
CIS C02	2.6	Address Unapproved Software	Informal Policy	Implemented on Some Systems	Automated on Some Systems	Not Reported
CIS C03	3.4	Deploy Automated Operating System Patch Management Tools	Approved Written Policy	Implemented on All Systems	Automated on All Systems	Reported on Most Systems
CIS C03	3.5	Deploy Automated Software Patch Management Tools	Approved Written Policy	Implemented on Most Systems	Automated on Most Systems	Parts of Policy Reported
CIS C04	4.2	Change Default Passwords	Approved Written Policy	Implemented on Most Systems	Automated on Most Systems	Not Reported
CIS C04	4.3	Ensure the Use of Dedicated Administrative Accounts	Written Policy	Implemented on All Systems	Automated on All Systems	Not Applicable
CIS C05	5.1	Establish Secure Configurations	Informal Policy	Not Implemented	Not Automated	Not Reported
CIS C06	6.2	Activate Audit Logging	No Policy	Implemented on Some Systems	Automated on Some Systems	Not Reported
CIS C07	7.1	Ensure Use of Only Fully Supported Browsers and Email Clients	No Policy	Implemented on Most Systems	Automated on Most Systems	Reported on Most Systems
CIS C07	7.7	Use of DNS Filtering Services	Partially Written Policy	Implemented on Most Systems	Automated on Most Systems	Reported on Most Systems
CIS C08	8.2	Ensure Anti-Malware Software and Signatures are Updated	Informal Policy	Implemented on All Systems	Automated on Most Systems	Reported on All Systems
CIS C08	8.4	Configure Anti-Malware Scanning of Removable Devices	Informal Policy	Implemented on All Systems	Automated on All Systems	Reported on All Systems
CIS C08	8.5	Configure Devices to Not Auto-Run Content	Informal Policy	Implemented on Most Systems	Automated on Most Systems	Not Applicable
CIS C09	9.4	Apply Host-Based Firewalls or Port Filtering	No Policy	Not Implemented	Not Automated	Not Reported
CIS C10	10.1	Ensure Regular Automated Backups	Informal Policy	Implemented on Most Systems	Automated on Most Systems	Reported on All Systems
CIS C10	10.2	Perform Complete System Backups	Approved Written Policy	Implemented on All Systems	Automated on All Systems	Reported on All Systems
CIS C10	10.4	Protect Backups	Written Policy	Implemented on All Systems	Automated on All Systems	Reported on All Systems
CIS C10	10.5	Ensure Backups Have At least One Non-Continuously Addressable Destination	Informal Policy	Parts of Policy Implemented	Automated on Some Systems	Not Reported
CIS C11	11.4	Install the Latest Stable Version of Any Security-Related Updates on All Network Devices	Informal Policy	Implemented on All Systems	Not Automated	Reported on All Systems
CIS C12	12.1	Maintain an Inventory of Network Boundaries	Informal Policy	Implemented on Some Systems	Automated on Some Systems	Reported on Some Systems
CIS C12	12.4	Deny Communication Over Unauthorized Ports	Informal Policy	Implemented on Some Systems	Automated on Some Systems	Reported on Some Systems
CIS C13	13.1	Maintain an Inventory of Sensitive Information	Informal Policy	Implemented on Some Systems	Automated on Some Systems	Not Reported
CIS C13	13.2	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	Informal Policy	Implemented on Some Systems	Automated on Some Systems	Not Reported
CIS C13	13.6	Encrypt the Hard Drive of All Mobile Devices	Informal Policy	Implemented on Most Systems	Not Automated	Not Reported
CIS C14	14.6	Protect Information through Access Control Lists	Informal Policy	Implemented on Most Systems	Automated on Most Systems	Reported on Most Systems
CIS C15	15.7	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data	Approved Written Policy	Implemented on All Systems	Automated on All Systems	Not Applicable
CIS C15	15.10	Create Separate Wireless Network for Personal and Untrusted Devices	Informal Policy	Implemented on All Systems	Automated on All Systems	Not Applicable
CIS C16	16.8	Disable Any Unassociated Accounts	Informal Policy	Implemented on Most Systems	Not Automated	Reported on Most Systems
CIS C16	16.9	Disable Dormant Accounts	No Policy	Implemented on Some Systems	Not Automated	Reported on Some Systems
CIS C16	16.11	Lock Workstation Sessions After Inactivity	Approved Written Policy	Implemented on All Systems	Automated on All Systems	Not Applicable
CIS C17	17.3	Implement a Security Awareness Program	Written Policy	Implemented on All Systems	Automated on All Systems	Reported on Some Systems
CIS C17	17.5	Train Workforce on Secure Authentication	Approved Written Policy	Implemented on All Systems	Automated on All Systems	Not Applicable
CIS C17	17.6	Train Workforce on Identifying Social Engineering Attacks	Written Policy	Implemented on All Systems	Automated on Most Systems	Reported on All Systems
CIS C17	17.7	Train Workforce on Sensitive Data Handling	Approved Written Policy	Implemented on All Systems	Automated on All Systems	Not Applicable
CIS C17	17.8	Train Workforce on Causes of Unintentional Data Exposure	Approved Written Policy	Implemented on All Systems	Automated on All Systems	Not Applicable
CIS C17	17.9	Train Workforce Members on Identifying and Reporting Incidents	Approved Written Policy	Implemented on All Systems	Automated on All Systems	Not Applicable
CIS C19	19.1	Document Incident Response Procedures	Approved Written Policy	Implemented on Most Systems	Not Applicable	Not Applicable
CIS C19	19.3	Designate Management Personnel to Support Incident Handling	Approved Written Policy	Implemented on All Systems	Automated on All Systems	Not Applicable
CIS C19	19.5	Maintain Contact Information For Reporting Security Incidents	Approved Written Policy	Implemented on All Systems	Not Applicable	Not Applicable
CIS C19	19.6	Publish Information Regarding Reporting Computer Anomalies and Incidents	Approved Written Policy	Implemented on All Systems	Automated on Most Systems	Not Applicable

CIS Controls

https://www.cisecurity.org/controls/

Basic CIS Controls

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational CIS Controls

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational CIS Controls

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Attachment 2
Sample Cyber Incident Response Plan

NOTE: The Attachments provided in Exhibit 2 are Samples that can be used in carrying out the activities of this contract. The Contractor shall use these sample documents, an equivalent/improved version of their own creation, or an updated version published by the State at a future date on www.michigan.gov/cyberpartners.

Please Note: the sample RFP attachment isn't confidential
The plan that is created by a local entity using the sample will be confidential

Cyber Incident Response Plan

DATE

Version 1.0

NOTE: The following Incident Response Plan is intended to provide an example of how a policy and plan can be written. It is not intended to cover all possible situations. Each agency must evaluate their unique circumstances and incorporate those into their plan. The plan is not intended to be a "fill in the blank" plan. If an agency chooses to simply fill in the blanks, the plan may not be sufficient to cover the agency's unique requirements during a security incident and could potentially cause the agency additional harm.

This document was created from existing cyber response plans that were in use at several Michigan counties. Names were removed and replaced with *Our Organization*.

Please share your plan and experiences with colleagues to help improve these tools.

Use this with the accompanying Incident Response Planning Companion to Sample IR Plan PowerPoint presentation to guide your organization's development of a cyber response plan.

Table of Contents

SUMMARY

The elements of a traditional Information Security effort continue to be important and useful. Two trends necessitate the establishment of a Cyber Incident Response Plan:

1) Information Technology is widespread throughout *Our Organization*; *Our Organization* relies heavily on Information Technology and cannot afford denial of service.

2) *Our Organization* IT systems and networks are at much higher risk to threats such as computer viruses, intrusions, and exposures.

The following examples of cyber security incidents are now commonplace:

- A ransomware attack renders a municipality's systems inoperable until systems can be restored from backups (if available) or ransom is paid.
- A computer virus is copied to a LAN server; within minutes hundreds of other computers are infected; recovery takes several people and several days.
- Backups infected with viruses result in re-infected systems, requiring more time and expense.
- Vulnerabilities in software are discovered that permit unauthorized entry; explicit instructions on how to exploit the vulnerability become quickly known.
- System intruders copy password files and distribute them throughout large networks.
- Break-ins through international networks require cooperation of different government agencies.
- Outbreaks of viruses or system penetrations appear in the press, causing embarrassment and possible loss of public confidence.

These situations can cause *Our Organization* to face unnecessary expense in productivity, significant damage to systems, and damage to our reputation. Clearly, the need now exists to take action prior to suffering the consequences of a serious IT security problem.

Our Organization CYBER INCIDENT RESPONSE PLAN

1.0 Introduction

1.1 Purpose of the Cyber Incident Response Plan

A Cyber Incident Response Plan is required in order to bring needed resources together in an organized manner to deal with an adverse event related to the safety and security of *Our Organization* Information System Resources. This adverse event may be malicious code attack, unauthorized access to *Our Organization* systems, unauthorized use of *Our Organization* services, denial of service attacks, general misuse of systems, and accidental loss or hoaxes.

1.2 General Purpose of the Cyber Incident Response Team

The purpose of *Our Organization*'s Cyber Incident Response Team is to:

- Protect *Our Organization*'s Information assets
- Provide a central organization to handle incidents
- Comply with requirements
- Prevent the use of *Our Organization*'s systems in attacks against other systems (which could cause us to incur legal liability)
- Minimize the potential for negative exposure.

1.3 Operational Objectives of the Cyber Incident Response Team

The objectives of *Our Organization*'s Cyber Incident Response Team are to:

- Limit immediate incident impact to customers and partners
- Recover from the incident
- Determine how the incident occurred
- Find out how to avoid further exploitation of the same vulnerability
- Avoid escalation and further incidents
- Assess the impact and damage in terms of financial impact, loss of image etc.
- Update policies and procedures as needed
- Determine who initiated the incident
- Document al information, events, and efforts to provide to law enforcement.

2.0 Incidents

2.1 Incident Categories

An incident will be categorized as one of four severity levels. These severity levels are based on the impact to *Our Organization* and can be expressed in terms of financial impact, impact to services and/or performance of our mission functions, impact to *Our Organization*'s image or impact to trust by *Our Organization*'s customers, etc. Table 1 provides a listing of the severity levels and a definition/description of each severity level.

Severity Level	Description
0 (Low)	Incident where the impact is minimal. Examples are e-mail SPAM, isolated Virus infections, etc.
1 (Medium)	Incident where the impact is significant. Examples are a delayed ability to provide services, meet *Our Organization*'s mission, delayed delivery of critical electronic mail or data transfers, etc.
2 (High)	Incident where the impact is severe. Examples are a disruption to the services, and/or performance of our mission functions. *Our Organization* proprietary of confidential information has been compromised, a virus or worm has become wide spread, and is affecting over 1% of employees, Pubic Safety systems are unavailable or *Our Organization* Executive management has been notified.
3 (Extreme)	Incident where the impact is catastrophic. Examples are a shutdown of all *Our Organization* network services. *Our Organization* proprietary or confidential information has been compromised and published on a public site. Public safety systems are unavailable. Executive management must make a public statement.

Table 1: Severity Levels

3.0 Responding to an incident

There are generally six stages of response:

1. Preparation—one of the most important facilities to a response plan is to know how to use it once it is in place. Knowing how to respond to an incident BEFORE it occurs can save valuable time and effort in the long run.

2. Identification—identify whether or not an incident has occurred. If one has occurred, the response team can take the appropriate actions.

3. Containment—involves limiting the scope and magnitude of an incident. Because so many incidents observed currently involve malicious code, incidents can spread rapidly. This can cause massive destruction and loss of information. As soon as an incident is recognized, immediately begin working on containment.

4. Eradication—removing the cause of the incident can be a difficult process. It can involve virus removal, conviction of perpetrators, or dismissing employees.

5. Recovery—restoring a system to its normal business status is essential. Once a restore has been performed, it is also important to verify that the restore operation was successful and that the system is back to its normal condition.

6. Follow-up—some incidents require considerable time and effort. Often once the incident appears to be terminated there is little interest in devoting any more effort to the incident. Performing follow-up activity is, however,

one of the most critical activities in the response procedure. This follow-up can support any efforts to prosecute those who have broken the law. This includes changing any company policies that may need to be narrowed down or be changed altogether.

3.1 Organization

To adequately respond to an intrusion or incident, predetermined teams will participate depending on the incident characteristics. As the situation develops and the impact becomes more significant, the various teams will be called to contribute. Figure 1 depicts the Cyber Incident Response organization.

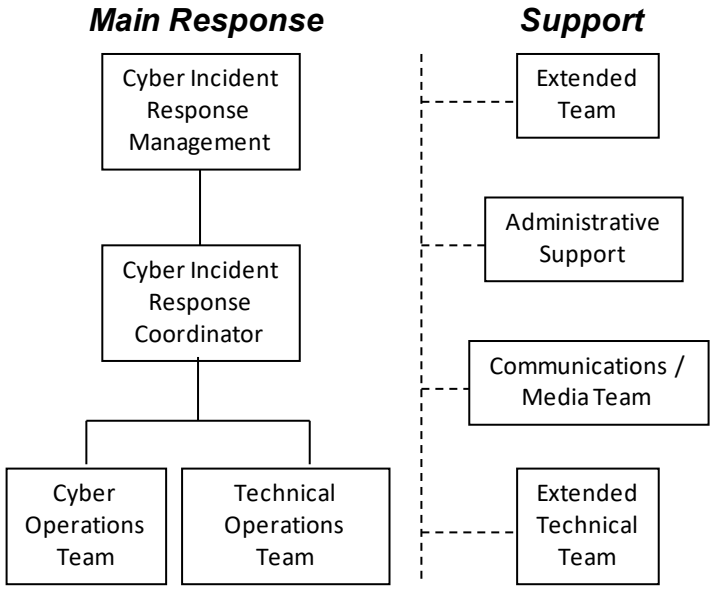


Figure 1: Cyber Incident Response Organization

Role	Responsibilities	Primary/Alternate(s)
Cyber Incident Response Management	Will have overall responsibility for directing activities in regard to the incident at Severity Level 2 and above. Will serve in advisory capacity for incidents at Severity Level 1.	
Cyber Incident Response Coordinator	Provides oversight to incident response. Requests resources as required to effectively contain and manage an incident response. Documents incident for purposes of law enforcement, lessons learned, and insurance.	
Cyber Operations Team / Technical Operations Team	Provide technical aspects of incident response.	
Communications / Media Team	Responsible for internal, external and media communications	
Extended Technical Team	Provides additional technical skill and capability to the Technical Operations team as required (ie. outside vendor or agency)	

Admin Support	Provides requested administrative support.	
Extended Team	Provide additional visibility and support to incident response as required. Provide specific HR, legal, finance, etc. skills as required.	

Table 2: Roles and Responsibilities

3.2 Escalation Levels

	Main Response			Support			
Severity Level	**Technical Ops Team, Cyber Ops Team**	**Cyber Incident Response Coordinator**	**Cyber Incident Response Mgmt**	**Comms / Media Team**	**Extended Technical Team**	**Admin Support**	**Extended Team**
0	X						
1	X	X	X				
2	X	X	X	X	X		
3	X	X	X	X	X	X	X

Table 3: Severity Level Matrix

The escalation process will be invoked to involve appropriate resources as the incident has more impact (severity level increases). Incidents should be handled at the lowest escalation level that is capable of responding to the incident with as few resources as possible in order to reduce the total impact, and to keep tight control. Table 4 defines the escalation levels with the associated team involvement.

Escalation Level	Affected Team(s)	Description
0	• Technical Operations Team • Cyber Operations Team	Normal Operations. Engineering and cyber groups monitoring for alerts from various sources.
1	• Technical Operations Team • Cyber Operations Team • Cyber Incident Response Coordinator • Cyber Incident Response Management	*Our Organization* has become aware of a potential or actual threat. Determine defensive action to take. Message employees of required actions if necessary.
2	• Cyber Incident Response Management • Cyber Incident Response Coordinator • Technical Operations Team • Cyber Operations Team • Extended Technical Team • Communications / Media Team	A threat has manifested itself. Determine course of action for containment and eradication. Message employees of required actions if necessary.
3	• Cyber Incident Response Management • Cyber Incident Response Coordinator • Extended Team • Technical Operations Team • Cyber Operations Team	Threat is wide spread or impact is significant. Determine course of action for containment, mitigation and eradication. Message employees. Prepare to take legal action. Prepare to make public statement.

	• Extended Technical Team • Communications / Media Team • Administrative Support Team	

Table 4: Escalation Levels

3.3 Escalation Considerations

Cyber Incident Response Management will consider several characteristics of the incident before escalating the response to a higher level. They are:

- How wide spread is the incident?
- What is the impact to business operations?
- How difficult is it to contain the incident?
- How fast is the incident propagating?
- What is the estimated financial impact to *Our Organization*?
- Will this affect *Our Organization*'s image negatively?

3.4 The Cyber Incident Response Process

The Cyber Incident Response Process is an escalation process where as the impact of the incident becomes more significant or wide spread, the escalation level increases bringing more resources to bear on the problem. At each escalation level, team members who will be needed at the next higher level of escalation are alerted to the incident so that they will be ready to respond if and when they are needed.

Appendix B depicts the overall process, while paragraph 3.5 outlines the roles and responsibilities of individual teams. Team membership is contained in Appendix A.

In cases where Criminal Justice Information (CJI) is involved, *Our Organization* will contact the MSP ISO and fill out and submit the CJIS 016 document if the incident significantly endangers the security or integrity of CJIS data. (reference CJIS Security Policy section 5.3 and the Michigan Addendum)

3.5 Cyber Incident Response Team Roles and Responsibilities

3.5.1 Escalation Level 0

<u>Technical Operations Team / Cyber Operations Team</u>

1. Monitors all known sources for alerts or notification of a threat.
2. Take appropriate defensive actions per known issues.
3. Escalate to Cyber Incident Coordinator if determined that Severity level may be greater than Level 0.

<u>Cyber Incident Coordinator</u>

1. Escalate Cyber Incident Response to Level 1 if information is received that the incident is likely greater than Level 0.

3.5.2 Escalation Level 1

Our Organization has become aware of a potential or actual threat.

i. Technical Operations Team / Cyber Operations Team

1. Determine initial defensive action required.
2. Notify the Cyber Incident Coordinator.
3. Determine appropriate course of action.

ii. Cyber Incident Coordinator

1. Receive and track all reported potential threats.
2. Start a chronological log of events.
3. Escalate Cyber Incident Response to Level 2 if a report is received indicating that the threat has manifested itself.
4. Determine relevant membership of the Technical Operations and Extended Technical teams.
5. Alert other IT personnel and applicable support organizations of the potential threat and any defensive action required.
6. Alert Cyber Incident Response Management of the potential threat. Seek advisory inputs as appropriate.
7. Alert Communications Team

iii. Cyber Incident Response Management

1. Provide advisory inputs as appropriate.

iv. Communications Team

1. If employee action required, message employees of required action.

3.5.3 Escalation Level 2

The threat has manifested itself.

i. Cyber Incident Coordinator

1. Notify Cyber Incident Response Management of the manifestation of the threat,
2. Receive status from the Technical Operations Team and report to Cyber Incident Response Management,
3. Start a chronological log of events.

Note: The chronological log will be used to support possible follow on legal action as determined by *Our Organization*'s General Counsel and Executive Directors.

ii. Technical Operations Team

1. Determine best course of action for immediate containment of the incident,
2. Notify the Technical Support Team of any action that is required,
3. Report actions taken and status to the Cyber Incident Response Coordinator.

Cyber Incident Response Management

1. Assume responsibility for directing activities in regard to the incident,
2. Coordinate discussion and analysis to determine best course of resolution,
3. Alert the Administrative Support Team of the incident,
4. Alert the Extended Team as applicable,
5. Determine whether Escalation Level 2 is appropriate or escalate to level 3,
6. Determine when the risk has been mitigated to an acceptable level.

Extended Technical Team

1. Take whatever action as determined by the Technical Operations Team
2. Report actions taken, number of personnel involved etc. to Incident Coordinator for the chronological log

Communications Team

1. Message *Our Organization* employee population informing them of the incident if deemed appropriate by Cyber Incident Response Management,
2. Message *Our Organization* employee population of any action they need to take as determined by the Technical Operations Team and directed by Cyber Incident Response Management.

3.5.4 Escalation Level 3

The threat has become widespread or has become a high severity level.

1. Cyber Incident Response Management
    1. Direct the response team to:

a. Set up communications channels between all teams.
b. Assume occupancy of the command center if exists.
c. Open a teleconference bridge for ongoing communications and team interaction or Initialize an incident voice mail box where status messages can be placed to keep *Our Organization* personnel statused

2. Organize scheduled team meetings. Define specific status update schedule.
3. Authorize initial communications to employees and executives. Use Smart Message system as desired.
4. Alert the Extended Team of the incident notifying them of the Severity Level.
5. Status Executive Management as appropriate.
6. Determine when the risk has been mitigated to an acceptable level.

2. Extended Team
    1. Contact local authorities if deemed appropriate,
    2. If local authorities are called in, make arrangements for them to be allowed into the building,
    3. Ensure that all needed information is being collected to support legal action or financial restitution.
3. Cyber Incident Response Coordinator
    1. Continue maintaining the Chronological Log of Event,
    2. Continue to manage incident response per direction of Cyber Incident Response Management.
4. Communication Team
    1. Message *Our Organization* population and external media as directed by Cyber Incident Response Management.

Technical Operations Team

1. Continue to monitor all known sources for alerts looking for further information or actions to take to eliminate the threat,
2. Continue reporting status to the Cyber Incident Response Coordinator for the chronological log of events,
3. Monitor effectiveness of actions taken and modify them as necessary,
4. Provide status to Cyber Incident Response Coordinator and Cyber Incident Response Management on effectiveness of actions taken and progress in eliminating the threat.

Extended Technical Team

1. Continue actions to eradicate the threat as directed by Cyber Incident

2. Response Coordinate and Cyber Incident Response Management and the Technical Operations team.
3. Continue to report actions taken, number of personnel etc. to the Cyber Incident Response Coordinator for the chronological log.

Administrative Support Team

1. Provide administrative support to all persons and teams involved in incident

3.6 Special Circumstances

5. Email Communications are compromised or otherwise unavailable
    1. There could be a cyber security incident that compromises the ability to communicate via email. In this case, the backup will be communications via desk phone or cell phone. A phone directory of key persons on the response teams is given in Appendix A.

6. Personal Identification Information / HIPAA or other Confidential Information is leaked via Internal Source
    1. The process defined above can also apply to the circumstance where information is leaked via an internal source by accident or maliciously. In this case, the steps in the response process would be very similar to the above process but would also include early determination of the type and quantity of data leaked, the source of the leak and the potential impact of the leak to the County or to the public at large.

4.0 Post incident

4.1 Cyber Incident Coordinator and Response Management

1. Report on:
    a) Estimate of damage/impact,
    b) Action taken during the incident (not technical detail),
    c) Follow on efforts needed to eliminate or mitigate the vulnerability,
    d) Policies or procedures that require updating,
    e) Efforts taken to minimize liabilities or negative exposure.
    f) Provide the chronological log and any system audit logs requested by the Extended Team,
    g) Document lessons learned and modify the Cyber Incident Response Plan accordingly.

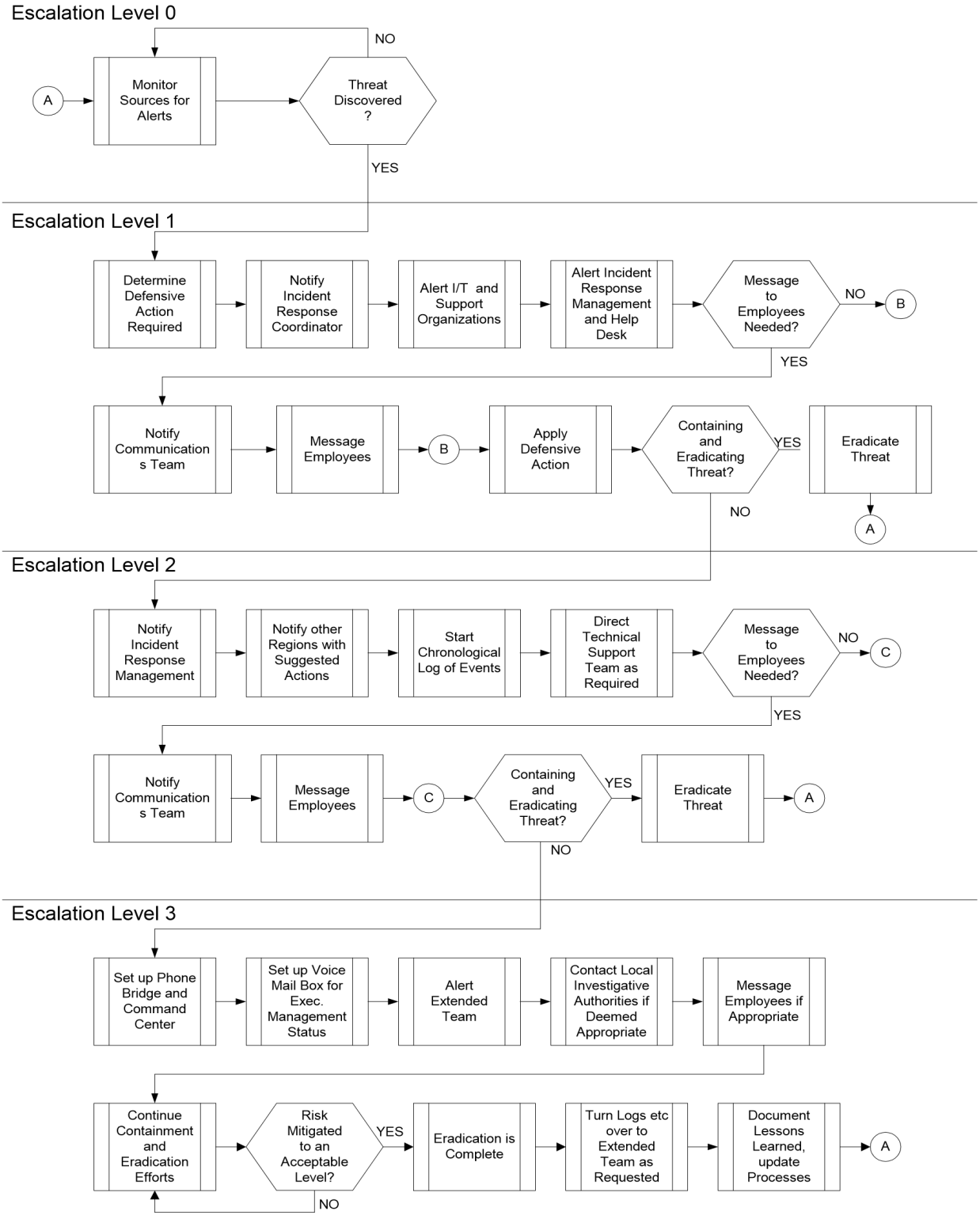
4.2 Extended Team

1. Legal and Finance work with the local authorities as appropriate in the case that the incident was from an external source,
2. HR and IT work with *Our Organization* management to determine disciplinary action in the case that the incident was from an internal source.
3. Homeland Security leveraged to support as necessary.

Appendix A. Cyber Incident Response Team

Team	Leadership / Members	Contact Information
Cyber Incident Response Management	CISO	
	Co-CISO	
Cyber Incident Response Coordinator	Security Operations	
Administrative Support Team	Administration	
	General	
Technical Operations Team	Infrastructure	
	Technical support	
	Applications	
Cyber Operations Team	Operations	
	Operations - Assigned technician	
Extended Technical Team	External Infrastructure and Applications personnel as needed	
Communications / Media Team	Communications	
Extended Team	Homeland Security	
	HHS (HIPAA)	
	Legal	
	HR	
	Finance	
	Sheriff	
	Treasurer	
	Clerk	
	Register of Deeds	
	Prosecutor	
Executive Management		

Appendix B: Incident Response Diagram and Examples



Threat Example 1: Server Software Vulnerability

Escalation Level 0

TECHNICAL OPERATIONS TEAM

1. A critical *zero-day* (discovered by its use in the wild) software vulnerability affects the operating system on a widely-used production server. The vulnerability allows for an unauthorized privilege escalation and therefore unauthorized data access. The threat is escalated to Level 1.

Escalation Level 1

TECHNICAL OPERATIONS TEAM

1. Determines that the defensive action required is a patch of the operating system from the vendor.

2. Notifies the Incident Coordinator of the vulnerability.

3. Determines that employee action is not required.

INCIDENT COORDINATOR

1. Receives and tracks the status of the vulnerability.

2. Does not escalate the threat to Level 2, since the vulnerability has not manifested itself.

3. Determines relevant membership of the Technical Operations and Extended Technical team.

4. Alerts IT organizations and applicable support organizations of the vulnerability. The action required to contain the threat is a patch of the operating system from the vendor. This patch must be applied and tested on a development server before being propagated to the production server.

5. Alerts Cyber Incident Response Management of the vulnerability.

6. Alerts the Communications Team.

COMMUNICATIONS TEAM

1. Since employee action is not required, no message to employees is necessary.

Post Incident

CYBER INCIDENT RESPONSE MANAGEMENT

1. Prepare a report for *Our Organization* Executive Management to include:

    a. Estimate of the impact of addressing the vulnerability and the potential cost of not doing so,

    b. Action taken during the vulnerability's assessment,

    c. Follow on efforts needed to eliminate or mitigate the vulnerability,

    d. Policies or procedures that may require updating (if applicable), and

    e. Efforts taken to minimize the liabilities of negative exposure of the vulnerability.

2. Provides the chronological log and any system audit logs requested by the Extended Team.

3. Documents any lessons learned and modifies the Cyber Incident Response Plan accordingly.

EXTENDED TEAM

1. Not needed, because there was no manifestation of the vulnerability.

Threat Example 2: Ongoing Phishing Attack on Employees

Escalation Level 0

TECHNICAL OPERATIONS TEAM

1. Emails have been circulating to *Our Organization* employees that link users to a fraudulent website designed specifically to gather user authentication credentials from *Our Organization* employees. The threat is escalated to Level 1.

Escalation Level 1

TECHNICAL OPERATIONS TEAM

1. Determines that the initial defensive action required is to notify employees of the phishing scam and educate them on avoiding these types of attacks.

2. Notifies Incident Coordinator.

3. Determines that employee action will be required, notifies Service Center.

CYBER INCIDENT COORDINATOR

1. Receives and tracks the phishing attack.

2. Escalates the threat to Level 2, since it has manifested itself.

3. Determines relevant membership of the Technical Operations and Extended Technical Team.

4. Alerts IT organizations and applicable support organizations of the phishing. The organizations begin modifying internal firewalls to block the offending website as well as initiating a system-wide password reset.

5. Alerts Cyber Incident Response Management of the phishing threat.

6. Alerts the Communications Team.

COMMUNICATIONS TEAM

1. A message is composed to all employees and sent system-wide. Additionally, all departmental managers are alerted to the phishing scam and asked to notify all employees in person immediately.

Escalation Level 2

CYBER INCIDENT COORDINATOR

1. Notifies Cyber Incident Response Management of the phishing attack.

2. Alerts the Cyber Incident Response Support Team of the phishing attack.

3. Alerts the Extended Team.

4. Receives status from the Technical Operations Team regarding the status of employee education. Reports the status to the Cyber Incident Response Management.

5. Starts a chronological log of the events, including logs of emails and, if possible, logs of users accessing the offending website.

TECHNICAL OPERATIONS TEAM

1. Determines that the best course of action for containing the attack is educating all employees about the attack and blocking any further emails from arriving on mail servers. Additionally, concludes that blocking the fraudulent website from being accessed internally. Finally, decides that a system-wide user password reset is necessary, since email is accessible from outside of *Our Organization*'s network and merely blocking the offending site will not be sufficient and the emails have been circulating for an unknown amount of time to only select employees.

2. Notifies the Extended Technical Team team of the above actions that are required.

3. Reports actions taken and status to the Cyber Incident Response Coordinator.

CYBER INCIDENT RESPONSE MANAGEMENT

1. Assumes responsibility for directing activities in regard to the phishing attack.

2. Determines that the attack does not need to be escalated to Level 3.

3. Determines when the risk has been mitigated to an acceptable level.

EXTENDED TECHNICAL TEAM

1. Takes the actions required by the Technical Operations Team.

2. Reports the actions taken, the number of personnel involved etc. to Cyber Incident Coordinator for the chronological log.

COMMUNICATIONS TEAM

1. Carries out the education of *Our Organization* employees by informing them of the incident and making sure everyone is aware of the scam as deemed appropriate by Cyber Incident Response Management.

2. Messages the *Our Organization* employees about the system-wide password reset, and how the employees must go about regaining access to their user accounts as determined by the Technical assessment team and directed by Cyber Incident Response Management.

Post Incident

CYBER INCIDENT RESPONSE MANAGEMENT

1. Prepare a report for *Our Organization* Executive Management to include:

   a. Estimate of the impact of addressing the phishing attack and the potential cost of not doing so,

   b. Action taken during the attack's assessment,

   c. Follow on efforts needed to eliminate or mitigate the vulnerability presented by the phishing attack,

   d. Policies or procedures that may require updating, such as password change rules and procedures, and

   e. Efforts taken to minimize the liabilities of negative exposure of the attack.

2. Provides the chronological log and any system audit logs requested by the Extended Team.

3. Documents any lessons learned and modifies the Cyber Incident Response Plan accordingly.

EXTENDED TEAM

1. Legal works with the authorities to present any information relating to the phishing party.

2. No disciplinary action will need to be taken.

3. Executive Management Team (EMT) leveraged to communicate to employees about the threat of phishing attacks and to be vigilant.

Threat Example 3: Stolen Asset, Leaked Confidential Information

Escalation Level 0

TECHNICAL OPERATIONS TEAM

1. An *Our Organization* employee has his or her laptop stolen, which contains unencrypted confidential personal information of *Our Organization* residents, including names, addresses, Social Security numbers, etc. The information has been found and posted on the public Internet. The threat is escalated to Level 1.

Escalation Level 1

TECHNICAL OPERATIONS TEAM

1. Determines that the attack has already taken place and that there is no initial technical defense possible in this circumstance. However, an internal data security practices audit is necessary to keep a data leak from happening again.

2. Notifies the Cyber Incident Coordinator.

3. Determines that employee action required to secure confidential data in the future through education. Contacts Service Center to arrange for instructions.

CYBER INCIDENT COORDINATOR

1. Receives and tracks the stolen data event.

2. Escalates to Level 2, because the threat has manifested itself.

3. Determines relevant membership of the Technical Operations and Extended Technical teams.

4. Alerts IT organizations and applicable support organizations of the situation. Defensive action that must be taken involves an audit of information security practices internally to ensure further data breaches do not occur.

5. Alert Cyber Incident Response Management of the data leak.

6. Alert the Communications team.

COMMUNICATIONS TEAM

1. Employee action is going to be required for the internal information security practices audit. The Communications Team notifies employees of the data breach and the actions that are going to be taken to prevent such a leak in the future.

Escalation Level 2

CYBER INCIDENT COORDINATOR

1. Notifies Cyber Incident Response Management of the data leak.

2. Alerts the Cyber Incident Response Support Team of the data leak.

3. Alerts the Extended Team.

4. Receives status of the information security audit from the Technical Assessment Team and reports to Cyber Incident Response Management.

5. Starts a chronological log of events from the origin of the data to determine how the data ended up in a situation where it could be leaked. The chronological log will be used to support possible follow on legal action as determined by *Our Organization*'s General Counsel and Executive Directors.

TECHNICAL OPERATIONS TEAM

1. Determines that containment of the incident is going to be legal in nature, but that information security practices will need to be overhauled.

2. Notifies Extended Technical Team of the plan to audit and augment data security practices internally, including any technical measures that will need to be put into place to that end.

3. Reports actions taken and status to the Cyber Incident Response Coordinator.

CYBER INCIDENT RESPONSE MANAGEMENT

1. Assumes responsibility for directing activities in regard to the incident.

2. Determines that escalation Level 2 is not sufficient and escalates the incident to Level 3.

3. Determines when the risk has been mitigated to an acceptable level.

EXTENDED TECHNICAL TEAM

1. Takes action to begin comprehensive information security practices audit internally, as determined by the Technical Operations Team.

2. Reports actions taken, number of personnel involved etc. to Incident Coordinator for the chronological log.

COMMUNICATIONS TEAM

1. Messages *Our Organization* employee population informing them of the information leak and the ensuing legal action, as deemed appropriate by Cyber Incident Response Management.

2. Messages *Our Organization* employee population of the forthcoming comprehensive information security practices audit and the organization-wide practices that will be augmented as determined by the Technical Operations team and directed by Cyber Incident Response Management.

Escalation Level 3

CYBER INCIDENT RESPONSE MANAGEMENT

1. Directs the Cyber Incident Response Support team to:

   a. Set up communications between all Cyber Incident Response Team Managers, and the Extended Support Team in the field,

   b. Assume occupancy of the command center, and

   c. Initialize an incident voice mail box where status messages can be placed to keep *Our Organization* personnel statused.

2. Alerts the Extended Team of the incident notifying them of the Severity Level.

3. Determines when the risk has been mitigated to an acceptable level after the comprehensive information security data protection audit and overhaul.

4. Statuses Executive Management as appropriate.

EXTENDED TEAM

1. Contacts local, state, and federal authorities.

2. Makes arrangements for authorities to be allowed into the command center.

3. Ensures that all needed information is being collected to support legal action against the leaker and financial restitution for

those affected by the breach of their personal information by *Our Organization* personnel.

CYBER INCIDENT RESPONSE COORDINATOR

1. Continues maintaining the Chronological Log of the event.

2. Posts numbered status messages in the incident voice mail box for statusing *Our Organization* Executive Management Team (if applicable).

COMMUNICATION TEAM

1. Messages *Our Organization* population as directed by Cyber Incident Response Management regarding the status of the information security data practices audit and any forthcoming changes to be made to policy.

TECHNICAL OPERATIONS TEAM

1. Continues to monitor all known sources for alerts looking for further information or actions to take to eliminate the threat of further data being lost in any way, both internally and externally.

2. Continues reporting status to the Cyber Incident Response Coordinator for the chronological log of events.

3. Monitors effectiveness of the information security practices audit and subsequent changes and modifies them as necessary.

4. Statuses Cyber Incident Response Management on effectiveness of actions taken and progress in eliminating the threat of further information leakage.

EXTENDED SUPPORT TEAM

1. Continues the information security practices audit and changes to eradicate the further threat of data leaks as directed by Cyber Incident Response Management and the Technical Operations team.

2. Continues to report actions taken, number of personnel etc. to the Cyber Incident Response Coordinator for the chronological log.

Post Incident

CYBER INCIDENT RESPONSE MANAGEMENT

1. Prepare a report for *Our Organization* Executive Management to include:

a. Estimate of the impact of addressing the data leak and the potential cost of not doing so,

b. Action taken during the comprehensive information security practices audit and assessment,

c. Follow on efforts needed to eliminate or mitigate any and all vulnerabilities that exist in terms of confidential data security,

d. Policies or procedures that may require updating to ensure strict oversight of sensitive data within *Our Organization*,

e. Efforts taken to minimize the liabilities of negative exposure of the attack.

2. Provides the chronological log and any system audit logs requested by the Extended Team.

3. Documents any lessons learned and modifies the Cyber Incident Response Plan accordingly.

EXTENDED TEAM

1. Legal works with the authorities to present any information relating to the leaking party that may lead to prosecution.

2. Human Resources and Information Services work with *Our Organization* management to determine disciplinary action for the negligent employee.

3. Executive Management Team leveraged to communicate to employees about the seriousness of keeping data safe and the costs of not doing so, as exemplified in this case.

Appendix C: ACIS Security Incidents Reporting Template*

Incident Detector's Information				
Date/Time of Report				
First Name				
Last Name				
Department/Division				
Title/Position				
Work Email Address				
Contact Phone Numbers	*Work*	*Mobile*	*Pager*	*Other*

Reported Incident Information	
Incident Location	
Incident Point of Contact (if different than above)	
Priority	*Level 1 / Level 2 / Level 3*
Data Breach?	*Yes / No*
Breach Category	
Incident Type	
US-CERT Category	*DoS / Malicious Code / Probes and Scans / Unauthorized Access / Other*
US-CERT Number	
Description	
Additional Support Action Requested	
Method Detected	*IDS/Log Review/ A/V Systems/ User Notification/ Other*
Configuration Item(s) Affected	
Department/ Division Impact	
Information Sharing	*Entities with which ACIS can share incident data*
System for Sharing	
Status	*Ongoing/ Resolved/ Etc.*

Attacking Computer(s) Information				
IP Address / Range	Host Name	Operating System	Ports Targeted	System Purpose

Victims Computer(s) Information				
IP Address / Range	Host Name	Operating System	Ports Targeted	System Purpose

Action Plan	
Action Description	
Requestor	
Assignee	
Time Frame	
Status	

	Conclusion / Summary
Entities Notified	
Resolution	*Include whether lost materials recovered as part of the solution*

CJIS Reporting Template

Other?

Attachment 3
SAMPLE CIS Controls IG 1 Assessment and Plan

NOTE: The Attachments provided in Exhibit 2 are Samples that can be used in carrying out the activities of this contract. The Contractor shall use these sample documents, an equivalent/improved version of their own creation, or an updated version published by the State at a future date on www.michigan.gov/cyberpartners.

The following is a screenshot of Attachment 3. To obtain complete file please see [www.michigan.gov/cyberpartners.](www.michigan.gov/cyberpartners)

CIS Control	CIS Sub-Control	Asset Type	Security Function	Title	Description	Implementation Group 1	Implementation Group 2	Implementation Group 3
1				**Inventory and Control of Hardware Assets**		X	X	X
				Actively manage (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.		X	X	X
1	1.1	Devices	Identify	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.		X	X
1	1.2	Devices	Identify	Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.			X
1	1.3	Devices	Identify	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.		X	X
1	1.4	Devices	Identify	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.	X	X	X
1	1.5	Devices	Identify	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.		X	X
1	1.6	Devices	Respond	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined, or the inventory is updated in a timely manner.	X	X	X
1	1.7	Devices	Protect	Deploy Port Level Access Control	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.		X	X
1	1.8	Devices	Protect	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.			X