Whole-of-State Service Agreement and Work Order Contract

State of Minnesota

Executive Summary

Minnesota IT Services (MNIT), in partnership with the Minnesota Cybersecurity Task Force, launched the Whole-of-State Cybersecurity Plan in 2023 to strengthen local government cyber defenses. The whole-of-state approach presents a strong, united front against cyber threats, and bolsters cybersecurity across Minnesota.

The Cybersecurity Task Force established four goals to advance the Whole-of-State Plan: Mature cyber capabilities throughout the state; collaborate and share information throughout the state; increase participation in programs and services known to work; and strengthen the cyber-resiliency of critical infrastructure. These goals are designed to provide a solid foundation for a long-term, sustainable cybersecurity system that builds on results and moves with the times.

MNIT is creating a framework built on collaboration and inclusion to provide the tools, resources, and information eligible entities need to help secure the data that Minnesotans have entrusted to their organization.

Under the whole-of-state approach, the Statewide Security Monitoring Initiative (SSMI) – also referred to as the State Homeland Security Grant Program (SHSP) - and the State and Local Cybersecurity Program (SLCGP) use funding to create a layered approach to security. This helps protect Minnesotans by advancing stronger, sustainable cybersecurity tools and processes that leverage best practices, build on past successes, meet every organization where they are, educate, and freely share information.

Work Order Contract

This Work Order Contract is between the State of Minnesota, acting through its commissioner of Minnesota IT Services ("State") and Minneapolis Parks and Recreation Board ("Governmental Unit"), whose designated business address is 2117 River Road North Minneapolis, MN 55411. "Governmental Unit" includes any agents, employees, or third-party service providers working on behalf of the Governmental Unit.

The Statewide Security Monitoring Initiative (SSMI) is a program devoted to protecting the data of all Minnesotans by partnering with participating county governments, port cities, and Tribal Nations to ultimately fortify the cybersecurity of the entire state of Minnesota. The State and Local Cybersecurity Grant Program (SLCGP) is a program devoted to protecting the technology, data, and systems that make our government and schools run is one of our highest priorities and aims to make sure that our state, county, municipal, and tribal government, education, public health, critical infrastructure, and peacekeepers have all the cybersecurity tools and resources they need.

Governmental Unit is requesting State to provide certain security services through its SSMI and/or SLCGP program as identified in this Work Order Contract.

Contract

1. Term of Work Order

1.1 Effective date. This Work Order is effective on the date State obtains all required signatures under Minn. Stat. § 16C.05, subd. 2. State will not begin work under this contract until this contract is fully executed and State has been notified by Governmental Unit's Authorized Representative to begin work.

1.1 Expiration date. This Work Order is effective through June 30, 2027.

2. Service Selection and Authorization

Upon execution of this Work Order, State will provide the services selected by Governmental Unit in Table 1. Some services are performed only by State ("First-Party Services"). Some services include work performed or tools provided by third parties, either in conjunction with or independent of State's provision of services ("Third-Party Services"). For more information visit **https://mn.gov/mnit/about-mnit/security/wos/.**

SELECTION(S)	SERVICE OFFERING	DESCRIPTION OF SERVICE OFFERING
	1 – External Vulnerability Scans	The Minnesota IT Services (MNIT) Threat and Vulnerability Management Unit (TVMU) provides external vulnerability Management service. MNIT provides a comprehensive vulnerability scanning service that utilizes sophisticated and automated vulnerability scanning and attack surface management technology. MNIT continuously monitors scan results, assesses critical and high-risk vulnerabilities, and communicates actionable information to the participating entity. **The term of this contract expires on June 30, 2027.** More information available here: https://mn.gov/mnit/about-mnit/security/wos/
	2 – Internal Vulnerability Scans	The MNIT Threat and Vulnerability Management Unit (TVMU) provides internal vulnerability management service to SSMI eligible entities. TVMU provides a comprehensive vulnerability scanning tool that utilizes sophisticated enterprise class scanning technology to conduct in-depth vulnerability and configuration compliance scanning using credentials/agents' technology. The TVMU team conduct regular briefing meetings with participating organizations to discuss scan findings and remediation. **The term of this contract expires on June 30, 2027.** More information available here: https://mn.gov/mnit/about-mnit/security/wos/ Billing is done on a monthly basis, according to the size category the Governmental Unit falls within and the number of addresses scanned. Contact the TVMU team (TVMU@state.mn.us) for more information on Internal Vulnerability Scanning billing.
☑	3 - SIEM	The Next Generation Security Information and Event Management (SIEM) program is provided at a reduced cost to Minnesota counties, cities, townships, public K12s, Tribal entities, and other partner organizations through the CrowdStrike console. Pricing is based on daily ingest amount and record retention needs. More information available here: https://mn.gov/mnit/about-mnit/security/wos/ **The term of this contract expires on June 30, 2027.** Billing is done monthly based on data ingest and contracted end-point counts. Billing will be based on monthly usage. Contact the Cyber Navigator team (CN.MNIT@state.mn.us) for more

		information on SIEM billing: https://mn.gov/mnit/about-mnit/security/whole-of-state-cybersecurity-plan/ngs.jsp
☑ 660 Licenses Minimum	4 – MDR	The Managed Detection and Response (MDR) program is provided at a reduced cost to Minnesota counties, cities, townships, public K12s, Tribal entities, and other partner organizations through the CrowdStrike console. More information available here: https://mn.gov/mnit/about-mnit/security/wos/ **The term of this contract expires on June 30, 2027.** Governmental Unit agrees to be billed monthly based on the contracted amount specified in this agreement. If the Governmental Unit's usage exceeds the contracted amount, the Governmental Unit will be invoiced for the overage at the rates specified in this agreement. Contact the Cyber Navigator team (CN.MNIT@state.mn.us) for more information on MDR billing.
	5 - EDR	The Endpoint Detection and Response (EDR) program is provided at a reduced cost to Minnesota counties, cities, townships, public K12s, Tribal entities, and other partner organizations. The EDR program does not include oversight and management from CrowdStrike or MNIT. More information available here: https://mn.gov/mnit/about-mnit/security/wos/ **The term of this contract expires on June 30, 2027.** Governmental Unit agrees to be billed monthly based on the contracted amount specified in this agreement. If the Governmental Unit's usage exceeds the contracted amount, the Governmental Unit will be invoiced for the overage at the rates specified in this agreement. Contact the Cyber Navigator team (CN.MNIT@state.mn.us) for more information on EDR billing.
☑	6 – MDBR	Malicious Domain Blocking and Reporting (MDBR): A cloud-based solution that uses technology to prevent IT systems from connecting to harmful web domains and limit infections related to malware, ransomware, phishing, and other cyber threats. **The term of this contract expires on June 30, 2027.** For more full program participation rules and more information see website: https://mn.gov/mnit/about-mnit/security/wos/ This is a no charge service. Governmental Unit will not be billed as this service is being covered by the SLCGP grant. For more information, contact the Cyber Navigator team (CN.MNIT@state.mn.us)

Table 1

Governmental unit understands that State is subsidizing some or all these services through a combination of State Homeland Security Grant Program (SHSP) and State and Local Grant Program (SLCGP) funds allocated to Minnesota. This funding includes:

- State and Local Cybersecurity Grant Program for Federal Fiscal Year (FFY) 2023, Funding Opportunity **DHS-23-137-000-01**, as authorized by Section 2220A of Homeland Security Act of 2002, as amended (Pub. L. No. 107-296) (6 U.S.C. § 665g).
- State Homeland Security Grant Program (SHSP) for FFY 2023, Funding Opportunity (**DHS-23-GPD-067-00-01**) as authorized by Section 2002 of the Homeland Security Act of 2002 (Pub. L. No. 107-296, as amended) (6U.S.C. § 603).
- Minnesota State and Local Cybersecurity Grant Program has a State Match requirement for FFY23 **(see** Laws of Minnesota 2023, chapter 62, article 1, section 10**)**.

- For more information on these grants and their allocation, please see the MNIT Whole of State program webpage here: https://mn.gov/mnit/about-mnit/security/wos/

Governmental unit consents and accepts these services in lieu of direct allocation of funds from these grant programs. Governmental unit agrees that it is responsible for subsidized portion in the event these funding sources are no longer available. For more information on these programs, please refer to https://mn.gov/mnit/about-mnit/security/wos/.

Governmental Unit understands and agrees State's provision of services under this Work Order do not include remediation of any security issues identified during State's provision of services.

Governmental Unit understands and agrees that some selected Third-Party Services may require a minimum term commitment ("Minimum Commitment") from Governmental Unit, as identified in Table 1. Governmental Unit agrees to pay for the quantity of services identified in Table 1 with a Minimum Commitment selected for the duration of the Minimum Commitment.

3. Representations and Warranties

3.1 Under Minnesota Statutes Ch. 16E, State is empowered to create and maintain state cyber security systems and ensure overall security of the state's information and technology systems and services; promote cooperation and collaboration among state and local governments in developing intergovernmental information and telecommunications technology systems and services; and enter into contracts with agencies of the federal government, local governmental units, the University of Minnesota and other educational institutions, and private persons and other nongovernmental organizations as necessary to perform its statutory duties.

3.2 Governmental Unit represents and warrants that it possesses the legal authority to enter into this Work Order and that it has taken all actions required by its procedures, by-laws, and applicable laws to exercise that authority, and to lawfully authorize its undersigned signatory to execute this Work Order, or any part thereof, and to bind Governmental Unit to its terms.

4. Consideration and Payment

All service costs and billing considerations are available on https://mn.gov/mnit/about-mnit/security/wos/ or by contacting the Cyber Navigator team (CN.MNIT@state.mn.us) or TVMU team (TVMU@state.mn.us). MNIT will provide 90 days notice before changing the published rates of these programs.

Billing is compiled after the end of each month and invoices are posted within CosWeb (cosweb.mnit.state.mn.us) for Governmental Unit access, under Computing Services. Governmental Unit billing contact(s) will receive an email message notifying them there is at least one new invoice to review.

Internal Vulnerability Scanning billing is based upon the size category assigned to the Governmental Unit as well as the number for addresses requested to be scanned. These address amounts are audited annually.

MDR billing is based upon the number for MDR licenses requested, so will always be at least that number – if more licenses are in use at the end of the month, Governmental Units will be charged for that larger number of licenses.

EDR billing is based upon the number for EDR licenses requested, so will always be at least that number – if more licenses are in use at the end of the month, Governmental Units will be charged for that larger number of licenses.

SIEM billing is based upon the number for SIEM licenses requested, so will always be at least that number – if more licenses are in use at the end of the month, Governmental Units will be charged for that larger number of licenses.

5. Authorized Representatives
State's Authorized Representative, their delegate, or successor in office is required to sign this Work Order.

6. Third Party Terms
Governmental Unit acknowledges it has reviewed the terms of the agreements State has with its third-party contractors used to provide the services selected by Governmental Unit under this Work Order, which are available at https://mn.gov/mnit/about-mnit/security/wos/, as updated. ("Third-Party Terms"). Governmental Unit agrees to comply with the Third-Party Terms to the extent those terms apply to the services ordered and received by Governmental Unit under this Work Order.

7. Assignment, Amendments, Waiver, and Contract Complete.

7.1 Assignment. Neither Party may assign nor transfer any rights or obligations under this Agreement without the prior consent of the other Party and a fully executed assignment agreement, executed and approved by the authorized parties or their successors.

7.2 Amendments. Any amendment to this Agreement must be in writing and will not be effective until it has been executed and approved by the authorized parties or their successors.

7.3 Waiver. If either Party fails to enforce any provision of this Agreement, that failure does not waive the provision or its right to enforce it.

7.4 Contract Complete. This Work Order, including as applicable Third-Party Waivers, Master Control Agreements, and Third-Party Terms incorporated by reference, contains all negotiations and agreements between State and Governmental Unit. No other understanding regarding this Agreement, whether written or oral, may be used to bind either party.

8. Liability.

8.1 Each party will be responsible for its own acts and behavior and the results thereof.

8.2 Nothing within this Agreement, whether express or implied, shall be deemed to create an obligation on the part of State to indemnify, defend, hold harmless or release Governmental Unit. This shall extend to all agreements related to the subject matter of this Contract, and to all terms subsequently added, without regard to order of precedence.

9. State Audits.
Under Minn. Stat. § 16C.05, subd. 5, Governmental Unit's books, records, documents, and accounting procedures and practices relevant to this Agreement are subject to examination by State, the State Auditor, or Legislative Auditor, as appropriate, for a minimum of six years from the expiration or termination of this Agreement.

10. Government Data Practices.
Governmental Unit and State must comply with the Minnesota Government Data Practices Act, Minn. Stat. Ch. 13, (or, if State contracting party is part of the Judicial Branch, with the Rules of Public Access to Records of the

Judicial Branch promulgated by the Minnesota Supreme Court as the same may be amended from time to time) as it applies to all data provided by State under this Agreement, and as it applies to all data created, collected, received, stored, used, maintained, or disseminated by the Governmental Unit under this Contract. The civil remedies of Minn. Stat. § 13.08 apply to the release of the data governed by the Minnesota Government Practices Act, Minn. Stat. Ch. 13, by either Governmental Unit or State.

If the Governmental Unit receives a request to release the data referred to in this clause, Governmental Unit must promptly notify and consult with State's Authorized Representative as to how the Governmental Unit should respond to the request. Governmental Unit's response to the request shall comply with applicable law.

11. Governing Law, Jurisdiction, and Venue.
Minnesota law, without regard to its choice-of-law provisions governs this Work Order. Venue for all legal proceedings out of this Work Order, or its breach, must be in the appropriate state or federal court with competent jurisdiction in Ramsey County, Minnesota.

12. Termination
State or Governmental Unit may terminate this Work Order at any time, with or without cause, upon 60 days written notice to the other Party. Termination will be effective at the end of the month in which the 60 day period concludes. The State will bill through the end of the next closest month following the termination. For Third-Party Services with a Minimum Commitment, Governmental Unit understands and agrees that termination will terminate provision of services, but Governmental Unit will remain obligated to the amounts owed for the Minimum Commitment. This Work Order will terminate automatically upon execution between State and Governmental Unit of a subsequent Work Order covering the same or additional service selections.

13. Renewal

Governmental Unit shall notify State of its desire to enter into a new Work Order for further provision of services within 60 days of the expiration date of this Work Order.

1. **Governmental Unit**
The Governmental Unit certifies that the appropriate person has executed the Work Order Contract on behalf of the Governmental Unit as required by applicable laws, articles, bylaws, resolutions, or ordinances.

Print Name: Al Bangoura

Signature: _____

Title: Superintendent

Date: _____

2. **State Agency**
With delegated authority

Print Name: John Israel _____

Signature: _____

Title: MNIT CISO Date: _____

3. **Commissioner of Administration**
As delegated to The Office of State Procurement

Print Name: _____

Signature: _____

Title: _____ Date: _____

Admin ID: _____