MATANUSKA-SUSITNA BOROUGH INFORMATION MEMORANDUM IM No. 24-075

SUBJECT: INFORMING THE ASSEMBLY OF THE MANAGERS SIGNATURE ON AND SUBMITTAL OF A FEDERAL FISCAL YEAR 2022/2023 STATE AND LOCAL CYBERSECURITY GRANT APPLICATION.

AGENDA OF: April 2, 2024

ASSEMBLY ACTION: Presented to the Assembly 04/02/24 - BJH

AGENDA ACTION REQUESTED: For information only.

Route To	Signatures
Originator	3/18/2024 X Mark Sowers Signed by: Mark Sowers
IT Director	3/19/2024 X Leah Jones Signed by: Leah Jones
Finance Director	3/20/2024 X Cheyenne Heindel Signed by: Cheyenne Heindel
Borough Attorney	3/20/2024 X John Aschenbrenner Signed by: John Aschenbrenner
Borough Manager	3/20/2024 X MichaelBrown Signed by: MichaelBrown
Borough Clerk	3/21/2024 X Lonnie McKechnie Signed by: Lonnie McKechnie

ATTACHMENT(S): Local Cybersecurity Grant Program Applications (8 pp)

SUMMARY STATEMENT: The Department of Information Technology has submitted an application for the local cybersecurity grant program. This total of $79,000 in funding will support $64,000 for improvement and expansion of current cybersecurity processes into a cohesive and integrated system, and $15,000 will be used for aligning all Borough networks to a uniform security standard.

Alaska Division of Homeland Security and Emergency Management

Federal Fiscal Year 2022/2023 State and Local Cybersecurity Grant Program (SLCGP) Application Coversheet

Application Deadline 11:59 p.m., Friday, March 29, 2024

Application Checklist

☒ Application Package includes the following:

1. Completed Federal Fiscal Year (FFY) 2022/2023 State and Local Cybersecurity Grant Program (SLCGP) Application Coversheet.
2. Completed Federal Fiscal Year (FFY) 2022/2023 State and Local Cybersecurity Grant Program (SLCGP) Project Application Form(s). ***You must complete one form for each individual project***.
3. Signatory Authority Form with required three (3) signatures for jurisdiction (available at https://ready.alaska.gov/Grants)
4. Print-out of Jurisdiction's www.SAM.gov Entity Overview record displaying the jurisdiction's UEI Number

☐ Attach any applicable Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) related to the inter-agency project.

Jurisdiction:	Matanuska-Susitna Borough
Responsible Borough: (if applicable)	Matanuska-Susitna Borough

Only four (4) projects per jurisdiction may be submitted.

Project Priority	Project Budget Category (drop-down options)	Project Title	Funding Request
1	Exercise	Robust Vulnerability Management Software Implementation	$64,000
2	Equipment	Emergency Services Security Infrastructure Alignment	$15,000
	Choose an item.		$
	Choose an item.		$
		Total Request	**$79,000**

Jurisdiction Point of Contact for Project Applications

Name: Dan Monarch

Address: 350 E Dahlia St., Palmer, AK 99645

Email Address: dan.monarch@matsugov.us

Telephone Number: 907-861-8558

Fax Number:

Certification and Authorization to Submit Application

By signature below, the undersigned certifies and acknowledges:

The jurisdiction has a financial management system in accordance with the 2 CFR Part 200 *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards, §200.300-.309 Standards for Financial and Program Management* and;

the jurisdiction complies with all local procurement policies and procedures and conforms to applicable state and federal law and the standards identified in 2 CFR Part 200 *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*, *§200.317-.326 Procurement Standards* to include having a written code of standards when using federal funds and;

the undersigned has been duly authorized by the jurisdiction to submit this application and will comply with the assurances, agreements, and/or special conditions set forth upon receipt of the grant award.

Jurisdiction Financial Officer
Printed Name:

_____
Signature

Jurisdiction Signatory Official
Printed Name:

_____
Signature

Project Applications and Cover Sheet must be submitted electronically (in PDF format with complete signatures) by email to:

Division of Homeland Security and Emergency Management
Email: mva.grants@alaska.gov

Phone: (907) 428-7000 or 1-800-478-2337

Alaska Division of Homeland Security and Emergency Management

Federal Fiscal Year 2022/2023 State and Local Cybersecurity Grant Program (SLCGP) Application

Application Deadline 11:59 p.m., Friday, March 29, 2024

Please contact **mva.grants@alaska.gov** or call the Grants Section at 907-428-7000 or 1-800-478-2337 if you have any questions regarding this application.

This form must be completed for each project. To qualify as a **single project**, the pieces of the project must be integral toward achieving one precise objective. See state overview and guidelines for more information.

Ensure all questions on this form are completed. Questions that are left blank will receive a score of 0.

Please duplicate this form as necessary.

Jurisdiction:	Matanuska-Susitna Borough	
Amount Requested	$64,000	Project Priority 1 Up to four (4) projects may be submitted.
Project Title	Robust Vulnerability Management Software Implementation	
Choose the budget category.	☒ Exercise	☐ Equipment
	☐ Planning	☐ Training
Is this a continuation project from a previous grant year?	☐ Yes or ☒ No If yes, which grant/year?	

1. Describe the project. (Make sure to include what the project is, who the project is for, how the project will help the jurisdiction, quantity of items, etc.)

Project Description:
Implementing a robust vulnerability management software solution for the Matanuska-Susitna Borough will transform our current ad-hoc vulnerability assessments into a systematic, automated, and continuous process. In an age where cyber threats evolve rapidly, establishing a routine and proactive approach to vulnerability management is crucial. This project will implement software that provides advanced technologies and methodologies to regularly scan, identify, and address security vulnerabilities, thereby enhancing our digital defenses and resilience. By enhancing our cyber defenses, the borough aims to establish a benchmark in cybersecurity excellence, ensuring the safety and trust of our community members and stakeholders.

Objectives:

- Implement an enterprise grade software platform for robust vulnerability management.
- Establish Routine Vulnerability Assessments: Implement a structured schedule for regular vulnerability scanning to identify and evaluate potential security threats systematically, transitioning from an ad-hoc to a continuous, predictable process.
- Automate Vulnerability Management Processes: Leverage state-of-the-art automation tools and technologies to streamline the identification, assessment, and mitigation of vulnerabilities, reducing human error and increasing efficiency.
- Enhance Cybersecurity Posture: By identifying and addressing vulnerabilities promptly and effectively, improve the overall cybersecurity posture of the Matanuska-Susitna Borough, reducing the risk of successful cyber-attacks.

- Build a Scalable and Adaptable Framework: Develop a vulnerability management framework that is both scalable to accommodate growth and adaptable to evolving cyber threats, ensuring long-term resilience and security.
- Foster a Culture of Cybersecurity Awareness: Promote cybersecurity awareness and best practices within the organization to encourage proactive detection and reporting of security vulnerabilities, creating a more secure and informed workplace environment.

Anticipated Outcomes:
Upon the successful of the vulnerability management project, the Matanuska-Susitna Borough anticipates achieving a series of transformative outcomes that will significantly bolster our cybersecurity framework. Key among these is the alignment with CIS Critical Security Control 7, ensuring that our vulnerability management processes are continuous, informed, and actionable. By establishing a routine and automated system, we expect a marked reduction in the incidence and impact of cyber threats, enhanced efficiency in identifying and addressing vulnerabilities, and improved compliance with industry standards. This project will not only fortify our cyber defenses but also foster a culture of cyber resilience, ultimately safeguarding our stakeholders' data and trust.

2. Explain how the project supports increased cybersecurity preparedness/response.
The vulnerability management project, initiated by the Matanuska-Susitna Borough, is set to significantly elevate our cybersecurity preparedness and response capabilities. By transitioning from ad-hoc to scheduled, repetitive, and automated vulnerability assessments, we will achieve a continuous and real-time understanding of our security posture. This proactive approach allows us to swiftly identify and remediate vulnerabilities before they can be exploited, minimizing the risk of cyber incidents. Additionally, the systematic documentation and analysis of vulnerabilities will enhance our incident response strategies, enabling more informed and rapid decision-making in the face of potential cyber threats. Ultimately, this project will not only fortify our defenses but also streamline our response mechanisms, ensuring that the borough can quickly and effectively counteract and recover from cyber incidents, thus maintaining the integrity, availability, and confidentiality of our critical digital resources."

3. Does this project address a gap identified in the Cybersecurity Assessment? If yes, please provide a page number.
Funding for a third-party security assessment, aimed at enhancing the cybersecurity posture of the Matanuska-Susitna Borough, was successfully secured during the 2022 SLCGP application period. While the grant has been awarded, the funds are pending receipt, and consequently, the security assessment has not yet commenced. Despite this, our cybersecurity staff have identified preliminary weaknesses in our current vulnerability management processes. Based on these insights, we anticipate that the forthcoming security assessment will underscore these issues, validating the need for a structured, comprehensive approach to vulnerability management. This project is strategically designed to address this anticipated gap, demonstrating our proactive stance and commitment to strengthening our cybersecurity infrastructure. Upon completion of the assessment, we will refine our project's focus and activities based on its specific findings, ensuring a targeted and effective enhancement of our cybersecurity resilience.

4. Explain the implementation of this project and how start-up will begin within the first 90 days of award.
During the first 90 days of the award, we will prepare an SOW that can be incorporated into an RFP that will be released to select a vendor to provide the vulnerability management functionality we require.

5. Explain the financial need for this grant to support this project. Please include if any jurisdictional funds are being used and how you plan to maintain and sustain the project financially.
The Matanuska-Susitna Borough is committed to enhancing our cybersecurity defenses, particularly in the area of vulnerability management. While we recognize the critical importance of this initiative, the financial constraints of our local budget limit our capacity to implement such a comprehensive project independently. The grant funding is essential to bridge this financial gap, enabling us to acquire the necessary tools, technologies, and expertise to establish and maintain a robust vulnerability management program.

To ensure the sustainability and financial maintenance of the project beyond the grant period, we plan to:

- Integrate the project's ongoing costs into our annual budgeting process, prioritizing cybersecurity as a critical aspect of our operations.
- Monitor and evaluate the project's effectiveness and efficiency, adjusting our strategies to ensure cost-effective use of resources.

By securing this grant, alongside our strategic planning for future sustainability, the Matanuska-Susitna Borough will significantly enhance our cybersecurity posture, protect our digital assets, and better serve our community.

6. This section must describe and itemize expenses for all project components regardless of budget category (including travel costs, training fees, planning contracts, etc.) Columns not applicable can be left blank.

*Please provide the authorized equipment list (AEL) number for equipment. The DHS AEL can be found at https://www.fema.gov/authorized-equipment-list to look up the number.

Description	AEL # (If equipment)	Qty	Unit Cost	Cost Total
Proactive Vulnerability Management		1	64,000	64,000

7. Can this project be broken out into phases for funding? If so, please provide a possible phasing breakdown. ***Note:** Partial funding may be allocated if phases are or are not provided.

The project cannot be broken out into phases. It will be the one-time implementation of a vulnerability management platform to cover the entire environment at a single point in time.

Project Applications and Cover Sheet must be submitted electronically (in PDF format with complete signatures) by email to:

Division of Homeland Security and Emergency Management
Email: mva.grants@alaska.gov

Phone: (907) 428-7000 or 1-800-478-2337

Alaska Division of Homeland Security and Emergency Management

Federal Fiscal Year 2022/2023 State and Local Cybersecurity Grant Program (SLCGP) Application

Application Deadline 11:59 p.m., Friday, March 29, 2024

Please contact **mva.grants@alaska.gov** or call the Grants Section at 907-428-7000 or 1-800-478-2337 if you have any questions regarding this application.

This form must be completed for each project. To qualify as a **single project**, the pieces of the project must be integral toward achieving one precise objective. See state overview and guidelines for more information.

Ensure all questions on this form are completed. Questions that are left blank will receive a score of 0.

Please duplicate this form as necessary.

Jurisdiction:	Matanuska-Susitna Borough	
Amount Requested	$15,000	Project Priority 2 Up to four (4) projects may be submitted.
Project Title	Emergency Services Security Infrastructure Alignment	
Choose the budget category.	☐ Exercise	☒ Equipment
	☐ Planning	☐ Training
Is this a continuation project from a previous grant year?	☐ Yes or ☒ No If yes, which grant/year?	

1. Describe the project. (Make sure to include what the project is, who the project is for, how the project will help the jurisdiction, quantity of items, etc.)

This project will enable the Matanuska-Susitna Borough to align all networks to a uniform security standard. The information Technology department has worked to enhance the security posture for all software and hardware within the departments' scope of control. This project will allow the department to assist other departments that maintain critical infrastructure within the organization that do not currently meet these requirements. In order to complete this project, we would need to purchase (2) Firewalls, (1) Monitoring Server, and (1) SMS Alert system. This would allow us to meet the objectives listed below.

Objectives:

- Adopt an Enterprise-wide Network Infrastructure Security Standard: Implement a network security standard across all Borough networks current and future, transitioning from ad-hoc implementations and aligning to a uniform standard and security centric network approach.
- Enhance Cybersecurity Posture: By addressing network vulnerabilities, this will improve the overall cybersecurity posture of the Matanuska-Susitna Borough, reducing the risk of successful cyber-attacks.
- Build a Scalable and Adaptable Network: Build out a network that is both scalable to accommodate growth and adaptable to evolving cyber threats, ensuring long-term resilience and security.

2. Explain how the project supports increased cybersecurity preparedness/response.

This Emergency Services Security Infrastructure Alignment project will align all critical corporate networks with adopted uniform security standards. This alignment will ensure long-term resilience and security. Increased network resiliency and uptime will aid in all Borough operations across all corporate networks.

3. Does this project address a gap identified in the Cybersecurity Assessment? If yes, please provide a page number.

Funding for a third-party security assessment, aimed at enhancing the cybersecurity posture of the Matanuska-Susitna Borough, was successfully secured during the 2022 SLCGP application period. While the grant has been awarded, the funds are pending receipt, and consequently, the security assessment has not yet commenced. Despite this, our cybersecurity staff have identified preliminary weaknesses in our Emergency Services network environment. Based on these insights, we anticipate that the forthcoming security assessment will underscore these issues, validating the need for modifications to the Emergency Services network environment. This project is strategically designed to address this anticipated gap, demonstrating our proactive stance and commitment to strengthening our cybersecurity posture. Upon completion of the assessment, we will refine our project's focus and activities based on its specific findings, ensuring a targeted and effective enhancement of our cybersecurity resilience.

4. Explain the implementation of this project and how start-up will begin within the first 90 days of award.
During the first 90 days of the award, we will prepare an SOW that can be incorporated into an RFP that will be released to select a vendor to provide hardware and support assistance for installation and configuration.

5. Explain the financial need for this grant to support this project. Please include if any jurisdictional funds are being used and how you plan to maintain and sustain the project financially.
The Matanuska-Susitna Borough is committed to enhancing our cybersecurity defenses. While we recognize the critical importance of this initiative, the financial constraints of our local budget limit our capacity to complete the initial implementation for this project. The grant funding is essential to bridge this financial gap, enabling us to acquire the necessary tools, technologies, and expertise to establish and maintain the new equipment.

To ensure the sustainability and financial maintenance of the project beyond the grant period, we plan to:

- Integrate the project's ongoing costs into our annual budgeting process, prioritizing cybersecurity as a critical aspect of our operations.
- Monitor and evaluate the project's effectiveness and efficiency, adjusting our strategies to ensure cost-effective use of resources.

By securing this grant, alongside our strategic planning for future sustainability, the Matanuska-Susitna Borough will significantly enhance our cybersecurity posture, protect our digital assets, and better serve our community.

6. This section must describe and itemize expenses for all project components regardless of budget category (including travel costs, training fees, planning contracts, etc.) Columns not applicable can be left blank.

*Please provide the authorized equipment list (AEL) number for equipment. The DHS AEL can be found at https://www.fema.gov/authorized-equipment-list to look up the number.

Description	AEL # (If equipment)	Qty	Unit Cost	Cost Total
Palo Alto 440 Firewall	04HW-03-NETD	2	5000	10000
SMS Notification Server	04HW-03-NETD	1	1000	1000
Local Server	04HW-03-NETD	1	3500	3500

7. Can this project be broken out into phases for funding? If so, please provide a possible phasing breakdown. ***Note:** Partial funding may be allocated if phases are or are not provided.

The project could be broken out into phases with each line item in the itemized expenses list being purchased and implemented separately.

Project Applications and Cover Sheet must be submitted electronically (in PDF format with complete signatures) by email to:

Division of Homeland Security and Emergency Management
Email: mva.grants@alaska.gov

Phone: (907) 428-7000 or 1-800-478-2337