

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

**AGENDA OF: September 5, 2023**

**ASSEMBLY ACTION: Presented to the Assembly 09/05/23 - BJH**

**AGENDA ACTION REQUESTED: For information only.**

Route To	Signatures
Originator	<div>8 / 2 4 / 2 0 2 3</div> <div>X      A n g e l i n a B l a n c h a r d</div> <div>S i g n e d   b y : A n g e l i n a B l a n c h a r d</div>
Department Director	<div>8 / 2 4 / 2 0 2 3</div> <div>X      C h e y e n n e H e i n d e l</div> <div>S i g n e d   b y : C h e y e n n e H e i n d e l</div>
Finance Director	<div>8 / 2 4 / 2 0 2 3</div> <div>X      C h e y e n n e H e i n d e l</div> <div>S i g n e d   b y : C h e y e n n e H e i n d e l</div>
Borough Attorney	<div>8 / 2 5 / 2 0 2 3</div> <div>X      N i c h o l a s S p i r o p o u l o s</div> <div>S i g n e d   b y : N i c h o l a s S p i r o p o u l o s</div>
Borough Manager	<div>8 / 2 5 / 2 0 2 3</div> <div>X      M i c h a e l B r o w n</div> <div>S i g n e d   b y : M i c h a e l B r o w n</div>
Borough Clerk	<div>8 / 2 5 / 2 0 2 3</div> <div>X      L o n n i e M c K e c h n i e</div> <div>S i g n e d   b y : L o n n i e M c K e c h n i e</div>

**ATTACHMENT (S):** Local Cybersecurity Grant Program Application (9 pp)

**SUMMARY STATEMENT:** The Department of Information Technology has submitted an application for the local cybersecurity grant program. This grant request of \$97,000 in funding will support \$60,000 for a Third-Party security assessment for enhancing Matanuska-Susitna Borough cybersecurity and \$37,000 will be used to end-user security awareness training content.

Additional legislation to accept and appropriate the funding will be sent forward once the grant is received.

Alaska Division of Homeland Security and Emergency Management

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

**Application Deadline 11:59 p.m., Thursday, August 31, 2023**

**Application Checklist:**

☒ **The application package includes the following:**

1. Completed Federal Fiscal Year (FFY) 2022 State and Local Cybersecurity Grant Program (SLCGP) Application Coversheet.
2. Completed Federal Fiscal Year (FFY) 2022 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. If already completed, provide a copy of the jurisdiction's Cybersecurity Assessment.
5. Print-out of Jurisdiction's [www.SAM.gov](http://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.

<b>Jurisdiction:</b>	Matanuska-Susitna Borough
<b>Responsible Borough: (if applicable)</b>	Matanuska-Susitna Borough

***Only three (3) projects per jurisdiction may be submitted.***

Project Priority	Project Budget Category (drop-down options)	Project Title	Funding Request
1	Planning	Third-Party Security Assessment for Enhancing Matanuska-Susitna Borough Cybersecurity	\$60,000
1	Training	End-User Security Awareness Training Content	\$37,000
	Choose an item.		\$
<b>Total Request</b>			<b>\$97,000</b>

**Jurisdiction Point of Contact for Project Applications**

**Name:** Dan Monarch

**Telephone Number:** 907-861-8558

**Address:** 350 E Dahlia St., Palmer, AK 99645 **Email Address:** [dan.monarch@matsugov.us](mailto:dan.monarch@matsugov.us)

## **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:** Cheyenne Heindel

  
\_\_\_\_\_  
Signature

### **Jurisdiction Signatory Official**

**Printed Name:** Michael Brown

  
\_\_\_\_\_  
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](mailto: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 State and Local Cybersecurity Grant Program (SLCGP) Application

**Application Deadline 11:59 p.m., Thursday, August 31, 2023**

Please get in touch with [mva.grants@alaska.gov](mailto: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.

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	\$60,000	Project Priority 1 <small>Up to three (3) projects may be submitted.</small>
Project Title	Third-Party Security Assessment for Enhancing Matanuska-Susitna Borough Cybersecurity	
Choose the budget category.	<input type="checkbox"/> Exercise	<input type="checkbox"/> Equipment
	<input checked="" type="checkbox"/> Planning	<input type="checkbox"/> Training
Is this a continuation project from a previous grant year? <input type="checkbox"/> Yes or <input checked="" type="checkbox"/> 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:

The Third-Party Security Assessment for enhancing Matanuska-Susitna Borough cybersecurity is a proactive initiative designed to bolster the cybersecurity defenses of the borough's digital ecosystem through a comprehensive evaluation conducted by an independent third-party. This project aims to assess potential vulnerabilities, identify weaknesses, and provide expert recommendations for mitigating cyber risks in the Matanuska-Susitna Borough environment.

#### Objectives:

- **Comprehensive Evaluation:** The core objective of this project is to conduct an in-depth evaluation of the Matanuska-Susitna Borough's cybersecurity landscape by leveraging the expertise of a third-party security assessment team. This evaluation will cover a wide spectrum of digital assets, including systems, networks, applications, and data repositories.
- **Vulnerability Identification:** The project will identify and analyze potential vulnerabilities and security gaps within the borough's digital infrastructure. Through meticulous testing and analysis, the third-party assessment team will pinpoint areas of concern that might be exploited by malicious actors.
- **Risk Assessment:** Following the identification of vulnerabilities, a rigorous risk assessment will be undertaken to gauge the potential impact of each vulnerability. This assessment will provide a clear understanding of the overall cybersecurity risk landscape, enabling informed decision-making and resource allocation.

- **Expert Recommendations:** Based on the assessment findings, the third-party security assessment team will provide a comprehensive set of expert recommendations. These recommendations will encompass technical, procedural, and policy-driven measures aimed at enhancing the borough's cybersecurity posture and resilience.
- **Report and Documentation:** A detailed report will be generated, presenting the assessment outcomes, risk analysis, and actionable recommendations. This report will serve as a valuable resource for borough leadership, IT personnel, and stakeholders, guiding future cybersecurity initiatives.

#### Anticipated Outcomes:

The Third-Party Security Assessment for Enhancing Matanuska-Susitna Borough Cybersecurity project is expected to yield a comprehensive understanding of the borough's cybersecurity strengths and vulnerabilities. By leveraging third-party expertise, the borough will be empowered to proactively address potential threats, secure critical assets, and bolster public confidence in the integrity of digital services. The Matanuska-Susitna Borough aims to elevate its cybersecurity resilience, fortify its defenses against emerging cyber threats, and ensure the confidentiality, integrity, and availability of digital assets for the benefit of its residents and stakeholders.

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

The Third-Party Security Assessment project will significantly enhance cybersecurity preparedness for the Matanuska-Susitna Borough by engaging an independent expert team to comprehensively evaluate its digital environment. By identifying vulnerabilities and quantifying risks, the project will empower the borough to prioritize and implement targeted security measures. Expert recommendations will guide the enhancement of technical safeguards, procedural protocols, and policy frameworks. The project's detailed report will serve as a strategic guide for informed decision-making, incident response planning, and future security initiatives. Ultimately, this initiative will equip the borough with a proactive, well-informed, and resilient cybersecurity posture, safeguarding critical assets, bolstering public trust, and enabling swift and effective responses to potential cyber threats.

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

This project does not address a gap identified in the Cybersecurity Assessment. It is the Cybersecurity Assessment. The Matanuska-Susitna Borough completes the Nationwide Cybersecurity Review (NCSR) on an annual basis but this is an internal assessment and may include biased results since it is completed by internal resources that are responsible for the IT systems and infrastructure.

#### 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 third-party security assessment.

#### 5. Please briefly explain if this project could have a multi-jurisdictional or statewide benefit. Include any correspondence and/or MOUs as support.

Other than providing improved security for the Matanuska-Susitna Borough which has an impact on the overall safety for other jurisdictions and the state as a whole, the primary benefit of this project will be for the Borough.

#### 6. 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 performs ongoing security assessments using internal resources and existing funding. There is no funding that has been budgeted to perform a third-party security assessment that will provide an evaluation of the current security posture from an external perspective. The last third-party security assessment performed for the Matanuska-Susitna Borough was completed three years ago.

#### 7. 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
Third-Party Security Assessment		1	\$60,000	\$60,000

8. 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 a one-time security assessment to evaluate 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](mailto: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 State and Local Cybersecurity Grant Program (SLCGP) Application

**Application Deadline 11:59 p.m., Thursday, August 31, 2023**

Please get in touch with [mva.grants@alaska.gov](mailto: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.

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	\$37,000	Project Priority 2 <small>Up to three (3) projects may be submitted.</small>
Project Title	End-User Security Awareness Training Content	
Choose the budget category.	<input type="checkbox"/> Exercise	<input type="checkbox"/> Equipment
	<input type="checkbox"/> Planning	<input checked="" type="checkbox"/> Training
Is this a continuation project from a previous grant year? <input type="checkbox"/> Yes or <input checked="" type="checkbox"/> 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:

The Matanuska-Susitna Borough presently utilizes a training platform offered by the current vendor, KnowBe4, to educate Borough end-users on the crucial matter of cybersecurity awareness. This training holds immense value in ensuring end-users are trained on various security concepts and we have consistently relied on it for multiple years. We have found that engaging content is one of the keys to successfully training staff. Lessons that provide engaging content help to ensure that what staff learn is being internalized and retained. Any type of SCORM eLearning content can be integrated into the KnowBe4 training platform and then made available for various training purposes. This project will allow the Matanuska-Susitna Borough to procure engaging security awareness training content from an esteemed vendor, NINJIO, acknowledged through multiple awards for the exceptional quality of their offerings. This content will be integrated into the existing KnowBe4 learning platform and provided through various training initiatives.

#### Objectives:

- **Comprehensive Understanding of Threat Landscape:** The project seeks to equip end-users with an understanding of the current cyber threat landscape. Engaging content, including interactive modules, real-world case studies, and multimedia presentations, will provide insight into prevalent attack vectors, social engineering techniques, and emerging threats. By comprehending the adversary's tactics, end-users can proactively recognize and respond to potential risks.
- **Empowerment with Best Practices:** The engaging training content will offer actionable guidance on cybersecurity best practices. End-users will gain practical knowledge on password management, safe

browsing habits, secure email practices, device hygiene, and data protection. This empowerment will enable them to make informed decisions and contribute to the organization's defense against cyberattacks.

- **Cultivation of Vigilance:** Through compelling narratives and simulated scenarios, the content will foster a culture of vigilance among end-users. They will learn to recognize suspicious behaviors, phishing attempts, and other deceptive tactics employed by cybercriminals. By honing these skills, end-users can serve as the first line of defense, promptly identifying and reporting potential security incidents.
- **Behavioral Change:** The project aims to effect a positive behavioral change among end-users. The engaging content will be designed to not only inform but also inspire action. Users will be encouraged to apply newly acquired knowledge in real-world scenarios, reinforcing safe practices and transforming cybersecurity awareness into habitual behavior.
- **Mitigation of Human-Related Vulnerabilities:** Human error remains a significant contributor to cybersecurity breaches. By utilizing captivating content, the project aims to reduce human-related vulnerabilities. End-users will be sensitized to the consequences of lapses in security practices, leading to a reduction in incidents arising from unintentional actions or oversights.
- **Continuous Learning and Adaptation:** The content will be curated to reflect the evolving threat landscape, ensuring that end-users are always up-to-date with the latest cybersecurity challenges. Regularly updated content will facilitate continuous learning, enabling end-users to stay ahead of new tactics employed by cybercriminals.

#### Anticipated Outcomes:

By securing grant funding to acquire engaging content for end-user security awareness training, this project aspires to foster a cyber-resilient workforce. Empowered with knowledge, practical skills, and an innate sense of vigilance, end-users will play an active role in fortifying the organization's cybersecurity defenses, ultimately mitigating risks and enhancing overall digital security.

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

This project strongly bolsters cybersecurity preparedness and response by equipping end-users with essential knowledge and practical skills through engaging content. By fostering a deep understanding of cyber threats, promoting best practices, and cultivating a vigilant mindset, this initiative empowers individuals to proactively recognize and mitigate potential risks. As end-users internalize safe behaviors and contribute to incident reporting, the organization's overall response capabilities are heightened. This heightened awareness and active participation form a robust first line of defense, significantly enhancing the organization's ability to prevent, respond to, and recover from cyber incidents.

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

This project doesn't directly target any gaps pertaining to end-user security awareness that have been pinpointed in a Cybersecurity Assessment. Rather, it elevates the existing security awareness training framework already established within the Matanuska-Susitna Borough. It's important to recognize that end-users constitute the final line of defense against cybersecurity threats. Equipping them with the knowledge of utilizing technology in a safe and secure manner not only bolsters protection for the Borough but also extends to safeguarding their families and the broader community.

#### 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 be able to complete the procurement process for the new content and begin incorporating it into the existing cybersecurity awareness training platform.

#### 5. Please briefly explain if this project could have a multi-jurisdictional or statewide benefit. Include any correspondence and/or MOUs as support.

Other than providing improved security for the Matanuska-Susitna Borough and Borough Staff, which has an impact on the overall safety of other jurisdictions and the state as a whole, the primary benefit of this project will be for the Borough.



6. 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 already budgets annually for end-user cybersecurity training. This funding allows the Borough to purchase licensing to use the training platform and provided content. The existing platform has some good content but developing content is not their area of focus. Additional funding is required to purchase high-quality content that can be used on the platform. Users are already exposed to some great content on the web. If the Borough is not able to provide engaging content, end-user training becomes monotonous and boring. Users will find ways to avoid it and the money, time, and energy spent on these efforts is greatly minimized.

7. 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
Security Awareness Training Content		1	\$37,000	\$37,000

8. 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 a one-time purchase of SCORM format cybersecurity awareness training content that will be incorporated into the existing training platform. New content being developed by NINJIO will also be added as it is available.




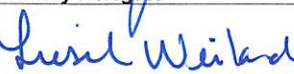



Project Applications and Cover Sheet must be submitted electronically (in PDF format with complete signatures) by email to:

**Division of Homeland Security and Emergency Management**

**Email: [mva.grants@alaska.gov](mailto:mva.grants@alaska.gov)**

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

## Signatory Authority Form

<b>Grant Program(s):</b> State and Local Cybersecurity Grant Program		<b>Effective Date</b>	
<b>UEI #</b>	QRK7LJ2Y3RJ1	<b>Tax ID#</b>	92-0030816
<b>Name of Applicant (Jurisdiction):</b> Matanuska-Susitna Borough			
<b>Signatory Information</b>			
<i>Project Manager, Chief Financial Officer, and Signatory Official must be three (3) different individuals.</i>			
	<i>Primary Signatories: Grant Award/Amendments and Quarterly Grant Reports</i>	<i>Primary Delegations: Quarterly Financial and Narrative Grant Reports (only)</i>	<i>Secondary Delegations: Quarterly Financial and Narrative Grant Reports (only)</i>
<b>Project Manager Name</b> <i>Individual who will manage project</i>	Dan Monarch	Leah Jones	
<b>Project Manager Address</b> City, State Zip	350 E. Dahlia Ave Palmer AK 99645	350 E. Dahlia Ave Palmer AK 99645	
<b>Project Manager Telephone</b>	1-907-861-8558	1-907-861-8570	
<b>Project Manager Email</b>	dan.monarch@matsugov.us	leah.jones@matsugov.us	
<b>Chief Financial Officer Name</b> <i>Highest level financial officer, authorized to certify financial expenditures and records</i>	Cheyenne Heindel	Liesel Weiland	Tonya Loyer
<b>Chief Financial Officer Address</b> City, State Zip	350 E. Dahlia Ave Palmer AK 99645	350 E. Dahlia Ave Palmer AK 99645	350 E. Dahlia Ave Palmer AK 99645
<b>Chief Financial Officer Telephone</b>	907-861-8630	907-861-8624	907-861-8585
<b>Chief Financial Officer Email</b>	cheyenne.heindel@matsugov.us	liesel.weiland@matsugov.us	tonya.loyer@matsugov.us
<b>Signatory Official Name</b> <i>Jurisdiction's Chief Executive Governing Official</i>	Michael Brown	George Hays	
<b>Signatory Official Address</b> City, State Zip	350 E. Dahlia Ave Palmer AK 99645	350 E. Dahlia Ave Palmer AK 99645	
<b>Signatory Official Telephone</b>	907-861-8689	907-861-8405	
<b>Signatory Official Email</b>	mike.brown@matsugov.us	george.hays@matsugov.us	
Grant Correspondence such as award documents and payment notifications will be sent to primary delegates. If you would like additional contacts cc'd in the email please list them below and provide email address if not listed above.			
Pamela Graham, Grants Coordinator - <a href="mailto:pamela.graham@matsugov.us">pamela.graham@matsugov.us</a>			
<b>Signatures**</b>			
<i>**Signature required by each of the above named individuals.</i>			
<b>Project Manager</b>			
	<i>Primary Signatory</i>	<i>Primary Delegate</i>	<i>Secondary Delegate</i>
<b>Chief Financial Officer</b>			
	<i>Primary Signatory</i>	<i>Primary Delegate</i>	<i>Secondary Delegate</i>
<b>Signatory Official</b>			
	<i>Primary Signatory</i>	<i>Primary Delegate</i>	<i>Secondary Delegate</i>