City of Billings

Prepared by City of Billings
for Montana Disaster and Emergency Services FY24 Homeland Security

Primary Contact: Ted Wilson

Opportunity Details

Opportunity Information

Title

FY24 Homeland Security

Description

IMPORTANT

Please review and follow the State Homeland Security Program (SHSP) grant guidance document. FEMA/DHS expects all grant recipients and subrecipients to utilize the State Homeland Security Program (SHSP) grant funding to address the high priority-low capacity core capabilities. SHSP provides financial support to build and deliver core capabilities that improve the ability of jurisdictions to prepare for and prevent terrorism and other catastrophic events.

The Grant Program Guidance document provides information on the top priorities for the coming years SHSP project applications. The State of Montana solicits projects that will measurably improve these high priority-low capacity capabilities and increase our resiliency all across the State.

Overview

The purpose of this fiscal year's SHSP is to support state and local efforts to prevent terrorism and other terrorist related catastrophic events and to prepare the nation for the threats and hazards that pose the greatest risk to the security of the United States. This year's SHSP provides funding to implement investments that build, sustain, and deliver the 32 core capabilities essential to achieving the national preparedness goal of a secure and resilient nation. The building, sustainment, and delivery of these core capabilities are not exclusive to any single level of government, organization, or community, but rather, require the combined effort of the whole community, inclusive of children, individuals with disabilities and other with access and functional needs, diverse communities, and people with limited English proficiency. This year's SHSP supports the core capabilities across the five mission areas of Prevention, Protection, Mitigation, Response, and Recovery based on allowable costs.

• Prevent a threatened or an actual act of terrorism;

• Protect citizens, residents, visitors, and assets against the greatest threats that pose the greatest risk to the security of the United States;

• Mitigate the loss of life and property by lessening the impact of future catastrophic events caused by terrorism;

• Respond quickly to save lives, protect property and the environment, and meet basic human needs in the aftermath of a catastrophic incident caused by terrorism;

• Recover through a focus on the timely restoration, strengthening, accessibility and revitalization of infrastructure, housing, and a sustainable economy, as well as the health, social, cultural, historic, and environmental fabric of communities affected by a catastrophic incident caused by terrorism; and do so in a manner that engages the whole community while ensuring the protection of civil rights.

Awarding Agency Name

Montana Disaster and Emergency Services

Agency Contact Name

Amanda Avard

Agency Contact Phone

406-324-4777

Agency Contact Email

mtdesprep@mt.gov

Fund Activity Categories

Disaster Prevention and Relief

Category Explanation

Departments
Montana Disaster and Emergency Services

Subjects
HS

Opportunity Manager
Amanda Avard

Opportunity Posted Date
1/3/2024

Opportunity Archive Date

Announcement Type
Initial Announcement

Funding Opportunity Number

Agency Opportunity Number

Assistance Listings Number

Public Link
https://mt.amplifund.com/Public/Opportunities/Details/b6c805b5-ec3f-4a91-87d6-849978d6d88e

Is Published
Yes

Funding Information

Total Program Funding
$0.00

Funding Sources
Federal Or Federal Pass Through

Funding Source Description

Funding Restrictions

Award Information

Award Period
Ends 09/30/2025

Award Announcement Date
9/4/2024

Award Type
Competitive

Capital Grant
No

Indirect Costs Allowed

Yes

Restrictions on Indirect Costs

Yes

Matching Requirement

No

Submission Information

Submission Window

01/03/2024 8:00 AM - 03/16/2024 5:59 AM

Submission Timeline Type

One Time

Submission Timeline Additional Information

No more than 3 applications from a jurisdictional area will be considered under the competitive pool. Senior Advisory Committee (SAC) approved regional projects and Combating Domestic Violence Extremism projects are not counted against the 3 projects.

Allow Multiple Applications

Yes

Application Review Start Date / Pre-Qualification Deadline

03/18/2024 12:00 AM

Question Submission Information

Attachments

- AmpliFund Applicant Portal Guide for SHSP
- FY24 SHSP State Guidance Jan 2024

Eligibility Information

Eligibility Type

Public

Eligible Applicants

- State Governments
- County Governments
- City or township governments
- Public and State controlled institutions of higher education
- Native American tribal governments (Federally recognized)

Additional Eligibility Information

Nonprofits who provide services to a local government agency may also submit applications. A local jurisdiction may act as a host on behalf of an entity, including non-profits and associations, to address critical needs.

Additional Information

Additional Information URL

https://des.mt.gov/Grant-Programs/State-Homeland-Security-Grants

Award Administration Information

State Award Notices

This is a competitive state grant, and there are often more funding requests than funding available. The State Homeland Security Advisor will make the final decision on projects to be included in the state application to FEMA in late spring. All applicants will be informed as to the status of their projects after the state application has been submitted. Please note - project period of performance will not begin until 10/1/2024.

Administrative and National Policy Requirements

We anticipate that the national priorities from last year will remain the same. Updated information will be provided when the Notice of Funding Opportunity is released, typically around February.

State Awarding Agency Contacts

State Awarding Agency Contacts
Amanda Avard - State Authorized Representative

Pam Fruh
Pam.Fruh@mt.gov
406-439-5917

Sarah Harmon
SarahHarmon@mt.gov
406-417-9354

Project Information

Application Information

Application Name
City of Billings

Award Requested
$90,000.00

Total Award Budget
$90,000.00

Primary Contact Information

Name
Ted Wilson

Email Address
wilsont@billingsmt.gov

Address
PO Box 1178
Billings, Montana 59103-1178

Phone Number
(406) 869-3997

Project Description

SHSP Overview

Jurisdiction/Agency Information

Entity Name
City of Billings

Entity Street Address
PO Box 1178

Entity City
Billings

Entity State
Montana

Entity Zip
59103-1178

Principal Elected Official (PEO) or Commissioner Information

The PEO or Commissioner listed has been informed of the submission of this grant and may receive notices about reports submitted by the Authorized Representative.

Name of PEO or Commissioner
Bill Cole

Title
Mayor

PEO Email Address
coleb@billingsmt.gov

PEO Phone Number (xxx-xxx-xxxx)
406657-8296

Project Manager (Authorized Representative)

Project Manager First Name
David

Project Manager Last Name
Watterson

Project Manager Phone Number (xxx-xxx-xxxx)
406-657-8330

Project Manager Email Address
wattersond@billingsmt.gov

Project Manager Street Address
PO Box 1178

Project Manager City

Billings

Project Manager State
MT

Project Manager Zip
59103-1178

Fiscal Officer / Agent Information

Fiscal Officer Name
Andy Zoeller

Title
Finance Director

Organization
City of Billings

Fiscal Officer Telephone Number (xxx-xxx-xxxx)
406-657-8209

Fiscal Officer Email Address
zoellera@billingsmt.gov

Administrative

Organization Type
- ○ County Government
- ○ Tribal Government
- ◉ Local/City Government
- ○ State Government
- ○ Other Non-Profit Entity

UEI Number

Provide your valid Unique Entity Identification (UEI) number. This is NOT your Employer Identification Number (EIN).

Please be aware that the federal government has discontinued use of the Data Universal Number System (DUNS). The Unique Entity Identification (UEI) number is now the required means of entity identification for federal awards government-wide. ***If you are registered in SAM.gov, you've already been assigned a new UEI. It's viewable in your SAM.gov entity registration record. If you do not know your UEI number, ask your local clerk and recorder or finance person, they will typically have that information. Refer to the link provided for more information regarding this update and how to obtain a UEI number.*** ***Click Here for Unique Entity Identifier Update Information***

Applicant's Unique Entity Identification (UEI) Number (UEI is a 12 digit number with a combination of letters and numbers)
FAEFYK4YL4M1

Applicant Assessment

Fiscal Assessment

Has applicant organization substantially changed their financial management and/or grant administration systems in the last 24 months?

- ○ Yes
- ◉ No

Does applicant organization's fiscal officer maintain written policies and procedures regarding the operation of all financial management systems?

- ◉ Yes
- ○ No

Has applicant organization received federal awards directly from a Federal Awarding agency over the last 24 months?

- ◉ Yes
- ○ No

If yes to above, list the grant name, year(s) received and awarding agency name. If there are to many to list enter the most recent 5.

RAISE, 2022, Department of Transportation; Operating Subsidy Grant, 2023, Department of Housing and Urban Development; Community Development Block Grant, 2023, Department of Housing and Urban Development; Home Investment Partnerships Program, 2023, Department of Housing and Urban Development; Treatment Court, 2021, Department of Justice; Public Housing Operating Fund, 2020, Department of Housing and Urban Development.

Has the applicant organization applied for any other grant funding to support the project that is being submitted?

- ○ Yes
- ◉ No

Have there been any audit/financial findings for your organization within the last 24 months?

- ○ Yes
- ◉ No

Procurement Procedures

For non-state agencies, does your jurisdiction have a locally written and approved procurement policy?

- ◉ Yes
- ○ No
- ○ N/A - State Agency

If yes to above, please upload your local procurement policy (if applicable)

AO149 Purchasing Procedures.pdf

Conflict of Interest

Does the jurisdiction have a potential or real conflict of interest?

- ○ Yes
- ◉ No

Non-Tax Revenue Source

Does this project fall under a program that is supported by a non-tax revenue source (i.e. enterprise fund)?

- ○ Yes
- ◉ No

If "YES", additional information may be required on the project.

Indirect Cost Rate Documents - Only fill this section out if applicable for your organization.

Indirect Cost Rate Proposal

Indirect Cost Allocation Plan

Indirect Cost Certification

Project Information

Instructions

APPLICATIONS ARE DUE NO LATER THAN 11:59PM FRIDAY, MARCH 15, 2024.
Applicants are not guaranteed to receive funding even if the project falls within a state or national priority.

To qualify as a single project, all parts of the project must be integral towards achieving one precise objective. If additional items are included in the project that do not support the primary objective, they may be removed from the project application.

Scoring Criteria

Attachment E - Criteria with Standard issue Section.pdf

PROJECT

Please include your entity name in the Project Title. For example: County ABC Warning System.

Project Title

City of Billings Cyber Security Enhancement Internal Assessment and Response

CORE CAPABILITIES

Please use the drop-down box to select the core capability the project supports. Applicants must show justification as to how the project supports the core capability. Definitions of the core capabilities are attached below.

Core Capabilities Definitions

Attachment F - CC Definitions.pdf

Select the Primary Core Capability

Make your selection from the drop-down box below

Cyber Security

NATIONAL PRIORITIES

Please use the drop-down box to select the national priority the project supports. If your project does not support a national priority please select "Not a National Priority". Definitions of the national priorities are attached below.

National Priorities Definitions

Attachment C - National Priorities.pdf

Select the National Priority

Make your selection from the drop-down box below.

Enhancing Cybersecurity

ENVIRONMENTAL AND HISTORICAL PRESERVATION (EHP)

Projects that have the potential to impact the environment and/or historic properties, including but not limited to construction of communication towers or repeaters, modification or renovation of existing buildings, structures, or facilities, updating electrical wiring, or new construction including replacement of facilities, or sonar equipment must participate in the DHS/FEMA Environmental and Historic Preservation (EHP) review process. If you have questions regarding EHP please contact MT DES Grant Section.

Does this project require EHP Approval?

- ○ Yes
- ◉ No

Local Emergency Planning Committees (LEPC) Project Priority Letter

LEPC Project Priority Letter Template

Attachment G - LEPC Project Priority Letter Template.docx

Please attach a signed LEPC project priority letter, required for SHSP sub-recipients. This is not required for state agencies as the governor and HSA prioritize state applications. SAC approved regional projects and National Priority - Combating Domestic Violence Extremism projects do not count against the 3-project limit.

LEPC Project Priority Letter

Project Information

Please provide a detailed explanation of the project including how the project supports the priority selected and any identified gaps it addresses. Describe how this project would prevent, protect, or reduce the impact to the community population from terrorism.

Remember that individuals from various disciplines will be reading this application so spell out acronyms, use plain language and avoid technical jargon.

Project Narrative

The City of Billings has identified a need for improved cybersecurity policies and procedures to protect our networks, data, and IT services from unauthorized use or exploitation. We are requesting grant funding for cybersecurity experts to perform an objective external cybersecurity risk assessment, develop a security roadmap, and to provide support to our organization from a strategic cybersecurity expert to guide us in the implementation of the recommendations identified and outlined throughout the process.

The project will consist of three major phases: a cybersecurity risk assessment, development of a security roadmap, and mitigation of the risks identified in the assessment through policy development, enhancing procedures, system and structural changes to mitigate identified risks, and identifying areas requiring additional investments. Throughout the project and beyond, the City of Billings is committed to providing staffing resources from the entire IT staff including the Network/Security Team and the full resources of our IT Security Engineer. Post-project the city is committed to internally funding resource acquisition (hardware/software/services), ongoing internal and external penetration (PEN) testing, and periodic cybersecurity policy/procedure review.

The risk assessment is the initial major phase. We will require the risk assessment to be based around the standards and best practices established by the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS) Critical Controls. The risk assessment will establish a baseline for our current cybersecurity posture so that we can build a functioning, measurable security strategy based on nationally accepted industry standards. The assessment of our environment will focus on the identification of existing vulnerabilities and the documentation of best

practice and standards compliance or non-compliance. Specific areas of investigation will include:

Administrative Controls: End-user and departmental appropriate use standards, end-user security awareness, risk management, policy relevance, policy enforcement, endpoint compliance scanning, patching and update procedures, resource access auditing, backup, archive, and retention.

Technical Controls: Perimeter security (firewalls, log management and analysis), multi-factor authentication, pen-testing, VPN access, contract/vendor remote access auditing, and web application development.

Physical Controls: Physical access restrictions to communications, computer and storage equipment, surveillance and access audit for high security areas, signage for equipment areas proximate to publicly accessible areas.

The next major phase will be the development of a Security Roadmap: Once we have a clear understanding of our current risk and deviations from best practices, the next step is to determine how to move forward. We need to define what tasks require attention, assign a priority for each task, and determine who will take on each task. This will include participation by contract information security consultant(s), city officials, external security partners, and IT staff. The decisions made in this phase would address the deficiencies documented in the assessment phase. The foundational work product will be formal policy documents adopted by our city council.

The final major phase of the project will be to leverage the professional services of a cybersecurity expert to assist and guide us as we address the technical planning and process issues identified by the previous stages. Major components of this phase will include documenting new or improved processes, managing the organization and employee change process, update of the security roadmap as we progress, answer questions concerning compliance with regulatory & best practices, enhanced incident response plans for scenarios including malicious and natural events as well as identification, and prioritization of post-project funding requirements for improving our prevention and recovery abilities. The City of Billings has committed to funding regular external network penetration (PEN) testing to identify new or developing risks, maintain awareness and manage existing risks, and to document mitigation of known risks eliminated by our efforts. We plan to further utilize the expertise of a cybersecurity expert to review the results of our PEN tests and provide analytical and strategic advice on how to address identified risks through policy, procedure, updates to our Security Roadmap, and/or future investments.

Though this project is primarily involved with cyber security it also addresses several of Montana' s State Homeland Security Program Core Capabilities priorities. For example, the development of administrative controls and IR/DR plans are consistent with the goals described in the planning priority. Physical, internal, and external controls speak to several of the core capabilities including interdiction, detection, and access control.

Please attach supporting documentation like AAR that points directly to the identified gap being addressed.

Identified Gap Supporting Document(s)

iv.pdf, pentest.pdf, exec-summary-report.pdf

Please provide a detailed explanation of the project objective(s) and desired measureable outcome(s). The objective(s) of this project should be clear and realistic, with clearly defined and quantified project benefits. The project should reflect specific, measurable, achievable, relevant, and time-bound (SMART) objectives that directly contribute to the achievement of the project goals.

Project Objective/Outcome

The primary goal of this project is to improve our ability to protect and recover city IT data and resources over the long term. To accomplish this goal IT needs to communicate the security issues, solutions and potential costs to our departmental leadership team, city administration, and city officials. By committing to an independent risk assessment based on nationally accepted industry security standards of where we are and developing a clear roadmap for how to move forward, we can present this information to key stakeholders and provide invaluable periodic updates on our progress and current environment. It is our intention to involve a wide spectrum of city decision-makers, end-users, and City Council to ensure a consensus buy-in to the project goals and commitment to funding post-project costs.

Our risk assessment will include professional evaluation of our bi-annual external network penetration (PEN) testing based on the Penetration Testing Execution Standard (PTES) and adjustment of our security roadmap to address and prioritize mitigation of identified risks.

City Council will adopt revised IT cybersecurity policies as identified by the policy committee within one year of the initial system scan and roadmap development. IT and administration will implement policies adopted by Council. IT will implement policies within 90 days of adoption.

The outcome of this project will be a non-biased picture of our current cybersecurity posture followed by the development of enhanced policies and procedures and a security roadmap to formally identify what needs to be done, by whom, and when. IT will adopt the new policies and procedures, actively address risks and exposures identified throughout this project, and utilize the new security roadmap to advance our overall cybersecurity today and into the future.

Multi-Jurisdictional Impact and Support

Please explain the impact this project will have on other entities or jurisdictions. What elements within the project scope may be shared, deployed, or utilized by other entities or jurisdictions?

Impact Narrative

The city shares information with a variety of local, state, and federal agencies. We also provide ownership, taxation, permitting, planning, and GIS data to local, regional, and national private entities such as banks, mortgage brokers, real estate appraisers, contractors, developers, and title companies. Improving our security policies and procedures will include documenting the types of information that will be shared, approved sources and destinations, and the means by which data is transmitted and received. This in turn will provide better security for all parties by ensuring the provenance and accuracy of shared data. For our CJIS partners meeting required standards and practices will allow city and non-city public safety services to continue to share timely and accurate information.

Please attach any signed letters demonstrating support from other entities or contiguous jurisdictions.

Letter of Support Template
Attachment D - Letter of Support Template.docx

Letter of Support 1
Judge Kolar LOS.pdf

Letter of Support 2
Billings Cybersecurity LOS Chamber.pdf

Letter of Support 3
2024 City of Billings Cybersecurity BSED.pdf

Letter of Support 4
City of Billings LOS from Yellowstone County.pdf

Letter of Support 5
Combined City LOS.pdf

Resource Availability

Please provide information on the availability of this resource, training, or equipment from a contiguous jurisdiction. If the project duplicates a resource, training, or equipment currently available from a contiguous jurisdiction, please provide justification as to why this project is necessary.

Resource Availability

The City of Billings has unique statutory and regulatory responsibilities to deliver services and information to our residents, as well as public and private entities. The city is accountable and liable for the security of the information systems that store and communicate the data we are tasked to maintain, no matter who owns and operates the systems. Our own staff needs to be trained, and our own organization needs to have policies and procedures in place to protect our data and systems. We cannot cede this responsibility to another jurisdiction - nor would another jurisdiction wish to take it on.

Maintenance, Support, and Sustainment Plan

Provide detailed information on how the project will be maintained, supported, and sustained following the cessation of federal funding.

Maintenance, Sustainment, and Support Plan

The City of Billings Information and Technology Department has existing staffing, including a full-time IT security engineer, that are focused on the daily ongoing protection of our network and critical data. They are committed to engaging in this project, the ongoing support of the assessment and development of the security roadmap, to the development of our policies and procedures, and to leveraging the outcomes to strengthen our overall cybersecurity organizational health for years to come.

By engaging city leadership throughout the project, we will be able to demonstrate the compliance and operational cyber security deficiencies that face the city now as well as inform them of the potential costs of not addressing these deficiencies. Also, by providing a planning and prioritization framework we can provide a normalized capex and maintenance schedule over a three to five-year fiscal horizon. Historically our City Council has been very responsive to supporting budget requests related to mitigating risks on IT operations. We are confident that post-project funding will be available to accomplish our mid- to long-term goals.

Budget

Proposed Budget Summary

Expense Budget

	Grant Funded	Total Budgeted
Consultants/Contracts		
Cybersecurity Risk Assessment, Security Roadmap Development, and Consulting Services/Implementation	$90,000.00	$90,000.00
Subtotal	**$90,000.00**	**$90,000.00**
Total Proposed Cost	**$90,000.00**	**$90,000.00**

Revenue Budget

	Grant Funded	Total Budgeted
Grant Funding		
Award Requested	$90,000.00	$90,000.00
Subtotal	**$90,000.00**	**$90,000.00**
Total Proposed Revenue	**$90,000.00**	**$90,000.00**

Proposed Budget Detail

See attached spreadsheet.

Proposed Budget Narrative

Consultants/Contracts

Include specifics in the narrative section

Cybersecurity Risk Assessment, Security Roadmap Development, and Consulting Services/Implementation

The City will follow its procedures for soliciting and approving contracts in order to complete a full risk assessment of IT systems security, development of a security roadmap, and engage the services of a cybersecurity consultant to aide in the implementation of enhanced policy, new and refined procedures, review of external & internal PEN tests, and identifying future investments. Our request is based on a quote provided by a local firm in which one year costs are estimated to be $73,500 for assessment tasks, $10,920 for roadmap development, and $6,000 for consulting services, plus additional room for inflation and projected actual costs when the project goes out to bid.

Performance Plan

Proposed Performance Plan

Quarter 1 - 10/1/24 to 12/31/24

Goal Name	Goal Type	Goal Details
Recruit Cybersecurity Committee Members	Milestone	Due Date 12/20/2024
Contract Services	Milestone	Due Date 12/31/2024
Initiate Full Security Risk Assessment	Milestone	Due Date 12/31/2024

Quarter 2 - 1/1/25 to 3/31/25

Goal Name	Goal Type	Goal Details
Develop Roadmap	Milestone	Due Date 03/31/2025
Cybersecurity Committee Meets	Milestone	Due Date 03/31/2025

Quarter 3 - 4/1/25 to 6/30/25

Goal Name	Goal Type	Goal Details
Policy Formulation and Risk Mitigation Planning	Milestone	Due Date 06/27/2025

Quarter 4 - 7/1/25 to 9/30/25

Goal Name	Goal Type	Goal Details
IT Procedure Documentation, Post-project Goal Prioritization, Policy Implementation, and Review	Milestone	Due Date 09/30/2025

Quarter 5 - 10/1/25 to 12/31/25

Goal Name	Goal Type	Goal Details
Post-project Assessments, Project Closeout	Milestone	Due Date 12/31/2025

Proposed Performance Narrative

Quarter 1 - 10/1/24 to 12/31/24

Please provide goals or milestones to account for anticipated project activities being accomplished during the first quarter.

Recruit Cybersecurity Committee Members

Put together a cybersecurity committee from city leadership, external security partners, contractor, and IT staff.

Contract Services

Follow procurement guidelines to secure contract services.

Initiate Full Security Risk Assessment

Initiate security risk assessment process, including pre-project internal and external pen testing.

Quarter 2 - 1/1/25 to 3/31/25

Please provide goals or milestones to account for anticipated project activities being accomplished during the second quarter.

Develop Roadmap

Develop a security roadmap to determine how to address identified risks, determine who will own the execution of those decisions, and when to act.

Cybersecurity Committee Meets

Cybersecurity committee meets to review assessment results and review roadmap proposed by contractor.

Quarter 3 - 4/1/25 to 6/30/25

Please provide goals or milestones to account for anticipated project activities being accomplished during the third quarter.

Policy Formulation and Risk Mitigation Planning

Work on policy recommendations and adoption. Implement risk mitigation based on roadmap. Update City Council on risk assessment results, developing policies, and additional steps being taken to address identified risks.

Quarter 4 - 7/1/25 to 9/30/25

Please provide goals or milestones to account for anticipated project activities being accomplished during the fourth quarter.

IT Procedure Documentation, Post-project Goal Prioritization, Policy Implementation, and Review

Document enhanced IT security procedures and roadmap. Create multi-year budget projections for hardware, software, and services related to the risks identified by this project and priorities assigned in the roadmap.

Quarter 5 - 10/1/25 to 12/31/25

Please provide goals or milestones to account for anticipated project activities being accomplished during the fifth quarter.

Post-project Assessments, Project Closeout

Conduct internal and external pen tests to evaluate post-project system vulnerability improvements. Perform project closeout activities.