RESOLUTION NO.

A RESOLUTION AUTHORIZING THE RATIFIED SUBMISSION OF A GRANT APPLICATION TO THE WYOMING OFFICE OF HOMELAND SECURITY FOR THE FFY 2022 STATE HOMELAND SECURITY GRANT PROGRAM (SHSP), ON BEHALF OF THE GOVERNING BODY OF LARAMIE COUNTY, WYOMING TO REQUEST FUNDING FOR THE LARAMIE COUNTY INFORMATION TECHNOLOGY DEPARTMENT IN THE AMOUNT OF $80,000.

FOR THE PURPOSE OF: REQUESTED FUNDS WILL BE USED FOR THE PURCHASE OF TWO WEB APPLICATION FIREWALLS FOR CYBERSECURITY.

WITNESSETH

WHEREAS, the Wyoming Office of Homeland Security receives FFY 2022 SHSP funds from the Federal Emergency Management Agency and;

WHEREAS, the Wyoming Office of Homeland Security distributes a portion of these FFY 2022 SHSP funds to Wyoming Counties and;

WHEREAS, the Laramie County Board of Commissioners is eligible to apply for and receive FFY 2022 SHSP funds for the Laramie County Information Technology Department and;

WHEREAS, the Governing Body of Laramie County desires to participate in the Wyoming Office of Homeland Security Grant Program (SHSP) by sponsoring this grant application to assist in financing the Information Technology Department; and

WHEREAS, the Governing Body of Laramie County has been provided with preliminary cost estimates and information on this project; and

NOW, THEREFORE, BE IT RESOLVED BY THE GOVERNING BODY OF LARAMIE COUNTY that a grant application for $80,000 be submitted to the Wyoming Office of Homeland Security for consideration of assistance in funding the Laramie County Information Technology Department under the FFY 2022 SHSP grant program.

BE IT FURTHER RESOLVED, that Sandra Newland, or her successor in the position of Laramie County Grants Manager, is appointed as agent of the Laramie County Board of Commissioners to execute and submit applications and certifications for these funds and to receive funds and implement the programs funded under this grant.

PASSED, APPROVED AND ADOPTED THIS 17th DAY OF MAY 2022.

By: _____ Date: _____

Troy Thompson, Chairman

ATTEST:

_____ Date: _____

Debra Lee, Laramie County Clerk

Received and Approved as to Form only By:

_____ Date: 5/4/22

Laramie County Attorney's Office

Wyoming Office of Homeland Security

FY 2022 SHSP
Deadline: 5/6/2022

310 W. 19th Street, Suite 300

Cybersecurity

Jump to: Application Questions Budget Documents

USD$ 80,000.00 Requested

Submitted: 5/2/2022 8:36:06 AM (Pacific)

Project Contact
Sandra Newland
sandra.newland@laramiecountywy.gov
Tel: 307-633-4201

Additional Contacts
brad.alexander@laramiecountywy.gov

310 W. 19th Street, Suite 300

310 W 19th St Ste 300
Cheyenne, WY 82001
United States

Chairman
Troy Thompson
commissioners@laramiecountywy.gov

Telephone	307-633-4260
Fax	
Web	laramiecountywy.gov
EIN	83-600111
UEI	E9DLJC1HGNQ8
SAM Expires	12/27/2022

Application Questions top

Project Details

1. Type of Jurisdiction

- ☐ County Emergency Management
- ☐ Law Enforcement
- ☐ Coroner
- ☐ RERT
- ☐ Bomb Team
- ☐ School District
- ☐ State Agency
- ☐ Special District
- ☐ City/Town
- ✔ Other: County

2. Please provide your Unique Entity ID (SAM UEI number)
This takes the place of your DUNS number effective April 4, 2022.
E9DLJC1HGNQ8

3. Please describe "What" your need is and "Why" you need it.
Laramie County and our IT department is requesting funding for two, web application firewalls for cybersecurity. These would act as a high availability pair in case of failure or attack on our system. These reverse proxies protect our outside/public facing websites including GIS mapping for public safety and elections, along with other services. Our current solution is being pushed to capacity and no longer meets our needs for current cybersecurity standards. Our existing solution is also not a high availability pair, so if it goes offline then our critical services also go offline. The requested firewalls would identify and block all unwanted traffic to include potential terrorist threats to county government. A proper firewall system is essential for protecting Laramie County security.

4. List your AEL Codes here. REQUIRED for all equipment requests. The AEL is available at http://www.fema.gov/authorized-equipment-list.

Some equipment items require prior approval before the obligation or purchase of the items. Please reference the grant notes for each equipment item to ensure prior approval is not required.
05NP-00-FWAL Firewall, Network (copy of AEL printout attached).

5. Does this project require new construction, renovation, retrofitting or modifications of an existing structure?
Are you drilling holes in walls, turning dirt or modifying an existing structure in any way?
☐ YES - An EHP may be required
✔ NO

6. Does the requested funding cover all components of the project?
✔ YES
☐ NO

7. Will you accept partial funding?
✔ YES
☐ NO, explain:

8. Have you applied for other grant opportunities to fund this request?
If yes, please name what other grants have been applied for, the amount of funding received and what portion of the project the funding was for.
No, we currently do not have any other grant requests for this cybersecurity measure.

9. Does this project support a previous SHSP award?
☐ YES
✔ NO

10. ** If you answered YES to number 9, please answer: (a) what previous year; (b) the project name; and (c) the last completed milestone. ** If you answered NO, please put N/A.
N/A

11. Is this project part of a multi-year strategy? If YES, please explain. Otherwise, put NO.
No, but Laramie County is always looking to increase our security. This project would be part of a multiyear refresh for all of our primary security appliances through the Laramie County IT Department, but not part of a multi-year strategy for funding purposes.

12. Did you or your jurisdiction participate in the THIRA?
✔ YES
☐ NO

13. Does this project address gaps identified in the THIRA/SPR?
✔ YES
☐ NO

14. If YES to #13, explain how this project ties into your THIRA/SPR and how it addresses the gap. If NO, explain what other assessments, exercises or real world events identified the gap being addressed.
(For example: cyber/physical security assessment)
Cybersecurity and secure networks are a continuing concern that has been identified in our THIRA. Our cybersecurity project will protect county systems to include information and services as outlined in the priority investment. The firewalls will allow sensitive information to be secure from damage, unauthorized use and exploitation along with providing protection from all hazards. Having a robust firewall system addresses many sections of the THIRA/SPR as several agencies use our systems (law enforcement, EMA & health department). Several specific areas of the THIRA/SPR are addressed including; planning, public information and warning, operational coordination, operational communications, health and social services, intelligence and information sharing, access control & identity verification, cybersecurity, and threats and hazards identification. The cybersecurity project ties into the mission area of providing protection for Laramie County's critical data.

Securing Laramie County data is one of the most important job functions that I.T. does, and is considered the highest of our priorities. Backups and data/resource availability is listed in the Laramie County Emergency Response Plan and the Laramie County Cyber Security Plan as being a critical aspect of cyber/emergency readiness. Firewall protection have also been identified in several roundtables, as the best recovery option for terrorist and cyber-attacks within Laramie County.

15. All projects under this grant must have a nexus to terrorism. Please describe how your project relates to acts of terrorism.
Cyber-attacks are their own form of terrorism and cybersecurity is critical to protecting county government operations. Our county houses several essential partners to include law enforcement, EMA, elected officials, and the health department. Our county is active in coordinating events with the city and state and we act as partners in response operations. A key component of being able to mitigate a terrorist threat is a robust cybersecurity system to protect critical information and systems to allow a comprehensive and timely response.

16. Provide justification on how the project will be maintained, supported, and sustained.
Our cybersecurity project will be supported, maintained and sustained by Laramie County if funded. Once purchased the annual maintenance of the firewalls will be included into the fiscal I.T. budget for on-going maintenance. Once implemented the project will save the county money and time and provide state of the art security for the sensitive data of Laramie County and its partnering agencies.

17. Select your Primary core capability
See Core Capabilities Reference Document under Library Section above (select link to download)

- ☐ Planning
- ☐ Public Information and Warning
- ☐ Operational Coordination
- ☐ Intelligence
- ☐ Interdiction
- ☐ Screening, Search
- ☐ Access Control and Identity Verification
- ✔ Cybersecurity
- ☐ Physical Protective Measures
- ☐ Community Resilience
- ☐ Long-term Vulnerability Reduction
- ☐ Risk and Disaster Resilience Assessment
- ☐ Threats and Hazard Identification
- ☐ Infrastructure Systems
- ☐ Environmental Response/Health and Safety
- ☐ Fatality Management Services
- ☐ Logistics and Supply Chain Management
- ☐ On-Scene Security, Protection, and Law Enforcement
- ☐ Operational Communications
- ☐ Other:

18. Select your Secondary core capability (if applicable)
If not applicable, put NONE under Other

- ☐ Planning
- ☐ Public Information and Warning
- ☐ Operational Coordination
- ☐ Intelligence
- ☐ Interdiction
- ☐ Screening, Search
- ✔ Access Control and Identity Verification
- ☐ Cybersecurity
- ☐ Physical Protective Measures
- ☐ Community Resilience
- ☐ Long-term Vulnerability Reduction
- ☐ Risk and Disaster Resilience Assessment
- ☐ Threats and Hazard Identification
- ☐ Infrastructure Systems
- ☐ Environmental Response/Health and Safety
- ☐ Fatality Management Services
- ☐ Logistics and Supply Chain Management

- ☐ On-Scene Security, Protection, and Law Enforcement
- ☐ Operational Communications
- ☐ Other:

19. Select your Tertiary/Third core capability (if applicable)
If not applicable, put NONE under Other

- ☐ Planning
- ☐ Public Information and Warning
- ☐ Operational Coordination
- ☐ Intelligence
- ☐ Interdiction
- ☐ Screening, Search
- ☐ Access Control and Identity Verification
- ☐ Cybersecurity
- ☐ Physical Protective Measures
- ☐ Community Resilience
- ☐ Long-term Vulnerability Reduction
- ☐ Risk and Disaster Resilience Assessment
- ☐ Threats and Hazard Identification
- ☐ Infrastructure Systems
- ☐ Environmental Response/Health and Safety
- ☐ Fatality Management Services
- ☐ Logistics and Supply Chain Management
- ☐ On-Scene Security, Protection, and Law Enforcement
- ☐ Operational Communications
- ✔ Other: NONE

20. Does this investment focus on building new capabilities or sustaining existing capabilities?

- ☐ BUILD
- ✔ SUSTAIN

21. Is any part of this proposed project a deployable and/or shareable asset?
An asset that can be utilized as a local, state, regional, or national resource.

- ☐ YES
- ✔ NO

22. Does this project support a NIMS typed resource?
Resource typing is defining and categorizing, by capability, the resources requested, deployed and used in incidents. https://rtlt.preptoolkit.fema.gov/Public

- ☐ YES
- ✔ NO

Milestones

Submit a minimum of four (4) milestones for all projects. Milestones should represent a logical progression of the project to allow for realistic monitoring and management of grant funding. This attribute will function as a tool for measuring project progress in future reporting periods. Provide a high level narrative description of activities to occur within each milestone including anticipated milestone dates/timeframes.

---

23. First Milestone/Key Activity. Include your projected Start and End Dates.
Example: December 15, 2022 to December 15, 2023.
A grant award is expected to occur in October 2022. We will establish a budget and accounting line items to prepare for the funding. Upon award, the County will work to explore vendors to provide the needed web based firewall protection. We will follow the Laramie County Procurement Policies on purchasing this software. We anticipate this step will be completed by February 2023.

24. Second Milestone/Key Activity. Include your projected Start and End Dates.
Example: December 15, 2022 to December 15, 2023.

We anticipate have our vendors outlined in March of 2023 and we will be ready to move forward with the purchase. We are allowing three months for this process to run through May 31, 2023.

25. Third Milestone/Key Activity. Include your projected Start and End Dates.
Example: December 15, 2022 to December 15, 2023.
Beginning in June 2023, we anticipate coordinating with the selected vendor for installation and setup of the firewall systems. We are allowing up to three months for this process to allow for fluctuating installation and scheduling demands. We anticipate being completed with this milestone in September 2023.

26. Fourth Milestone/Key Activity. Include your projected Start and End Dates.
Example: December 15, 2022 to December 15, 2023.
Our final milestone will be to closeout and finalize all grant items with the Wyoming Office of Homeland Security. We anticipate this taking place in October-November 2023.

Additional Information

27. Provide any additional information about the project you would like us to consider.
You may upload a document if you need more space.
Thank you for your consideration.

Budget top

Funding Uses/Expenses	Amount Requested	Total Project Cost
Planning		USD$ 0.00
Organization	USD$ 80,000.00	USD$ 80,000.00
Exercise		USD$ 0.00
Training		USD$ 0.00
Equipment		USD$ 0.00
Total	**USD$ 80,000.00**	**USD$ 80,000.00**

Budget Narrative
We are requesting a total of $80,000 for the purchase of two web application firewalls to be implemented in Laramie County fire cybersecurity protection. Each firewall is approximately $40,000. Our County IT Department will lead the project and coordinate with the selected vendor for setup and installation. We are putting this request under the category of organization, as it is not really considered equipment, but more of an operations expense. This purchase falls within AEL 05NP-00-FWAL for a firewall network.

Documents top

Documents Requested *	Required?	Attached Documents *
		AEL

Extra

1 *-empty-*

2 *-empty-*

3 *-empty-*

4 *-empty-*

5 *-empty-*

6 *-empty-*

7 *-empty-*

8 *-empty-*

9 *-empty-*

10 *-empty-*

11 *-empty-*

12 *-empty-*

13 *-empty-*

14 *-empty-*

15 *-empty-*

16 *-empty-*

17 *-empty-*

18 *-empty-*

19 *-empty-*

20 *-empty-*

Application ID: 401899

Description:	Software for protection against viruses, spyware, and malicious code. May be obtained for individual hosts or for entire network segments.
Applicable Grant Programs:	BZPP , EMPG , EOC , IBSGP , LETPA-SHSP , LETPA-UASI , MMRS , OPSG , PSGP , PSIC , SHSP , THSGP , UASI
Grant Notes:	
Applicable Core Capabilities:	Environmental Response/Health and Safety , Intelligence and Information Sharing , Interdiction and Disruption , Mass Search and Rescue Operations , On-scene Security and Protection , Operational Communications , Operational Coordination , Physical Protective Measures , Planning , Public Health and Medical Services , Public Information and Warning , Public and Private Services and Resources , Screening , Search , and Detection

05HS-00-PFWL System, Personal Firewall

Description:	Personal firewall for operation on individual workstations. Usually a software solution, but appliances are also available.See also: 05NP-00-FWAL.
Applicable Grant Programs:	BZPP , DLSGP , EMPG , EOC , IBSGP , LETPA-SHSP , LETPA-UASI , MMRS , OPSG , PSGP , PSIC , SHSP , THSGP , UASI
Grant Notes:	
Applicable Core Capabilities:	Environmental Response/Health and Safety , Intelligence and Information Sharing , Interdiction and Disruption , Mass Search and Rescue Operations , On-scene Security and Protection , Operational Communications , Operational Coordination , Physical Protective Measures , Planning , Public Health and Medical Services , Public Information and Warning , Public and Private Services and Resources , Screening , Search , and Detection

(05NP) Network Level Security

(05NP-00) ...

05NP-00-FWAL Firewall, Network

Description:	Firewall (software or standalone appliance) for use in protecting networks. See also 05HS-00-PFWL.
Applicable Grant Programs:	BZPP , DLSGP , EMPG , EOC , IBSGP , LETPA-SHSP , LETPA-UASI , MMRS , OPSG , PSGP , PSIC , SHSP , THSGP , UASI
Grant Notes:	
Applicable Core Capabilities:	Environmental Response/Health and Safety , Intelligence and Information Sharing , Interdiction and Disruption , On-scene Security and Protection , Operational Communications , Operational Coordination , Physical Protective Measures , Public Health and Medical Services , Public Information and Warning , Public and Private Services and Resources , Screening , Search , and Detection

05NP-00-IDPS System, Intrusion Detection/Prevention

Description:	Intrusion Detection and/or Prevention System (IDS, IPS) deployed at either host or network level to detect and/or prevent unauthorized or aberrant behavior on the network. Software and hardware (appliance) solutions exist. This replaces item 05NP-00-IDS and incorporates more recent prevention technology.
Applicable Grant Programs:	BZPP , DLSGP , EMPG , EOC , IBSGP , LETPA-SHSP , LETPA-UASI , MMRS , OPSG , PSGP , PSIC , SHSP , THSGP , UASI
Grant Notes:	
Applicable Core Capabilities:	Environmental Response/Health and Safety , Intelligence and Information Sharing , Interdiction and Disruption , On-scene Security and Protection , Operational Communications , Operational Coordination , Physical Protective Measures , Public Health and Medical Services , Public Information and Warning , Public and Private Services and Resources , Screening , Search , and Detection

05NP-00-SCAN Tools, Network Vulnerability Scanning