

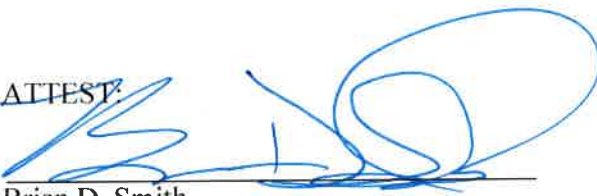
**HARDIN COUNTY FISCAL COURT
RESOLUTION NO. 2024-088**

BE IT RESOLVED, upon the recommendation of Judge/Executive Keith L. Taul, to approve the 2024 State Homeland Security Grant Program application and to authorize the Judge/Executive to sign all documents concerning the grant.

ADOPTED, by the Hardin County Fiscal Court in its regular meeting on 23 April 2024.



Keith L. Taul
Hardin County Judge/Executive

ATTEST:


Brian D. Smith
Hardin County Clerk

Guidance for Gap Identification – Threat, Vulnerability, and Consequences

DHS/FEMA requires states, territories, and Urban Areas to complete a Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) (formerly known as the State Preparedness Report) and prioritize grant funding to support closing capability gaps or sustaining capabilities identified in this process.

Threat: In considering threat, the applicant should discuss the potential for terroristic activity, domestic or international, faced by the community.

Vulnerabilities: In considering vulnerabilities, the applicant should discuss the community's susceptibility to destruction, incapacitation, or exploitation by a terroristic threat/attack.

Consequences: In considering potential consequences, the applicant should discuss potential negative effects on the community.

Threat/Hazard Selection

Select any Threat/Hazard from Kentucky's Strategic Preparedness Report that your proposed project could address:

- Active Shooter Cyber Attack CBRNE

Core Capability Selection

Select any primary Core Capability from FEMA's National Preparedness Goals that could be enhanced through your project's proposed solution:

- | | |
|--|---|
| <input type="checkbox"/> Access Control and Identity Verification | <input type="checkbox"/> Public Health, Healthcare and Emergency Medical Services |
| <input type="checkbox"/> Long Term Vulnerability Reduction | <input type="checkbox"/> Intelligence and Information Sharing |
| <input checked="" type="checkbox"/> Cybersecurity | <input type="checkbox"/> Screening, Search and Detection |
| <input type="checkbox"/> Mass Search and Rescue Operations | <input type="checkbox"/> Situational Assessment |
| <input type="checkbox"/> Infrastructure Systems | <input type="checkbox"/> Risk Management for Protection Programs and Activities |
| <input type="checkbox"/> Interdiction and Disruption | <input type="checkbox"/> Community Resilience |
| <input type="checkbox"/> Mass Care Services | <input type="checkbox"/> Risk and Disaster Resilience Assessment |
| <input type="checkbox"/> Threats and Hazards Identification | <input type="checkbox"/> Environmental Response/Health and Safety |
| <input type="checkbox"/> On-Scene Security, Protection and Law Enforcement | <input type="checkbox"/> Logistics and Supply Chain Management |
| <input type="checkbox"/> Operational Communications | |
| <input type="checkbox"/> Operational Coordination | |
| <input type="checkbox"/> Physical Protective Measures | |
| <input type="checkbox"/> Public Information and Warning | |



Include this Page in your Application

(A) Gap Identification
Page: 8

2024 HSGP Application Cover Sheet

Project # Mobile Protect and Device Management **E-Clearinghouse SAI#** KY202404110453
KWIEC Tracking # _____ **UEI #** P3ZAMPUAN2

Lead applicant agency Hardin County & Hardin County Jail
County Name: Hardin
Partnering Cities/Counties/Agencies _____

Organization: City County ADD Taxing District **Please provide:**
 School District _____ 25
Discipline: Law Enforcement Fire EMS State House District _____ 10
 HAZMAT Team EMA School District State Senate District _____
 Congressional District _____ 2
 Area Development District Lincoln Trail _____

Please choose the category and sub category below for which you are applying:

CATEGORY	SUB CATEGORIES
<input type="radio"/> Combating Domestic Violent Extremism	
<input type="radio"/> Community Preparedness & Resilience	
<input type="radio"/> Election Security	
<input type="radio"/> Emergency Medical Equipment	
<input type="radio"/> Emergency Communications	▶ Select One (if applicable) _____
<input type="radio"/> Soft Target/Crowded Places	▶ Select One (if applicable) _____
<input checked="" type="radio"/> Enhancing Cybersecurity	▶ Select One (if applicable) <u>Enhancing Cyber Security</u>
<input type="radio"/> Exercises & Training	

Funding Request: (Costs should match any requested vendor quotes. Local match must be subtracted from the subtotal and not included in the total amount of funding requested)

\$ \$61,300.00 **Total Funding Requested**

Who prepared this application?

Name Aaron Miller
Email amiller@hardincountyky.gov

	Authorizing Official	Project Manager	Financial Officer
Name	<u>Keith Taul</u>	<u>Aaron Miller</u>	<u>Lisa Pearman</u>
Title	<u>Judge Executive</u>	<u>IT Director</u>	<u>Treasurer</u>
Email	<u>ktaul@hardincountyky.gov</u>	<u>amiller@hardincountyky.gov</u>	<u>lpearman@hardincountyky.gov</u>



Include this Page in your Application

(B) Cover Sheet
Page: 10

Project Narrative

Describe the details of your project. Refer to the guidelines on Page 2 for guidance on information to include in the project description. Refer to key project description elements on Page 7 to complete your project narrative. **Please note:** Communications is the only funding category that requires project specific information. Add additional typed pages as needed. (Recommended: 1-3 pages)

Project Initiative

The convergence of terrorism and cyber threats presents a complex and evolving challenge for federal, state, and local governments throughout the United States. A terrorist organization, known for its sophisticated tactics and global reach, aims to carry out a large-scale cyber-attack against critical infrastructure targets in a large, populated area. The group seeks to maximize the impact of the attack, causing widespread disruption, economic damage, and fear among citizens. Cyberterrorism can target a wide range of entities, including government agencies, military organizations, critical infrastructure sectors (such as energy, transportation, finance, and healthcare), and individuals. The goal is to inflict damage, disrupt operations, or spread propaganda to achieve the terrorists' objectives. Governments, both State and Local employ various measures to prevent and mitigate cyberterrorism threats. These include enhancing cybersecurity defenses, conducting threat intelligence gathering and analysis, implementing incident response plans, promoting public awareness and education, and fostering international cooperation and information sharing. Hardin County and its knowledgeable staff seeks funding from the KOHS SHSGP 2024 State Homeland Security Grant Program in the amount of \$61,300.00 to enhance our cyber incident response in the new modern age of mobile users. This initiative aligns with the priorities outlined in the National Infrastructure Protection Plan and the National Cyber Incident Response Plan, which emphasize the importance of collaboration, information sharing, and coordinated response efforts to safeguard critical infrastructure against cyber threats.

Preventing/Preparing for/Protecting against

Utilizes artificial intelligence and machine learning algorithms to proactively detect and prevent malware, ransomware, and other cyber threats on mobile endpoints. Allows for a centralized control and management of mobile devices, enabling administrators to enforce security policies, device encryption, app whitelisting, and device lockdown. The proposed solution also Enables organizations to enforce security policies, conduct device inventory, and remotely wipe or lock devices in case of loss or theft. All the while providing real-time threat prevention and response capabilities to protect mobile endpoints from cyber-attacks, including zero-day exploits and fileless malware. Allowing Hardin County's Information Technology staff can establish a unified security framework in relation to NIST Cybersecurity Framework 2.0 (CSF) that extends across mobile devices, ensuring consistent protection against cyber terrorism threats regardless of the device's location or platform. This integration would enable us to strengthen our cybersecurity posture, mitigate the risk of cyber terrorism, and enhance their ability to prevent, prepare for, and protect against cyber threats across all mobile devices. By leveraging advanced threat prevention and management capabilities, effectively defending against cyber-attacks and safeguard critical assets and infrastructure from potential terrorist threats.

Multi-Agency Collaboration

A Unified Endpoint Manager (UEM) solution along with threat intelligence feeds to provide real-time information about emerging cyber threats and indicators of compromise. This will enable Hardin County mobile staff members to stay informed about potential terrorist activities and take the appropriate proactive measures to mitigate risks. Facilitate incident response planning by providing tools for remote device management, data wiping, and lockdown in case of lost or stolen devices. Developing procedures and testing to ensure readiness in the event of a security breach or terrorist incident. Ability to enforce encryption policies on mobile devices to protect sensitive data stored on the device or transmitted over the network. This helps safeguard government information from interception or unauthorized access by adversaries. Facilitate communication and coordination among government agencies during a crisis or terrorist incident. By providing secure channels for messaging and collaboration, UEM solutions help ensure that relevant stakeholders are informed and coordinated in their response efforts.



Include this Page in your Application

(C) Project Narrative
Page: 11

Project Narrative (Continued)

Budget Narrative

Hardin County Government Information Technology Department runs on a very well organized and thought-out budget for each fiscal year. Sustainable budget figures cost of all yearly services and software renewals. Because we were able to leverage cost savings with a particular software this fiscal year allows us to seek out new ways to add levels of security to workstations and mobile devices. Hardin County will be able to accommodate the required in-kind match. For continuing any software service, the IT Department will appropriate the necessary funding in future fiscal years' budgets.

Budget Planning

* Assessment and Planning - Assess current mobile device usage, security risks, and organizational needs.

* Licensing and Subscription Costs - Estimate the cost of UEM software licenses or subscription fees based on the number of devices to be managed and the desired feature set.

* Hardware and Infrastructure - Cloud-based Unified Endpoint Management solutions reduce the need for on-premises hardware and associated maintenance costs.

* Implementation and Integration - Require vendor to hold training sessions and supply needed documentation to ensure that IT staff are adequately trained to manage and support the solution effectively.

* Support and Maintenance - Estimate ongoing support and maintenance costs for the UEM solution, including software updates, patches, and technical support services.

* After Grant - Maintain highest level of security monitoring, mobile threat detection, app whitelisting, and containerization features i.e. Remote lock, remote wipe, or quarantine the device

Impact/Outcomes

With this additional funding, Hardin County will have implemented a mobile advanced threat protection solution that utilizes machine learning and artificial intelligence. Enabling Mobile Device Management (MDM), Jailbreak/root detection, Mobile Application Management (MAM), and Mobile Content Management (MCM) solution meeting the Common Criteria Evaluation Assurance Level 4 (EAL+4), UK Communications Electronic Security Group (CESG), and DoD STIG strengthening our mobile security posture, protect sensitive data, and prevent unauthorized access to government resources. Along with enforce security policies, mitigate threats, and improve incident response capabilities, reducing the overall risk of security breaches, cyber terrorism, and data loss on mobile devices.



Include this Page in your Application

**(C) Project Narrative
Page: 12**

Project Specific Information – Choose ONLY ONE category to complete for your project.

Project Specific Information: Communications Category

**To be completed for
Communications projects only**

Preliminary Information

Check boxes for each YES answer.

- 1. What is the KWIEC Tracking number that your communications project was assigned?
- 2. Did the KWIEC approve this project? (Include form in attachments)
- 3. Is this project in support of a primary means of communication for the agency?
- 4. Do you have a signed Mutual Aid agreement with KSP? (Include agreement in attachments)
- 5. Have your operational radios been programmed with the Mutual Aid frequency?
- 6. Do you participate in the annual Mutual Aid Communications exercises?
- 7. Are you partnering with other agencies on this project? (If yes, list them below)

Yes No
 Yes No
 Yes No
 Yes No
 Yes No
 Yes No

Partner Agencies (If you answered "yes" to Question 7):

- 8. Is this a continuation from a previous years' project? (If yes, provide details below)

Yes No

Enter the KOHS Grant number, KWIEC Tracking number, or other identifier (If you answered "yes" to Question 8):

Current Voice Communications Radio System

- 1. How old is the majority of the equipment in your current system (years)?
- 2. Mark all that apply below about your current system as it relates to this project:

Update noncompliant 25kHz wideband equipment	<input type="checkbox"/>	Replace 15+ year old equipment	<input type="checkbox"/>
New upgrade of a current non P-25 system to P-25	<input type="checkbox"/>	Continuation of a project to upgrade a non P-25 system to P-25	<input type="checkbox"/>
Upgrade of a current system to a non P-25 digital system	<input type="checkbox"/>	Continuation of a project to upgrade a non P-25 system	<input type="checkbox"/>
Procure P-25 handheld/mobile devices	<input type="checkbox"/>	Procure non P-25 handled/mobile devices	<input type="checkbox"/>
Add bridging/patching systems	<input type="checkbox"/>	Add backup satellite communications	<input type="checkbox"/>
Add microwave links	<input type="checkbox"/>	Add mobile repeaters	<input type="checkbox"/>

- 3. Below, list the emission designator(s) that your system is and will be operating under:

- 4. Is your primary voice system operating on (select one below):

Analog only Digital P-25 Digital non P-25 (NXDN, DMR, other)

- 5. Is your primary voice system: Trunked Encrypted Multicast Simulcast



**Include this Page in your Application
(Communications Projects Only)**

**(D) Communications
Page: 13**

Application Budget Table

AEL #	AEL Category	Equipment or Training Requested	Total Cost Per Unit	Number of Units Requested	Total Cost
05NP-00-IDPS	System, Intrusion D	BlackBerry Spark UEM Suite Device License - Advantage Sup	\$200.00	200	\$40,000.00
05NP-00-IDPS	System, Intrusion D	BlackBerry Spark UEM Express Cloud (Small to 250 users)	\$5,300.00	1	\$5,300.00
05NP-00-IDPS	System, Intrusion D	BlackBerry Cloud Hosting Service for Spark UEM Suite Subsc	\$80.00	200	\$16,000.00
				TOTAL	\$61,300.00

Authorized Equipment List (AEL)

Please attach documentation showing that the equipment you are requesting is on the Authorized Equipment List (AEL). You can find this list at: <https://www.fema.gov/authorized-equipment-list>.



Include this Page in your Application

Certification by Authorizing Official

I understand, and agree to comply with, the general and fiscal provisions of this grant application, including the terms and conditions; the provisions and regulations governing these funds and all other federal and state laws; that all information presented in this application is true and correct; that there has been appropriate coordination with all affected agencies; that costs incurred prior to grant approval may result in those costs being absorbed by the Sub-grantee, and that the receipt of these grant funds will not supplant state or local funds.

Name of Authorizing Official: Keith Taul
Title of Authorizing Official: Judge Executive
Agency/Organization: Hardin County & Hardin County Jail
Mailing Address: 150 North Provident Way, Suite 314
City, State, ZIP: Elizabethtown, KY 42701
Phone: +1 270.765.2350
Fax: +1 270.737.5590
Email Address: ktaul@hardincountyky.gov
Signature: 



Include this Page in your Application

(F) Certification
Page: 20