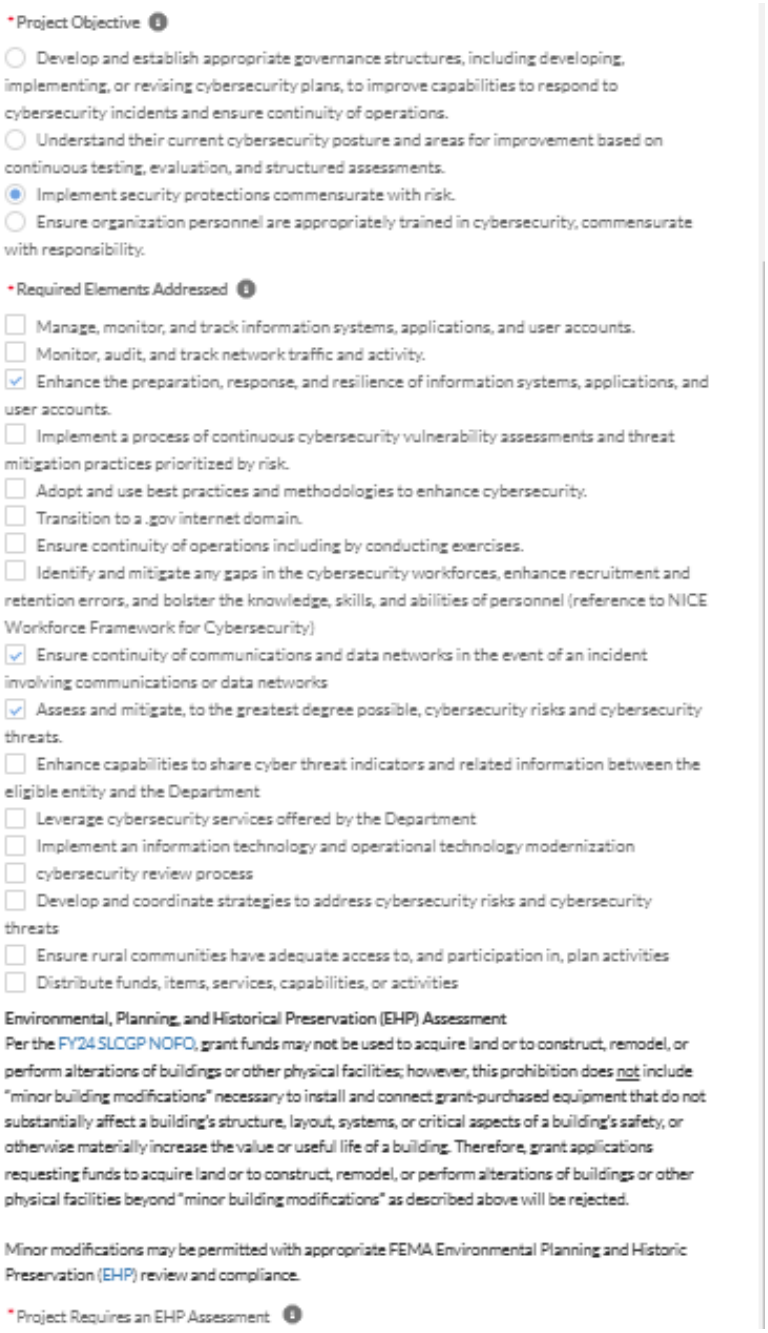
Application Questions

- **Project Title:** Alamance IT Storage Solution
- **Purpose:** The project seeks to upgrade Alamance County's outdated and insufficient storage area network to ensure continuity of operations in the event of a cyber attack or disaster event.
- **Project Objective** (select all that apply)



*Project Objective

- ○ Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.
- ○ Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments.
- ◉ Implement security protections commensurate with risk.
- ○ Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility.

*Required Elements Addressed

- ☐ Manage, monitor, and track information systems, applications, and user accounts.
- ☐ Monitor, audit, and track network traffic and activity.
- ☑ Enhance the preparation, response, and resilience of information systems, applications, and user accounts.
- ☐ Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by risk.
- ☐ Adopt and use best practices and methodologies to enhance cybersecurity.
- ☐ Transition to a .gov internet domain.
- ☐ Ensure continuity of operations including by conducting exercises.
- ☐ Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention errors, and bolster the knowledge, skills, and abilities of personnel (reference to NICE Workforce Framework for Cybersecurity)
- ☑ Ensure continuity of communications and data networks in the event of an incident involving communications or data networks
- ☑ Assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats.
- ☐ Enhance capabilities to share cyber threat indicators and related information between the eligible entity and the Department
- ☐ Leverage cybersecurity services offered by the Department
- ☐ Implement an information technology and operational technology modernization
- ☐ cybersecurity review process
- ☐ Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats
- ☐ Ensure rural communities have adequate access to, and participation in, plan activities
- ☐ Distribute funds, items, services, capabilities, or activities

Environmental, Planning, and Historical Preservation (EHP) Assessment

Per the FY'24 SLCGP NOFO, grant funds may not be used to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities; however, this prohibition does not include "minor building modifications" necessary to install and connect grant-purchased equipment that do not substantially affect a building's structure, layout, systems, or critical aspects of a building's safety, or otherwise materially increase the value or useful life of a building. Therefore, grant applications requesting funds to acquire land or to construct, remodel, or perform alterations of buildings or other physical facilities beyond "minor building modifications" as described above will be rejected.

Minor modifications may be permitted with appropriate FEMA Environmental Planning and Historic Preservation (EHP) review and compliance.

*Project Requires an EHP Assessment

- Project Narrative:
    - The existing storage area network is end of life within the current year (2025) and will not be supported for security updates, posing security risks. Additionally, the county has grown and the storage solution needs have increased. This project would address these needs and ensure the Department's ability to duplicate data and create the backup system that would allow recovery from a cyber disaster event, ensuring continuity of operations. Additional space is provided in the solution to test and validate recovery methods to ensure the recovery from a cyber event works.

- Investment Strategy *(Describe in narrative form how your project strategy effectively demonstrates the objectives of preventing, preparing for, protecting against, and responding to cyber incidents. Proposals must address closing the gaps in applicants' identified core capabilities and reducing the overall risk to the community, state or nation. (Refer to the four program objectives and 16 required elements as well as your responses in the gap assessment and any cyber vulnerability or risk assessments).*
    - Due to the current vulnerability of the outdated storage area network, the county must increase the size of the storage and convert to equipment that is under active support of the vendor. This project will address the gap in the county's ability to function in the event of a cyber or disaster event and reduce the overall risk to the community and allow the county to continue to serve them (including all major functions of the county not limited to the Sheriff's office, Department of Social Services, Emergency Management, EMS, Fire Services, Health). This project entails engineering a system that will allow growth and redundancy in the event of a cyber or disaster event, allowing the county to have secure access to its data. In preparation for any cyber incident the county would also gain the ability to test recovery methods per best practice in a sand box environment provided by this proposal.

- Collaboration *Regional, statewide or multi-state impact. Describe in narrative form the extent to which the project demonstrates a willingness to collaborate with federal, state, and local governments in efforts to prevent, prepare for, protect against, and respond to acts of cyber-crime and reduce the overall risk to the state or the nation.*
    - This project to upgrade the storage area network enables the county to remain a strong community partner by maintaining data security in the event of a cyber or disaster event. The project will serve all aspects of county government, including vital operations such as the Sheriff's office, Department of Social Services, Emergency Management, EMS, Fire Services, Health) allowing the county to offer mutual aid services in the event of a widespread emergency or disaster.

- Budget Narrative: *Describe in narrative form your project's budget plan, demonstrating how it will maximize cost-effectiveness of grant expenditures. Describe your plan for financial sustainability (how you will maintain the respective services/equipment after life of grant). Confirm that the required local matching funds are available.*
    - Network Equipment: $41,232.50
    - Storage Cost: $285,136.42
    - Support (4 Years): $97,197.68
    - Total Project Cost: $423,566.60
    - The total project cost is $423,566.60 and the county is requesting grant funding in the amount of $250,000 with a local county match of $173,566.60 - well over the 30% match requirement. The county's portion of the funding is secured and in hand and the county is ready to purchase the equipment and begin the project upon grant award. Additionally, the county has budgeted for ongoing maintenance and support after the life of the grant.

- Impacts/Outcome: *Describe in narrative form the solution; describe in detail what will be accomplished by this project. Include what procedures will be implemented, what capabilities will be enhanced, how identified threats*

and hazards will be mitigated, and the ways in which improvements will be measured/evaluated. Which objectives in the NOFO will be met (1-4)? Which sub-objectives? Which required elements will be met (1-16)?

- This project offers a solution to the outdated and unsupported storage area network and allows the county to increase the storage size to ensure continuity of service in the event of a disaster event or cyber attack. The grant would allow the county's IT department to engineer a system that will allow growth, redundancy and a testing area ensuring the county has secure access to its data in the event of a cyber or disaster event. Scheduled testing of the recovery solution would be gained as a result of the implementation. The improvements will be measured in the county's ability to comply with storage area network requirements and best practices. Quarterly disaster recovery

  NOFO objectives addressed by this project include..
  https://www.fema.gov/grants/preparedness/state-local-cybersecurity-grant-program/fy-24-fact-sheet

  (The first two can be addressed by the ability to sandbox off an environment and test recovery methods. This will be added as a scheduled event to train and assess preparedness.)

- Develop and implement cyber governance and planning.

- Assess and evaluate systems and capabilities.

NOFO required elements addressed through this project include…. https://www.ncdps.gov/SLCGP

(These are the items off the list that are addressed in this proposal, not sure how this would be worded)

1-Manage, monitor, and track information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology.
2-Monitor, audit, and track network traffic and activity transiting or traveling to or from information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
3-Enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state, against cybersecurity risks and cybersecurity threats.
4-Implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems, applications, and user accounts owned or operated by, or on behalf of, the state or local governments within the state.
5-Ensure that the state or local governments within the state, adopt and use best practices and methodologies to enhance cybersecurity, discussed further below.
Data encryption for data at rest and in transit
End use of unsupported/end of life software and hardware that are accessible from the internet
Ensure the ability to reconstitute systems (backups)

(Best practices addressed)

Additional best practices that the Cybersecurity Plan can address include:

Ensure continuity of operations of the state or local governments within the state, in the event of a cybersecurity incident, including by conducting exercises to practice responding to a cybersecurity incident.

Ensures continuity of communication and data networks within the jurisdiction of the state between the state and local governments within the state in the event of an incident involving those communications or data networks.

Implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives.

Distribute funds, items, services, capabilities, or activities to local governments.

Budget Line Items:

Equipment: 04SW-04-NETW