Project Proposal Identification—All Fields Must Be Completed Accurately!

Project Start Date:	1/2/2024	**Sub-recipient Org. Name:**	Greenville County, SC Information Systems
		Address:	301 University Ridge Greenville, SC
Project End Date:	12/31/2025	**Zip Code+4:**	29601-3659
		Recipient Type:	Local

*Less than 50,000 people in jurisdiction

Project Director:	Brendan Brewer	**E-Mail:**	bbrewer@greenvillecounty.org
		Phone:	(8640 467-7126
Funding Request ($):	1,800,000	**UEI Number:**	

Project Name (100 Character Max): SLCGP – Greenville County – South Carolina Comprehensive Cyber Security Plan – Upstate Region – Enhancing Cyber Resilience and Cyber Training.

Sustain or Build a capability? Build

Deployable: Yes

Shareable: Yes

Primary DHS Goal(s) (1, 2, 3 and/or 4) You Will Focus on for This Cyber Security Project:

1 – 1.1, 1.3, 1.5
2 – 2.1

Applicable Project Management Step for This Project (Initiate, Plan, Execute, Control, Close Out -- See Appendix 2): Project includes all phases of the Project Management Lifecycle – Initiate, Plan, Execute, Control and Close Out

I.B. Provide a narrative describing the project (3000 character maximum). Provide each of the cyber security objectives this project supports and how.

Project Name: Enhancing Cybersecurity Resilience Greenville County, SC and the Upstate Region

Objective 1.1: Facilitate EDR Adoption – Greenville County – SC Upstate

Scope: Implement Endpoint Detection and Response (EDR) solutions to improve real-time threat visibility and protection for state and local government assets.

Tasks:

1. *Align EDR solution with SC CIC for unified deployable solution across county and upstate region.*
2. *Procure and deploy EDR solutions across South Carolina Upstate in conjunction with SC-CIC*
3. *Provide training and guidance on EDR usage for IT staff.*
4. *Monitor and evaluate EDR effectiveness regularly.*

Objective 1.3: Support Vulnerability Scanning

Scope: Enhance vulnerability-scanning capabilities to identify and remediate weaknesses in government IT infrastructure in conjunction with SC – CIC.

Tasks:

1. *Evaluate existing vulnerability scanning tools and processes.*
2. *Upgrade or procure new vulnerability scanning solutions as needed.*
3. *Establish a regular scanning schedule for all government agencies.*
4. *Analyze scan results and prioritize vulnerabilities for remediation.*
5. *Provide guidance and resources to agencies for addressing vulnerabilities.*

Objective 1.5: Participate in a statewide comprehensive Managed Detection and Response (MDR) function capable of monitoring, alerting, and responding to cybersecurity incidents

Scope: Participating in a statewide MDR function leverages economies of scale. It enables agencies to access advanced cybersecurity tools, technologies, and expertise without bearing the full cost individually. This approach optimizes resource utilization and ensures that even smaller agencies can benefit from state-of-the-art cybersecurity capabilities.

Tasks:

1. *Identify Key Contacts: Designate a point of contact or liaison who will be responsible for interacting with the statewide MDR function.*
2. *Understand MDR Function Capabilities: Schedule a meeting or briefing with the statewide MDR function to gain a comprehensive understanding of their capabilities, processes, and resources.*
3. *Define Incident Handling Procedures: Collaborate with the MDR function to define incident handling procedures, including escalation paths, communication channels, and response timelines.*

4. *Establish Communication Channels: Set up dedicated communication channels for incident reporting and sharing threat intelligence between organizations and the statewide MDR function. This may include secure email addresses, phone numbers, or incident reporting platforms.*
5. *Clarify Roles and Responsibilities: Clearly define the roles and responsibilities of your organization and the MDR function in the event of a cybersecurity incident.*
6. *Document Incident Categories: Work with the MDR function to categorize different types of incidents based on severity and impact to prioritize response efforts.*
7. *Create Incident Playbooks: Develop incident response playbooks that outline step-by-step procedures for common incident scenarios, incorporating input from the MDR function.*
8. *Establish Service Level Agreements (SLAs): Collaborate with the statewide MDR function to create SLAs that define response times, reporting requirements, and incident resolution goals.*
9. *Conduct Tabletop Exercises: Periodically conduct tabletop exercises and simulations in conjunction with the MDR function to test incident response procedures, identify gaps, and enhance coordination.*
10. *Share Threat Intelligence: Establish a mechanism for sharing threat intelligence and indicators of compromise (IOCs) between your organization and the MDR function. This should include regular updates on emerging threats and vulnerabilities.*
11. *Regular Meetings and Updates: Schedule regular meetings or briefings with the MDR function to exchange information, discuss ongoing incidents, and provide updates on changes in your organization's infrastructure or threat landscape.*
12. *Review and Update Protocols: Periodically review and update the coordination protocols based on lessons learned, changes in technology, and evolving threats.*
13. *Incident Reporting: Ensure that your organization promptly reports all detected cybersecurity incidents to the MDR function in accordance with the established protocols.*
14. *Feedback and Improvement: Encourage a feedback loop with the MDR function to continuously improve coordination, incident response procedures, and overall incident readiness.*

Project Name: Enhancing Cyber Training
Objective 2.1 Deliver and participate in live fire cyber training through a shared platform to increase incident response readiness statewide

Scope: The scope of the project is to deliver and participate in live fire cyber training exercises through a shared platform with the objective of enhancing incident response readiness across the entire state. This initiative aims to simulate real-world cyber incidents, providing hands-on experience and training for cybersecurity professionals, thereby improving their ability to effectively respond to and mitigate cyber threats.

Tasks:

1. *Training Platform Selection: Identify and select a suitable shared platform for conducting live fire cyber training exercises. This may involve the procurement of new software or the utilization of existing platforms, ensuring they meet the necessary requirements for realistic training simulations.*
2. *Curriculum Development: Develop a comprehensive curriculum that covers various cyber threat scenarios and incident response strategies. The curriculum should be aligned with industry best practices and tailored to the specific needs of state cybersecurity teams.*
3. *Exercise Design: Create a series of realistic cyber threat scenarios and exercises that simulate actual incidents. These exercises should encompass a wide range of cyber threats, including malware infections, data breaches, DDoS attacks, and social engineering attacks.*

4. *Participant Recruitment: Identify and recruit cybersecurity professionals from state and local government agencies to participate in the training exercises. Ensure a diverse group of participants to facilitate knowledge sharing and collaboration.*
5. *Training Delivery: Conduct live fire cyber training sessions, allowing participants to respond to simulated cyber incidents in real-time. Provide guidance, mentorship, and feedback during the exercises to facilitate learning and improvement.*
6. *Scenario Evaluation: Assess the performance of participants during each training exercise, including their incident response effectiveness, decision-making, and communication skills. Use evaluation metrics to measure progress and identify areas for improvement.*
7. *Incident Response Documentation: Encourage participants to document their incident response actions and strategies during the exercises. Compile and analyze these documents to identify best practices and areas needing refinement.*
8. *Knowledge Sharing: Facilitate knowledge sharing sessions and debriefs after each exercise, where participants can discuss lessons learned, share insights, and collaborate on improving incident response strategies.*
9. *Continuous Improvement: Continuously refine the training curriculum and exercises based on feedback and evolving cybersecurity threats. Adapt the program to address emerging threats and technologies.*

II.A. Funding Plan by POETE elements

Provide the total estimated cost for the period of performance for this project by completing the following table:

- ***Provide funding requests by POETE (Planning, Organization, Equipment, Training, Exercise) areas***
- ***For each POETE element that has an associated funds requested, provide a brief summary description of the planned expenditures***

POETE	Homeland Security Grant Program Funding Request
Planning	
Organization	
Equipment	$1,800,000
Training	
Exercises	
Total	

Planning

Planning is a critical component of effective cybersecurity management. Greenville County IS will provide personnel to assist SC CIC in the development of strategic plans, policies, and frameworks to guide cybersecurity efforts including:

- **Cybersecurity Strategy Development:** Develop a comprehensive cybersecurity strategy that outlines goals, objectives, and a roadmap for improving cybersecurity posture.
- **Risk Assessment and Management:** Complete regular cybersecurity risk assessments to identify vulnerabilities and prioritize mitigation efforts.
- **Policy and Procedure Development:** Creation and implementation of cybersecurity policies, procedures, and guidelines to ensure compliance and security best practices.
- **Incident Response Planning:** Support the development of incident response plans, including the creation of incident response teams and communication strategies.

Organization

Organizational aspects involve structuring and staffing cybersecurity teams and aligning roles and responsibilities. Greenville County IS will contribute the structure and cyber teams required for the SC Upstate support including:

- **Cybersecurity Personnel:** Providing cybersecurity professionals, including security analysts, incident responders, and security architects.

- **Staff Training and Development:** Invest in ongoing training and certification programs to keep the cybersecurity workforce up to date with the latest threats and technologies.

Equipment

To effectively protect against cyber threats, adequate technologies are essential. Funding requests in this area include:

- **Endpoint Security Solutions:** Endpoint security tools to protect devices, including antivirus, anti-malware, and endpoint detection and response (EDR) solutions.

Training

Training is essential for ensuring that cybersecurity professionals have the knowledge and skills needed to defend against cyber threats. Greenville County will provide the cyber security analysts to participate and assist in leading training in support of a unified SC CIC Training solution for Greenville County and the Upstate of South Carolina.

Exercise

Exercises and simulations are vital for testing incident response capabilities and improving overall cybersecurity readiness including:

- **Cybersecurity Exercises:** Tabletop exercises, red team/blue team simulations, and other cybersecurity drills to evaluate incident response procedures.
- **Incident Response Training:** Allocate funds for specialized incident response training and drills to ensure that response teams can effectively manage and mitigate cyber incidents.