Project Proposal Identification—All Fields Must Be Completed Accurately!

Project Start Date: 1/2/2025

Project End Date: 12/31/2026

Sub-recipient Org. Name: Greenville County, SC Information Systems
Address: 301 University Ridge, Suite N-3000 Greenville, SC
Zip Code+4: 29601-3659
Type: Local

*Less than 50,000 people in jurisdiction

Project Director: Joe Newton

E-Mail: jnewton@greenvillecounty.org

Phone: (864) 467-7101

Funding Request ($): 2,400,000

UEI Number: KPTBH7N118S8

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? Sustain and Build Capabilities

Deployable: **Yes**

Shareable: **Yes – State and Upstate Region**

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

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: Systain Endpoint Detection and Response (EDR) solutions to improve real-time threat visibility and protection for state and local government assets in South Carolina Upstate.

Tasks:

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

Objective 1.3: Support Vulnerability Scanning

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

Tasks:

1. *Review and sustain existing vulnerability scanning tools and processes.*
2. *Upgrade, procure and sustain 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 and lead upstate capabilities to leverages economies of scale. Facilitate and support regional agencies access to 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.*

Objective 1.7: Promote Multifactor Authentication

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

Tasks:

1. *Review existing authentication practices across government agencies to identify reliance on single-factor authentication (SFA) and the associated risks.*

2. *Research and select appropriate MFA solutions that fit the needs of different agencies, considering factors like user experience, security requirements, and integration capabilities.*
3. *Create a clear timeline for MFA deployment that includes key milestones, deadlines, and responsibilities for each agency.*
4. *Develop training programs and materials to educate users on the importance of MFA, how to use it, and best practices for maintaining security.*
5. *Set up a support system for agencies to address any issues or questions related to MFA. Share resources such as FAQs, troubleshooting guides, and contact points for technical assistance.*

Objective 2.2 Support and participate in cyber training to ensure on-demand incident response capabilities and essential skills are current.

Scope: The objective of this initiative is to support and actively participate in comprehensive cyber training programs designed to enhance incident response capabilities and ensure essential skills remain current. This scope encompasses the development and delivery of training modules that cover the latest cybersecurity threats, incident response techniques, and best practices.

Tasks:

1. *Training Platform Selection: Identify and select a suitable shared platform for conducting incident response (IR) 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. *Exercise Design: Create a series of realistic cyber threat scenarios and exercises that simulate actual incident and instruct agencies on the incident response process.*
3. *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.*
4. *Training Delivery: Conduct incident response 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.*
5. *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.*
6. *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.*
7. *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.*
8. *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.*

Objective 3.3 Support, promote, and utilize CISA's Known Exploited Vulnerabilities Catalog in prioritizing patching decisions

Scope: The primary objective of this initiative is to incorporate and actively promote the use of the Cybersecurity and Infrastructure Security Agency's (CISA) Known Exploited Vulnerabilities (KEV) Catalog as a critical tool in making informed and effective patch management decisions. By leveraging this resource, organizations can prioritize patching efforts based on real-world threat intelligence, focusing on vulnerabilities that are known to be actively exploited in cyberattacks. This ensures a proactive approach to mitigating risks and enhancing security posture.

1. Integrate CISA KEV Catalog into Vulnerability Management Tools Work - with the IT security team to integrate CISA's Known Exploited Vulnerabilities (KEV) Catalog into existing vulnerability scanning and patching workflows. Ensure that all vulnerabilities identified through scans are cross-referenced with the KEV Catalog for prioritization in patch management.

2. Develop and Implement Patching Prioritization Criteria - Collaborate with cybersecurity and operations teams to create a set of criteria for prioritizing vulnerabilities, focusing on those actively exploited, as indicated by CISA's KEV Catalog to ensure patching schedules prioritize vulnerabilities listed in the KEV Catalog based on criticality, with immediate focus on those actively exploited.

3. Conduct Awareness Campaigns and Training Sessions - Organize training sessions and awareness campaigns for IT, security, and operations teams to promote the importance and utilization of the KEV Catalog in daily operations. Ensure that all key stakeholders understand the significance of the KEV Catalog in prioritizing vulnerabilities and risk mitigation.

4. Establish Continuous Monitoring and Automated Alerts for KEV Catalog Updates - Set up automated notifications and alerts within the SOC or vulnerability management platform to monitor updates from the KEV Catalog - Ensure that security teams receive real-time updates on newly added vulnerabilities to the KEV Catalog, triggering appropriate action.

5. Create Reporting Process for Tracking Patch Progress and Compliance - Develop a standardized reporting process to track and document the progress of patching vulnerabilities identified in the KEV Catalog, including timelines and metrics for management review. Provide leadership with regular updates on the status of patching efforts, ensuring accountability and compliance with risk management practices.

Objective 4.3 Develop and distribute relevant security awareness materials, alerts, and advisories

Scope: The primary objective is to establish a consistent and timely process for developing, distributing, and updating cybersecurity alerts and advisories. These alerts aim to inform stakeholders about emerging threats, vulnerabilities, and necessary actions to mitigate risks. This process ensures that organizations stay informed and prepared to respond to cyber incidents and evolving threats.
1. Threat Intelligence Collection – Implement solutions to source cyber threat intelligence including sensors and external sources to feed security information and event management and intelligence platforms.

2. Develop Cybersecurity Alerts - Source actionable cybersecurity alerts for new vulnerabilities and emerging threats from network sensors and security platforms.

3. Creation and Distribution of Cybersecurity Advisories - Create cybersecurity threat intelligence logging platforms to ensure that all relevant groups receive actionable guidance to mitigate risks and improve cybersecurity posture.

4. Establish Timely Distribution of Alerts - Implement centralize security information and event management platforms to distribute alerts ensuring that the right people receive critical information in a timely manner.

5. Continuous Monitoring and Follow-Up - Monitor the response to each alert, ensuring that recommended mitigations are implemented.

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	40,000
Organization	480,000
Equipment	1,800,000
Training	50,000
Exercises	30,000
Total	2,400,000

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 and the hardware platforms to support the logging, analysis, and storage of the EDR content.

Multi-factor Authentication Security Solutions: Security tools and technologies including hardware, software, and infrastructure components to implement and sustain a robust MFA solutions across the environment.

Vulnerability Management Solutions: Security tools and technologies including hardware, software, and infrastructure components to implement, maintain, and sustain a comprehensive vulnerability management program that aligns with NIST Frameworks.

Patch Management Solutions: Security tools and technologies including hardware, software, and infrastructure components to implement, maintain, and sustain a comprehensive patch management program to address known exploited vulnerabilities.

Alert Management Solutions: Security tools and technologies including hardware, software, and infrastructure components to implement, maintain, and sustain a robust alerting solution.

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.

II.B. Programmatic Milestones

Provide specific descriptive milestones for the project over the period of performance, including start and end dates for each milestone; up to 10 milestones may be provided.

Milestone 1: Your plan to address your POETE gaps above by sustaining/building capability

Project Initiation:

- *Define project objectives, scope, and stakeholders.*
- *Appoint project team members and roles.*

Start Date: 8/1/2025 **End Date:** 12/15/2025

Milestone 2: Your plan to address your POETE gaps above by sustaining/building capability

Sustain and Expand EDR Solution:

- *Protect critical infrastructure with the deployment and on-going administrative management of the broadly deployed EDR solution.*

Start Date: 8/2/2025 **End Date:** 8/15/2026

Milestone 3: Your plan to address your POETE gaps above by sustaining/building capability

Support Vulnerability Scanning

- *Enhance and sustain vulnerability-scanning capabilities to identify and remediate weaknesses in government IT infrastructure in conjunction with SC – CIC and NIST frameworks*

Start Date: 8/2/2025 **End Date:** 12/31/2026

Milestone 4: Your plan to address your POETE gaps above by sustaining/building capability

MFA Implementation

- *Review MFA requirements and define selection criteria*
- *Complete MFA validation and UAT*
- *Deploy and sustain MFA solution*

Start Date: 8/2/2025 **End Date:** 12/31/2026

Milestone 5: Your plan to address your POETE gaps above by sustaining/building capability

Participate in a statewide comprehensive Managed Detection and Response (MDR)

- Deploy the selected EDR technology and integrate w/ MDR
- Configure tools and technologies to leverage MDR capabilities

Start Date: 8/2/2025 **End Date:** 12/31/2026

Milestone 6: Your plan to address your POETE gaps above by sustaining/building capability

Full-Scale Training Rollout

- Sustain the full-scale cybersecurity training program for all employees.
- Monitor participation and track progress.

Start Date: 8/2/2025 **End Date:** 12/31/2026

Milestone 7: Your plan to address your POETE gaps above by sustaining/building capability

Rollout CISA Vulnerability Management, Alerting and Patch Mangement Programs

- Coordinate and select vulnerability management solution
- Deploy vulnerability management solution
- Select patch management solution
- Deploy, maintain and sustain patch management solution to address key vulnerabilities to protect critical infrastructure

Start Date: 8/2/2025 **End Date:** 12/31/2026

Milestone 8: Your plan to address your POETE gaps above by sustaining/building capability

Metrics and Progress Assessment:

- Evaluate program effectiveness by analyzing key performance indicators (KPIs) such as incident response times, incident detection rates, and employee engagement in training.
- Use assessment findings to make necessary adjustments.

Start Date: 8/2/2025 **End Date:** 12/31/2026

Milestone 9: Your plan to address your POETE gaps above by sustaining/building capability

Program Review and Expansion:

- Conduct a comprehensive program review to assess achievements and identify areas for improvement.
- Consider expanding the program to include advanced training modules and additional EDR features based on evolving cybersecurity threats.

Start Date: 8/2/2025 **End Date:** 12/31/2026

Milestone10:Your plan to address your POETE gaps above by sustaining/building capability

Start Date: **End Date:**

III.A. Project Impact / Used for Project Evaluation

What outcomes will indicate that this project is successful at the end of the period of performance? Discuss anticipated outcomes of success by Cybersecurity Planning Objectives:

Anticipated outcomes of success in "SLCGP – Greenville County – South Carolina Comprehensive Cyber Security Plan – Upstate Region – Enhancing Cyber Resilience and Cyber Training" initiatives are multifaceted, as these efforts are instrumental in enhancing an organization's ability to detect, respond to, and mitigate cyber threats effectively. Here are the anticipated outcomes of success for both EDR and training components:

Endpoint Detection and Response (EDR):

1. Advanced Threat Detection: A successful EDR implementation should result in improved advanced threat detection capabilities. This means promptly identifying and mitigating sophisticated threats like zero-day vulnerabilities, advanced persistent threats (APTs), and fileless malware.

2. Rapid Incident Response: EDR solutions enable faster incident response by providing real-time alerts and automated responses to security incidents. Success in EDR should result in shorter incident resolution times.

3. Reduced Dwell Time: Successful EDR implementation should reduce the dwell time of threats within the network. Dwell time is the duration an attacker remains undetected in the system, and shorter dwell times lead to reduced potential damage.

4. Improved Forensics and Investigation: EDR solutions typically provide detailed endpoint data and logs. Successful EDR usage facilitates better post-incident forensics and investigation, helping organizations understand the scope and impact of security incidents.

5. Proactive Threat Hunting: EDR tools support proactive threat hunting by security teams. Anticipated success includes the ability to identify emerging threats before they cause significant harm.

6. Endpoint Security Hygiene: EDR can improve endpoint security hygiene by identifying and remediating vulnerabilities, unauthorized software, and configuration issues on endpoints.

7. Compliance and Reporting: EDR solutions assist in maintaining compliance with regulatory requirements by providing detailed logs and reports. Successful EDR usage ensures compliance and simplifies reporting efforts.

8. Reduced False Positives: A successful EDR solution should minimize false positive alerts, ensuring that security teams can focus on genuine threats instead of noise.

Training and Awareness:

1. Cybersecurity Awareness: Successful training programs increase cybersecurity awareness among all employees. Anticipated outcomes include a workforce that can identify and report security threats, reducing the risk of successful social engineering attacks.

Reduced Phishing Susceptibility: Employees who undergo effective training are less likely to fall victim to phishing attacks. Success in training programs results in a more resilient workforce against social engineering threats.

3. Improved Incident Response: Training empowers employees to respond effectively to security incidents. They are more likely to follow the organization's incident response procedures, reducing the impact of incidents.

4. Security Best Practices: Successful training imparts security best practices to employees, such as strong password management, secure data handling, and safe browsing habits.

5. Compliance with Policies: Training ensures that employees understand and comply with cybersecurity policies and procedures, reducing the risk of policy violations.

6. Reduced Insider Threats: By fostering a security-conscious culture, training can help identify and mitigate insider threats, whether intentional or unintentional.

7. Security Champions: Effective training can identify and nurture security champions within the organization who can serve as advocates for cybersecurity best practices.

8. Ongoing Learning: Successful training programs encourage ongoing learning and self-improvement in the cybersecurity realm, ensuring that employees stay current with emerging threats and technologies.

9. Measurement of Success: Training programs should include metrics to measure their success, such as the number of reported incidents, the rate of employee participation, and the reduction in security incidents over time.

10. Adaptability to Changing Threat Landscape: Success in training includes the ability to adapt training content and methods to address evolving cybersecurity threats and risks effectively.

Overall, the anticipated outcomes of success for EDR and training initiatives are comprehensive and contribute to a more resilient organization that can effectively protect against cyber threats, respond to incidents, and empower its workforce to be an active part of its cybersecurity defense.