Virginia Cybersecurity Planning Committee
December 11, 2023 – 10am
VITA, Mary Jackson Boardroom

Agenda

Call to Order and Welcome	Mike Watson Chief Information Security Officer
Review of Agenda	Staff
Approval of Minutes	Staff
First project: Assessments	Mr. Watson
Public Comment Period	
Other Business	Staff
Adjourn	

VIRGINIA IT AGENCY

Virginia Cybersecurity Planning Committee
October 18, 2023 – 10:00 a.m.
7235 Beaufont Springs Dr, Mary Jackson Boardroom, Richmond, VA, 23225

Call to Order:

A meeting of the Virginia Cybersecurity Planning Committee was called to order at 10:02 am. Mr. Watson welcomed the members. Mr. Heslinga called the roll.

Presiding:

Michael Watson, Committee Chair, Chief Information Security Officer, Virginia IT Agency

Members Present:

Diane Carnohan, Chief Information Security Officer, Virginia Department of Education

Robbie Coates, Director, Grant Management and Recovery, VDEM

Adrian Compton, Tribal Administrator, Monacan Indian Nation

Charles DeKeyser, Major, Virginia Army National Guard. Major Dekeyser is on temporary duty from his home base for the National Guard.

John Harrison, IT Director, Franklin County

Derek M. Kestner, Information Security Officer, Supreme Court of Virginia

Benjamin Shumaker, Cyber Security Specialist, King William County Government.

Stephanie Williams-Hayes, Chief Information Security Officer, Virginia Department of Health

Wesley Williams, Executive Director of Technology, Roanoke City Public Schools

Members Participating Remotely:

Aliscia N. Andrews, Office of the Governor

Brenna R. Doherty, Chief Information Security Officer, Department of Legislative Automated Systems

Beth Burgin Waller, Chair, Cybersecurity and Data Privacy Practice, Woods Rogers Vandeventer Black. Wesley Williams, Executive Director of Technology, Roanoke City Public Schools

Ms. Andrews and Ms. Waller participated from their residence because their principal residence is more than 60 miles from the meeting location.

Ms. Doherty participated remotely due to personal reasons.

Members Not Present:

Michael Dent, Chief Information Security Officer, Fairfax County Department of Information Technology

Major Eric W. Gowin, Virginia State Police

Staff Present:

Joshua Heslinga, Director of Legal & Legislative Services, Virginia IT Agency

Joshua Reynolds, Assistant Attorney General, Office of the Attorney General

Mylam Ly, Legal Compliance & Policy Specialist, Virginia IT Agency

Review of Agenda:

Ms. Ly provided an overview of the agenda and corresponding items in the digital meeting packets.

Approval of Minutes:

The August meeting minutes were displayed on the screen. Upon a motion by Mr. Shumaker and duly seconded by Mr. Kestner, the committee unanimously voted to adopt the August meeting minutes.

Grant Update

Mr. Coates provided the year 2 grant update. The year 2 grant application was submitted for approximately 8.7 million dollars. The amounts for Year 3 and year 4 will decrease. The period of performance will be December 1, 2023 – November 1, 2027, seven years for all four grants. Award information should come shortly from FEMA.

The Year 1 cybersecurity plan was fully approved by FEMA.

Survey of Interest

Mr. Watson reviewed the outcomes of the survey of interest with the committee. There was a total of 140 applicants, of which 1% were tribal and 2% were vendors. Mr. Watson reviewed the PowerPoint presentation. Following reviewing the survey of interests the committee discussed prioritizing year 1 funds.

Prioritizing Year 1 Funds

During the discussion of year one funds, the grant requirements were discussed including the requirement for 25% of the funds be allocated to rural localities, and assessments being a foundational piece for the application. There was a discussion on assessments being the first project. Once assessments were completed additional projects would be released. Localities that did not fill out the survey of interest were still eligible to apply for various projects.

There was further discussion on prioritizing based on

1. Prioritizing based on risk
2. Setting a ceiling or floor per service.
3. Hybrid of the two above. Start with assessments then moving to other prioritized segments.

Returning to the discussion on assessment, the committee felt that assessments would help inform the needs and future investments of the project.

Contract Options Discussion

The committee then reviewed the contract options document. These were contracts that were known to GSA and state that were put together in a way to be informational to localities about what options they have. The document was designed to inform existing options and what it takes to make use of these. Vendors interested in being on the list of contract options refer them to cyberplanning@vita.virginia.gov

Public Comment Period:

There were no public comments.

Other Business:

Mr. Watson opened the floor for other business. Mr. Watson discussed hiring a Project Manager to assist with the grant. Ms. Ly discussed travel forms.

Adjourn

Upon a motion by Major Dekeyser and duly seconded by Ms. Carnohan, the committee unanimously voted to adjourn the meeting 11:23am.

STATEMENT OF REQUIREMENTS (SOR)

SOR #

State and Local Cybersecurity Grant Program Assessment Support

1. **Date:** December 18, 2023

2. **Authorized User**: Virginia Information Technology Agency (VITA)

3. **Authorized User Contact Information:**
Kelley Kapsak, kelley.kapsak@vita.virginia.gov

4. **Solicitation Schedule:**

Event	Date
Release SOR	December 18, 2023
Supplier Questions Due to CAI	December 28, 2023
Supplier Response Due	January 5, 2023
Award Decision	January 12, 2023
Estimated Project Start Date	January 18, 2023

5. **Evaluation and Scoring**

Supplier's Response must be submitted in the specified Statement of Work (SOW) format and will be evaluated for format compliance.

Supplier's Response will be evaluated for technical merit based on its appropriateness to the performance of Authorized User's requirements, its applicability to the environment, and its effective utilization of Supplier and Authorized User resources.

6. **Project/Service:** State & Local Cybersecurity Grant Program Support

7. **Specialty Area** (Check one)**:**

- ☐ Application Development
- ☐ Business Continuity Planning
- ☐ Business Intelligence
- ☐ Business Process Reengineering
- ☐ Enterprise Architecture
- ☐ Enterprise Content Management
- ☐ Back Office Solutions
- ☐ Geographical Information Systems
- ☒ Information Security
- ☐ IT Infrastructure
- ☐ IT Strategic Planning
- ☐ Project Management
- ☐ Public Safety Communications
- ☐ Radio Engineering Services
- ☐ IV&V Services

8. **Contract Type** (Check)**:**

☒ Fixed Price, Milestone-based

9. Introduction:

Project History

VITA and VDEM are administering Virginia's participation in the State and Local Cybersecurity Grant Program (SLCGP), under which a combination of federal grant money and state-provided matching funds will be used to assist state and local public entities with improving their cybersecurity posture. 80% of the grant fund will be allocated for local public entities and within that 80%, 25% is specifically designated for rural localities. For further information on the SLCGP generally, see CISA and FEMA's websites:

State and Local Cybersecurity Grant Program | CISA
State and Local Cybersecurity Grant Program | FEMA.gov

For further information on Virginia's participation in the SLCGP, see VITA's website:

Federal Cybersecurity Grants | Virginia IT Agency

The Virginia Cybersecurity Planning Committee has developed a Virginia Cybersecurity Plan, which has been approved by the federal government and is a prerequisite for using SLCGP funding. The Plan contains Virginia's objectives for the program and identifies a set of priority objectives. Year one funding is already available to Virginia, and localities will soon be able to seek that funding. With respect to year one funding at least, the intent is to prioritize localities conducting a needs / gap assessment against the program objectives.

The intent of this SOR is to identify and vet suppliers who will be ready to perform an assessment of specified locality's environment resulting in an artifact. The produced artifact will be the precursor for determining what cyber security services will be implemented in their environment as localities applications for assessment funding are approved. Authorized user will determine the localities for assessments.

Business Need

This SOR requires an overall review of a specified locality's current approach of the Cybersecurity Program, as well as development of recommended security artifacts to support operationalization of the Cybersecurity Program.

10. Scope of Work:

This Statement of Requirements (SOR) defines the Cybersecurity Program Support required by The Virginia Information Technology Agency (VITA). This SOR requires an overall review of specified locality's current approach of the Cybersecurity Program, as well as development of recommended security artifacts to support operationalization of the Cybersecurity Program.

The Supplier will review specified locality's current state of information security investment for the areas specified in the Commonwealth of Virginia SLGCP Cybersecurity Plan document. This assessment may include the review of Security Policies and Standards based on applicable security controls framework; Assess the Investment Division's use case against program standards to determine best approach to governance; Identify governance approach and requirements; Analyze resources, staffing and capabilities; and Confirm investment requirements and funding availability based on current program roadmap.

After this initial evaluation, the Supplier will generate a Findings and Recommendations Report using a supplied template for re-alignment of the Cybersecurity program including identification/update of the necessary governance artifacts. Upon acceptance of the recommendations, the Supplier will then develop initial approach for remediation of missing governance artifacts identified within the Commonwealth of Virginia SLGCP Cybersecurity Plan document (e.g., Security Management plan, updated policies, updated standards,

controls frameworks, capabilities, charters, etc.) as prioritized by Authorized User for this initial phase of this effort. Prioritizations may include but are not limited to

Manage, monitor, and track information systems, applications, and user accounts;

Monitor, audit, and track network traffic and activity;

Enhance the preparation, response, and resiliency of information systems, applications, and user accounts; Implement a process of continuous cybersecurity risk factors and threat mitigation. practices prioritized by degree of risk;

Adopt and use best practices and methodologies to enhance cybersecurity (references NIST);

Implement multi-factor authentication, implement enhanced logging, 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, prohibit use of known/fixed/default passwords and credentials, ensure the ability to reconstitute systems (backups), migration to the .gov internet domain;

Promote the delivery of safe, recognizable, and trustworthy online services, including using the .gov internet domain;

Ensure continuity of operations including by conducting exercises;

Identify and mitigate any gaps in the cybersecurity workforces, enhance recruitment and retention efforts, 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 relating to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the specified locality;

Enhance capabilities to share cyber threat indicators and related information between the eligible locality and the Authorized User;

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

Develop and coordinate strategies to address cybersecurity risks and cybersecurity threats.

11. Period of Performance:

Implementation of the solution will occur within 12 weeks of execution of this SOR with optional extensions to be approved at later date.

12. <u>Place of Performance</u> (Check one)<u>:</u>

☐ Authorized User's Location _____*(City, VA)*

☐ Supplier's Location _____*(City, State)*

☒ Specified Locality and/or _____*(Explain)*

Supplier's Location

13. Project Staffing:

a. Supplier Personnel

The roles listed in the table below represent the minimum Supplier personnel requirements for this engagement.

Role	Key Personnel (Y/N)	Years of Experience	Certifications	References Required (Y/N)
Security Executive Sponsor and QA	Y	20+ years	N/A	N
Senior Security Lead	Y	15+ years	N/A	N
Junior Security Support	Y	2-5 years	N/A	N

b. Authorized User Staff:

The roles listed in the table below represent Authorized User's staff and the estimated time each will be available to work on the project.

ROLE	DESCRIPTION	% PROJECT AVAILABILITY
VITA Chief Information Security Officer	Project Sponsor work product approval	5%
Various VITA Support Staff	Support discovery, provide expertise on current processes, provide feedback on recommendations and deliverables as appropriate	10%
VITA Project Manager	Primary POC for the project and support project coordination and discovery	85%

14. Milestones and Deliverables:

The minimum required milestones and deliverables and the estimated completion date for each deliverable are listed in the following table.

Milestone Event(s)	Deliverable	Estimated Completion Date
Project Initiation	Project Planning and Kickoff Presentations	January
Acceptance of Final Findings and Recommendations Report	Final Findings and Recommendations Report	XXX
Phase 1 Completion	Completion of Phase 1 Supporting Artifacts per sponsor agreement	XXX

The Supplier should provide all deliverables in hardcopy form and in electronic form, using the following software standards (or lower convertible versions):

Deliverable Type	Format
Text Document	Microsoft Word
Spreadsheets	Microsoft Excel
Presentation	Microsoft PowerPoint / Visio (standard)

15. Travel Expenses (Check one)**:**

☐ No travel will be required for this engagement

☒ Travel must be included in the total fixed price of the solution

16. Payment (Check all that apply)**:**

☒ Payment made based on successful completion and acceptance of deliverables

☐ All payments, except final payment, are subject to a *(XX)*% holdback

17. Acceptance Criteria:

The Project Manager will have *(10)* business days from receipt of the deliverable to provide Supplier with the signed acceptance receipt.

Final acceptance of services provided under the SOW will be based upon (Check one):

☐ User Acceptance Test

Acceptance Criteria for this solution will be based on a User Acceptance Test (UAT) designed by Supplier and accepted by Authorized User. The UAT will ensure that all of the functionality required for the solution has been delivered. The Supplier will provide the Authorized User with a detailed test plan and acceptance checklist based on the mutually agreed upon UAT plan. This UAT plan checklist will be incorporated into the SOW.

☒ Final Report

Acceptance criteria for this solution will be based on submission of completed assessments for each interviewed locality. In the SOR, Supplier and Authorized User will agree on the format and content of the report to be provided to Authorized User for final acceptance.

☐ Other (specify): _____

18. Project Roles and Responsibilities:

Responsibility Matrix	Supplier	Authorized User
Prepare Readiness plan	✓	
Review and Accept Plan		✓
Perform Readiness Assessment and Review	✓	

19. Criminal Background Checks and Other Security Requirements (check all that are required):

☒ Standard CAI Required Background Check

☒ Agency Specific Background Check

20. Performance Bond (Check one)**:**

☐ Required for *(XXX)*% of the SOW value

☒ Not Required

21. Reporting (Check all that are required):

☒ **Weekly Status Update**

The weekly status report, to be submitted by Supplier to Authorized User, should include: accomplishments to date as compared to the project plan; any changes in tasks, resources or schedule with new target dates, if necessary; all open issues or questions regarding the project; action plan for addressing open issues or questions and potential impacts on the project; risk management reporting.

☒ **Other(s)** (Specify): As defined in the Scope of Work and Deliverables sections of this SOR.

22. Federal Funds (Check one):

☒ Project will be funded with federal grant money

☐ No federal funds will be used for this project

23. Training and Documentation:

a. Training:

☐ Required as specified below

☒ Not Required

Training Requirements:
(Specify specific training requirements)

b. Documentation:

☒ Required as specified below

☐ Not Required

Documentation Requirements:
As detailed in Section 10 (Scope of Work) and Section 14 (Milestones and Deliverables) of this SOR

24. Additional Terms and Conditions:

The services to be provided are subject to the following additional provisions:

a. Effective July 1, 2020, the Code of Virginia requires contractors with the Commonwealth who spend significant time working with or in close proximity to state employees to complete sexual harassment training. As a result of the new code, VITA and the Department of Human Resource Management (DHRM) are requiring that all contractors working through the CAI contract complete DHRM's "Preventing Sexual Harassment" training. This training is available as either a short video or a written transcript on the DHRM website: https://www.dhrm.virginia.gov/public-interest/contractor-sexual-harassment-training. The selected Supplier must agree that any assigned resource will complete the training.

b. The selected Supplier must agree that any assigned resource will review and conform to the IT Contingent Labor Program (ITCL) Contractor Code of Conduct. The Code of Conduct can be reviewed on VITA's website at the following link: https://www.vita.virginia.gov/media/vitavirginiagov/supply-chain/pdf/Contingent-Worker-Code-of-Conduct.pdf

25. Scheduled Work Hours:

On an as needed basis, to be coordinated with the Authorized User's Project Sponsor and Project Manager.

26. Facility and equipment to be provided by Authorized User:

The specified locality may provide furniture and equipment within limited workspace on a temporary basis. Permanent office space, furniture and equipment are the responsibility of the Supplier. While on-site at the project location, the specified locality will provide access to a copier, fax, the agency LAN and the internet (for up to two connections). Specified locality will also provide temporary desk space. The Supplier must provide any cell phones, personal computers or laptops required by the Supplier team. The specified locality's technical staff supporting the specified locality's network must verify that any personal computers or laptops meet minimum-security configuration standards (e.g., current virus protection) before any equipment may be connected to the agency's LAN.

Specified locality will also provide access to all documentation for the referenced projects.

Date: October 31, 2023

Attn: Mike Watson, Virginia Cybersecurity Planning Committee (VCPC) Chair, Mylam Ly

From: Tonya Estes, Director of Information Technology, Town of Culpeper

This introductory cover letter describes a *proposed* multi-phased plan to develop a Culpeper Cooperative "Regional Security Operations Center" (R-SOC). Attached is a Phase I grant request of $40k for services to be supported by the Town of Culpeper, VA.

There are two primary requests:

1. Please review and comment on this proposal as we seek Committee feedback. The goal is that this proposal will serve as a template for other local governments' regional initiatives.
2. Please provide guidance on the attached Phase I Proposal document as the exact structure and content for a Grant Request may need to comply with a format desired by the Committee.

The Town of Culpeper has been engaged with other local government directors, technology providers and cybersecurity professionals. We believe it is possible to rapidly and cost-effectively identify capability gaps and obtain recommendations to improve our cyber resiliency. At the same time, we seek to create a platform for building more organizational capability and associated talent-development pathways.

The Culpeper region is an ideal location for creating a prototype program that can merge Phase I activity with the immediate operational needs described below. The Town of Culpeper is representative of other local governments in Virginia in regards to our limited expertise and funds, both of which require immediate support to meet our cybersecurity needs.

Based on conversations with local government IT directors, cybersecurity assistance is the top priority for our organizations. Recent VaLGITE survey results corroborate this finding. As we operate on the front lines of the daily cybersecurity battle, we urge the state to support us in our essential work.

The Proposed Multi-Phase Strategy

Phase I

The Town of Culpeper (TOC) has experienced cybersecurity events that require immediate outside expertise to augment our existing capabilities. Attached is an example SOW to engage members of the Rampart workgroup (via CAS Severn) to conduct a Needs & Risk Assessment as the first step to immediately enhance cyber resiliency. Members of the Rampart workgroup actively work with the TOC I.T. Department and are familiar with their operational environment. The specific work described in the SOW will be funded by the Town of Culpeper.

The attached Phase I Planning grant proposal ($40K) will leverage the TOC SOW and expand the immediate Needs & Risk Assessment to include more ***detailed planning*** to establish on-going operational capability. The planning will identify higher-level capability gaps and the operational elements required to ensure sustainable security. This plan will present an analysis of the value of new technology and the structure required to create a form of on-going managed service provider (MSP). **Phase I to be completed within 4 months.**

In parallel to the planning activity, this Phase I proposal will include additional scoping work with nearby regional governments (in effect, completing a high-level needs assessment) to establish the architecture associated with a regional cooperative. We will define the value of an R-SOC platform as compared to other options as we develop a detailed implementation strategy, defined project scope, technology options and organizational structure.

NOTE: There are many services that cross the local government boundaries and there are undoubtedly many common issues.

Phase II

Provided there is interest from multiple regional governments (e.g. Counties of: Culpeper, Fauquier, Spotsylvania, Rappahannock, Madison, Town of Warrenton & others) Phase II will:

1. Fully develop the concept of an affordable Regional SOC (R-SOC) to establish a fundamentally new platform for data protection, cybersecurity, technology interface and more, as outlined in the strategic framework developed by the Committee. It is intended to utilize VITA resources to help secure technology contracts and expertise.
2. Develop the talent pipeline. It is anticipated that Germanna Community College, Culpeper Technical Education Center, University of Mary Washington and other Higher Educational institutions will participate in providing experiential programs as the Regional SOC is developed.
3. The R-SOC will intersect with existing programs across Virginia (VITA, VSP, Commonwealth Cyber Initiative (CCI), the VT Cyber Range, etc.) and will provide real-time, collaborative, cybersecurity information sharing among government entities.

A Phase II grant proposal will be developed with input from selected Committee members. It is projected that the cost for this phase will be approximately $200,000. After an estimated 6 months, a specific actionable plan can be implemented (organization structure, people, budget, and technology resources).

Phase III

Based on the findings of the work in Phase II, a Phase III "Execution" program will be implemented. It is projected that operational funding will be provided by both the Commonwealth and the individual local governments.

Next Generation Workforce Innoation & Development

Establish and maintain mechanisms to increase workforce innovation and opportunities within the localities and the state. Many localities are struggling to find skilled workers for open technology positions. This problem carries over to localities providing job opportunities to their citizens. The United States passed the Workforce Innovation and Opportunity Act (WIOA) into law on July 22, 2014. This law provides some guidance on how to address this issue.

The Rampart workgroup will continue to work with Post-Secondary/Higher Education institutions to create a pipeline of skilled staff to fill positions in public and private sector.

Attachment A	Planning Grant (Phase I) to establish a Culpeper Regional Security Operations Center
Attachment B	Town of Culpeper SOW with Rampart

Attachment B

to the

Culpeper Regional Security Operations Center Proposal

Town of Culpeper (TOC)

Cyber Security Posture Assessment

Statement of Work

Redacted Version

Submitted by:

Carl Dodson, Sr. Account Exec

cdodson@cassevern.com

804.397.9268

Proprietary Notice: The information contained in this proposal constitutes a trade secret and is confidential. It is furnished to Town of Culpeper Town of Culpeper (TOC) with the understanding that it will not be disclosed to other parties or vendors.

Executive Summary

CAS Severn, Inc. (CAS Severn) working with Hyper Critical Infrastructure (HCI) will provide professional services to Town of Culpeper (TOC) for a Cyber Security Posture Assessment.

Scope of Work

CAS Severn and HCI have partnered to perform for TOC expert Cyber Security Posture Assessment services. HCI will team with TOC in this endeavor by performing an onsite security posture review and assessment of the in-scope facilities and locations at a fixed price. HCI will also include previously performed assessment findings to evaluate any recommended modifications.

HCI will provide a cybersecurity posture assessment is a comprehensive evaluation of an organization's overall security measures and readiness to defend against cyber threats. This baseline view of your organization's security capabilities end-to-end. The purpose of this assessment is to build maturity in the organization's cyber resilience strategy to minimize the risk of cyber-attacks and data breaches.

Analyzing various aspects of the organization's IT infrastructure, policies, procedures, and personnel to identify gaps and weaknesses.

HCI understands that the scope is comprised of the following tasks:

- Identify critical assets to the business needs and the attack surface
- Cyber Security Technologies Assessment
- Network Security Review
- Vulnerability Scanning
- Incident Response Readiness
- Security Awareness Training Review
- Policy and Compliance Review
- Business Continuity and Disaster Recovery Planning
- Weekly security report of work and services performed

Task 1: Kickoff and Project Management:

- Meet with key stakeholders to clarify project timelines, current environment, needs and strategic direction.
- Perform interviews with Subject Matter Experts (SME) resources to understand current environment.

Task 2: Cyber Security Posture Assessment:

Documentation and Solution Reviews:

- Identifying critical assets to the business and the attack surface. This includes measuring the exposure to malicious attackers, in the form of endpoints, infrastructure, and the network, to understanding which assets carry the highest risk in the case of a breach. This can include a threat actor threat intelligence picture of the organization.
- Cyber Security Technologies Assessment: Understanding the technical picture of security systems as applied to critical security controls and coverage/completeness of deployment.
- Network Security Review: Analyzing firewall configurations, intrusion detection/prevention systems, and other network security measures.
- Vulnerability Scanning: Review of latest reports of full internal and external scans. If no scanning is performed, conducting scans to detect known vulnerabilities and weaknesses in systems and applications.
- Incident Response Readiness: Evaluating the organization's preparedness and ability to respond effectively to a cyber incident.
- Security Awareness Training Review: Assessing the effectiveness of training programs aimed at educating employees about cybersecurity best practices.
- Policy and Compliance Review: Evaluating adherence to established security policies, procedures, and industry compliance standards. This can also include overall security program objectives and daily processes.
- Business Continuity and Disaster Recovery Planning: Reviewing plans and procedures for maintaining operations in the event of a cyber incident.

Deliverables: Results Documentation

- After conducting these assessments, a detailed report is generated, outlining identified vulnerabilities, risks, and recommendations for improvement. This report serves as a roadmap for enhancing the organization's cybersecurity posture and reducing its exposure to cyber threats.

Project Duration

HCI in collaboration with Town of Culpeper will be strategically involved over the scope and during the project execution. The project duration is estimated over 2 to 3-week timeframe. This will create a highly effective and compliant program for Town of Culpeper.

HCI Responsibilities

HCI will provide technical direction and management of HCI SME and project personnel. This direction will provide a framework for project planning, communications, reporting, procedural and contractual activity. This activity includes:

Planning

1 Review the SOW and the contractual responsibilities of both parties with customer designated point of contact.
2 Maintain project communications and/or status of scope of work.
3 Establish documentation and procedural standards for the deliverables identified in the Scope of Work.

Project Tracking and Reporting

1 Review scope or project tasks, schedules, and resources and make changes or additions, as appropriate.
2 Review the HCI standard invoice format and billing procedure to be used on the project, with customer designated point of contact.
3 Conduct regularly scheduled project status meetings, if necessary.
4 Coordinate and manage the technical activities of HCI project personnel.

Assumptions:

CAS Severn Responsibilities

CAS Severn will provide technical direction and management of CAS Severn engineering and/or project personnel. This direction will provide a framework for project planning, communications, reporting, procedural and contractual activity. This activity includes:

Planning

1. Review the SOW and the contractual responsibilities of both parties with customer designated point of contact.
2. Maintain project communications and/or status of scope of work.
3. Establish documentation and procedural standards for the deliverables identified in the Scope of Work.

Project Tracking and Reporting

1. Review scope or project tasks, schedules, and resources and make changes or additions, as appropriate.
2. Review the CAS Severn standard invoice format and billing procedure to be used on the project, with customer designated point of contact.
3. Conduct regularly scheduled project status meetings, if necessary.
4. Administer the Change Control Procedure with customer designated point of contact.
5. Coordinate and manage the technical activities of CAS Severn project personnel.

Town of Culpeper (TOC) Responsibilities

Town of Culpeper (TOC) must designate an authorized individual who will be CAS Severn's primary contact and liaison. This person is responsible for all critical and non-critical engagement tasks including, but not limited to, the following:

1. Reserve facilities (conference rooms, labs, staging areas, etc.).
2. Provide any prerequisite documentation, configuration, information, and diagrams needed to complete the tasks described in the scope of work.
3. Provide access to grounds, facilities, and equipment as required.

In the case that the Scope of Work requires CAS Severn to have access to computer systems for purposes of installation, changes and/or analysis Town of Culpeper (TOC) will be responsible for the following:

1. Provide guidance on customer's operational security policies.
2. Provide access or assist CAS Severn project staff in gaining access to systems for the purpose of the work being performed.
3. Ensure that backups are completed of all data that may be affected by any work performed by CAS Severn.

Schedule

The project or scope of work schedule for CAS Severn technical and engineering services will be determined upon the receipt of written authorization from the Town of Culpeper (TOC) of the acceptance of this Statement of Work, the tasks ordered and the final approved project plan.

Change Order Procedures

Changes to this Statement of Work must be agreed upon by CAS Severn and the customer in writing and can be requested by contacting assigned Project Manager.

Attachment A - Grant Proposal

for consideration by the

Virginia Cybersecurity Planning Committee (VCPC)

to commence work to create the

Culpeper Regional Security Operations Center (R-SOC)

Introduction

This document describes Phase I of a proposed multi-phase proposal that will lead to establishing a cost efficient, high capability Regional Security Operations Center (R-SOC) for the local governments in the Culpeper regional area. This specific initiative will involve local government, the technology community and regional academic institutions.

It is hoped that the VCPC and representatives from other related Virginia initiatives and agencies (e.g. VACorp) will participate in the planning, design and "cooperative" structure of a sustained operational capability.

In this **$40,000 Phase I** program, the core supporter is the Town of Culpeper. However, Phase I will also involve other nearby localities as there are existing shared services across entity boundaries. Like many local governments, the Town recently experienced a cybersecurity incident that could have compromised critical data.

Local government entities have "modest" IT and cyber capabilities but they do not have the financial resources to rapidly define and install enhanced resiliency. As such, the Town of Culpeper recently engaged outside expertise to conduct a rapid "Needs and Risk" assessment related to their existing operations and capabilities (a redacted Statement of Work is provided as Attachment B). *This Phase I proposal is intended to build upon the Statement of Work that will be funded by the Town of Culpeper.*

The parties involved have direct experience with many local government systems and operations, including the Town of Culpeper, and expect to complete the Phase I program within 4 months of the start date.

It is hoped that this proposal can also serve as a template for other Virginia regions and be a learning prototype for the VCPC.

Proposed Sequence of Activity

Except for Phase I, future Phases are to be fully developed as part of the initial Phase I planning process.

Phase I:

Enhanced Cyber Security Needs and Risk Assessment for Town of Culpeper and interested Regional partners. Development of specific plans, including initial members and service capabilities for a Regional Security Operations Center (R-SOC). The planning will include Regional academic institutions in an effort to enhance the existing Talent Pipeline initiatives (GoVa, Commonwealth Cyber Initiative, Lab School programs, etc).

Phase 2:

Design and development of organizational structure for sustained operations of the Regional Security Operations Center (R-SOC).

Phase 3:

Onboarding of members and sustained operation of the R-SOC.

Overview:

The Town of Culpeper (TOC) has identified the need for enhanced technology, systems, protocols and associated talent to help protect the Town and surrounding regional members from cyber threats. Threats increase constantly, and stated simply, ***the Town and regional partners need immediate access to additional resources.*** To that end, TOC, in coordination with other regional governments and the technology community, has conceived this plan to create a Regional Security Operations Center (R-SOC).

Summary of Project Terms:

- Project Supporter(s): Town of Culpeper, Regional Planning District #9, Germanna Community College and CoVA (VCPC FEMA funding)
- Project Funding Request Amount: $40, 000 (Phase I)
- Matching Value (cash and in-kind): by Town of Culpeper ($10,000)
- Duration: Four Months from approval
- Project Team Participants:
    - Town of Culpeper
    - Germanna Community College
    - University of Mary Washington
    - Hyper-Critical Infrastructure (HCI), as CAS Severn Contractor
    - Virginia Cyber Planning Committee (VITA)

Project Activity and Outcomes:

The activity scope includes the following tasks:

- Needs & Risk Assessment - Assess current IT environment and understand requirements for the Town of Culpeper and Regional interested parties

- Inventory existing operations and services and identify vulnerabilities that are not currently addressed
- Design and create R-SOC design template
- Identify options to locate the R-SOC
- Develop options related to new equipment, software and manpower required
- Create a real-time, 7 x 24 R-SOC SOAR (Security/Orchestration/Automation/Response) Platform. The Platform allows for Monitoring, Management, Reporting, Remediation and Incident Response which are the primary functions of the Managed Services that the R-SOC delivers
- Establish Higher Education Partners in the local area, e.g. Germanna Community College & UMW
- Higher Education Partnership works with R-SOC to create cybersecurity Talent Pipeline = Cyber Launch Program
- Build cybersecurity consulting practice to parallel the R-SOC managed services
- Commence cyber training program as part of Cyber Launch talent development
- Incubate R-SOC via Region #9 Planning District as eventual support mechanism for regional expansion

The outcomes include the following:

- Creation of the Culpeper R-SOC
- Creation of a common cyber security platform
- Development of Cyber Launch (talentpPipeline)

Budget Details and Operations Plan – Phase I

Sources of Funds:

1. VCPC - $40,000

2. Town of Culpeper - $10,000 (both cash and in-kind support)

3. Contractors - $10,000 (in kind management time)

Uses of Funds:

1. Payment to outside contractors $40,000

VIRGINIA IT AGENCY

2024 Meeting Dates

Wednesday, January 17, 2024 10:00 AM-12:00 PM
Wednesday, February 21, 2024 10:00 AM-12:00 PM
Tuesday, March 26, 2024 1:00 PM-3:00 PM
Tuesday, April 23, 2024 1:00 PM-3:00 PM
Wednesday, May 15, 2024 10:00 AM-12:00 PM
Tuesday, June 25, 2024 1:00 PM-3:00 PM
Tuesday, July 23, 2024 1:00 PM-3:00 PM
Wednesday, August 21, 2024 10:00 AM-12:00 PM
Wednesday, September 18, 2024 10:00 AM-12:00 PM
Wednesday, October 30, 2024 10:00 AM-12:00 PM
Wednesday, November 20, 2024 10:00 AM-12:00 PM
Wednesday, December 18, 2024 10:00 AM-12:00 PM