Job Posting #:	05BT05162022	**Posting Type:**	Exempt - Pay Commensurate with Experience
Job Title:	Cybersecurity Solutions Architect	**Location:**	Fredericksburg, VA

JOB DESCRIPTION

POSITION PROFILE

The Cybersecurity Solutions Architect is responsible for cybersecurity solution design, implementation, and execution of advanced cybersecurity solutions and services. This opportunity is a part of our new wholly owned subsidiary of Rappahannock Electric Cooperative (REC), BrilliT.

ROLE AND RESPONSIBILITIES

- Responsible for cybersecurity solution design, implementation and execution of advanced cybersecurity solutions and services.
- Provide recommendations to Director regarding technology, resourcing, and development of internal and external security services.
- Ensure that internal and external security services are delivered on time with high levels of customer satisfaction.
- Ensures security infrastructure is well designed, resilient and available in a 24x7x365 critical infrastructure environment, including but is not limited to firewalls, intrusion prevention systems, servers, endpoint security, security incident and event management systems, networks, internet, and email filtering solutions.
- Continuously tests for operational integrity and effectiveness of cybersecurity defenses.
- Maintain subject matter expert awareness of latest risk, threats, and cybersecurity mitigation strategies.
- Collaborate with Security Operations Team
- Other duties as assigned.

QUALIFICATIONS AND EDUCATION REQUIREMENTS

Bachelor’s degree or experience equivalent in Computer Science, Information Technology, Cybersecurity, or other related technical fields required. Advanced professional certifications in cyber and information systems are required. A minimum of 5 years of progressive experience in cybersecurity and 12 years of network security engineering is required. Previous experience working the electric utility industry is highly desirable.

Must be proficient in planning, designing, implementing, securing and supporting a comprehensive enterprise security environment(s) along with on premise hybrid-cloud infrastructure. Must be able to work with related disciplines to ensure the consistent application of security policies and standards across all environments. Applicant shall endeavor to be knowledgeable of all emerging and existing security technologies and performance Service Level Agreements (SLAs). Applicant will assist all stakeholders to understand security infrastructure, resources and costs as they relate to projects and business initiatives.

Must be proficient in supporting a comprehensive enterprise cyber and information security program and while supporting external stakeholders. Must be able to work with related disciplines to ensure the consistent application of cybersecurity controls and standards across all technology projects, systems, and services of the enterprise. Applicant shall endeavor to be knowledgeable of all emerging and existing threat vectors, continually assessing deterrence posture, while maintaining existing cyber toolset to minimize risk. Applicant will assist all stakeholders to understand all cyber risk associated with prospective business-impacting decisions. In addition, applicant will contribute on all security incidents, ensuring loss is minimized, and effective actions are taken to thwart malicious activity to protect the cooperative, its employees, assets, and member-owners.

Must be able to exercise sound business judgment and operate independently and within a team environment. Must be proficient in the following areas:

- Experience leveraging common security control frameworks, security management frameworks, such as CIS, NIST 800-53 and ISO 27001.
- Experience in provisioning and managing complex enterprise firewalls, complex intrusion prevention systems, packet capture, packet analysis, and related skillsets.
- Experience leveraging major cloud providers such as AWS, Azure, and GCC to advance security objectives.
- Experience in the development, implementation and enforcement of information security policies, standards, procedures, and guidelines.
- Actively participate in incident response. Perform regular exercises and report results to executive management, auditors, and regulators.
- Proven ability to present and communicate with all levels of management, board of directors and staff.
- Experience with securing cloud computing assets as well as Software as a Service (SaaS)

Most of the work will be performed at the Fredericksburg office. Will require periodic travel throughout REC's territory. Occasional travel for seminars and training will be required with the possibility of overnight travel.

HOW TO APPLY:

Internal Applicants: Interested parties should submit a resume/cover letter to rechr@myrec.coop.
External Applicants: Use our https://www.myrec.coop/careers to apply for the opportunity. Please indicate the Job Posting ID #05BT05162022
Deadline: Open until filled
*The above statements are intended to describe the general nature and level of work being performed by people assigned to this classification. They are not intended to be construed as a complete list of all responsibilities, duties, and skills required of personnel so classified. BrilliT is an equal opportunity provider and employer.