AUBURN
Human Resources

Program Director, Southeast Region Cybersecurity Collaboration

JOB INFORMATION

Job Code	JA23
Job Description Title	Program Director, Southeast Region Cybersecurity Collaboration Center
Pay Grade	CSUC
Range Minimum	$0
33rd %	$0
Range Midpoint	$0
67th %	$0
Range Maximum	$0
Exemption Status	Exempt
Approved Date:	6/17/2025 9:51:12 AM

JOB FAMILY AND FUNCTION

Job Family:	Information Technology
Job Function:	Cyber Security

JOB SUMMARY

The Program Director of the Southeast Region Cybersecurity Collaboration Center (SERC3) leads one of the nation's premier applied research and testbed environments for operational technology (OT) cybersecurity in critical infrastructure. Ensures the driving of the strategic vision, growth, and operational excellence of SERC3, with a focus on defending America's industrial control systems and energy delivery systems against emerging cyber threats. Leads and oversee research initiatives focused on securing operational technology (OT) systems across various industries. Manages a team of researchers who develop innovative cybersecurity solutions and collaborate with industry partners and government agencies to enhance the security and resilience of OT systems. Manages and maintains a cybersecurity collaborative ecosystem and developing, building, and operating a new OT and cybersecurity research operations center at the Auburn Research Park that includes faculty, students, and contractors are additional duties.

RESPONSIBILITIES

- Leads the execution and expansion of SERC3, building a nationally recognized testbed and applied research ecosystem focused on securing operational technology and critical infrastructure.
- Serves as the principal investigator (PI) or co-PI on major research proposals and grants, drive funding development and strategic partnerships.
- Manages and maintains a cybersecurity collaborative ecosystem. Develops, builds, and operates an OT and cybersecurity research operations center.
- Leads the design and implementation of advanced research programs that align with DOE, DOD, DHS, and utility cybersecurity priorities.
- Fosters a collaborative and innovative research environment and manage a multidisciplinary team of engineers, researchers, students, and collaborators across the university and partner organizations.
- Develops and tests new cybersecurity technologies and methodologies and apply cybersecurity tools in operational environments.
- Operates an OT and cybersecurity research operations center at the Auburn Research Park.
- Conducts advanced research on cybersecurity threats and vulnerabilities regarding energy, water, and wastewater systems and provide expert advice on cybersecurity policies and best practices for the energy, water, and wastewater sectors. Oversees the development and integration of high-fidelity, closed-loop cyber-physical test environments replicating real-world utility and industrial control systems.
- Serves as a public-facing leader for SERC3, representing the center at national conferences, convenings, and with the media as needed. Builds and sustains relationships with senior leaders across federal agencies, national laboratories, utilities, and cybersecurity technology providers.
- Supervises assigned McCrary Institute staff as well as manage various partnerships with Auburn University faculty, consultants, and contractors to capture and execute sponsored research. Conduct annual reviews for assigned staff.

RESPONSIBILITIES

- Manages and oversees complex relationship dynamics between industry partners, government agencies, government customers, and academic institutions.
- Ensures research activities comply with relevant regulations and standards.
- Translates research outputs into actionable, testable, and deployable solutions for government and industry. Guides the transition of SERC3-developed tools and frameworks into commercial, open-source, or utility-adopted solutions.
- May require extensive travel between Auburn and external partners and customers.
- May assist others with writing grant and contract proposals.

The responsibilities listed above show the typical duties for jobs in this classification. Actual tasks may differ depending on the department's needs. Other similar duties may be assigned with discretion of the supervisor. Not every duty will apply to every position, and the amount of time spent on each task can change based on department needs.

SUPERVISORY RESPONSIBILITIES

Supervisory Responsibility	May be responsible for training, assisting or assigning tasks to others. May provide input to performance reviews of other employees.

MINIMUM QUALIFICATIONS

To be eligible, an individual must meet all minimum requirements which are representative of the knowledge, skills, and abilities typically expected to be successful in the role. For education and experience, minimum requirements are listed on the top row below. If substitutions are available, they will be listed on subsequent rows and may only to be utilized when the candidate does not meet the minimum requirements.

MINIMUM EDUCATION & EXPERIENCE

Education Level	Focus of Education		Years of Experience	Focus of Experience	
Bachelor's Degree	Computer Science, Software Engineering, Cybersecurity, Electrical Engineering, or related field.	and	10 years of	Experience in operational technology, critical infrastructure, power systems, and cybersecurity experience. Proven track record of leading technical and multidisciplinary teams and managing large-scale, complex research and operational projects. Experience in the energy and water sectors is highly desirable. Demonstrated success in securing external funding and building public-private partnerships.	Or
Master's Degree	Computer Science, Software Engineering, Cybersecurity, Electrical Engineering, or related field.	and	8 years of	Experience in operational technology, critical infrastructure, power systems, and cybersecurity experience. Proven track record of leading technical and multidisciplinary teams and managing large-scale, complex research and operational projects. Experience in the energy and water sectors is highly desirable. Demonstrated success in securing external funding and building public-private partnerships.	

MINIMUM KNOWLEDGE, SKILLS, & ABILITIES

Knowledge of generally accepted information/cybersecurity principles and practices with the ability to apply that knowledge to perform complex and non-routine specialized OT security analysis functions.	
Ability to remain up to date with privacy and security regulations.	
Ability to recognize, analyze, and solve a variety of problems.	
Strong communication and presentation skills.	

PHYSICAL DEMANDS & WORKING CONDITIONS

Physical Demands Category:	Healthcare & Safety

PHYSICAL DEMANDS

Physical Demand	Never	Rarely	Occasionally	Frequently	Constantly	Weight
Standing					X	
Walking					X	
Sitting		X				
Lifting				X		
Climbing			X			
Stooping/ Kneeling/ Crouching				X		
Reaching				X		
Talking					X	
Hearing					X	
Repetitive Motions					X	
Eye/Hand/Foot Coordination					X	

WORKING ENVIRONMENT

Working Condition	Never	Rarely	Occasionally	Frequently	Constantly
Extreme temperatures		X			
Hazards				X	
Wet and/or humid		X			
Noise					X
Chemical				X	
Dusts			X		
Poor ventilation		X			

Vision Requirements:

Ability to see information in print and/or electronically and distinguish colors.