AUBURN
Human Resources

Deputy Director, Applied Research & Services and Director, Edge Lab

JOB INFORMATION

Job Code	JA34
Job Description Title	Deputy Director, Applied Research & Services and Director, Edge Lab
Pay Grade	CS09
Range Minimum	$120,970
33rd %	$161,290
Range Midpoint	$181,450
67th %	$201,610
Range Maximum	$241,930
Exemption Status	Exempt
Approved Date:	4/15/2026 4:52:42 PM

JOB FAMILY AND FUNCTION

Job Family:	Information Technology
Job Function:	Cyber Security

JOB SUMMARY

The Deputy Director, Applied Research & Services serves as the principal technical authority for the McCrary Institute and provides supervisory and strategic leadership over the Edge Lab and all technical capabilities housed within it, including the Southeast Region Cyber Collaboration Center (SERC3) and the Alabama Cybersecurity Intelligence Center (ACIC). Leads all technical staff, cybersecurity analysts, research engineers, and operational personnel — including the Field Deployment and SOC Manager and all subordinate positions — and is accountable for the strategy, execution, and performance of McCrary's applied research mission.

Reporting directly to the Associate Director and COO of the McCrary Institute, the Deputy Director, Applied Research & Services serves as a member of the Institute's executive leadership team. Works in close coordination with the Deputy Director for Business Development & Partnerships, the Program Managers of McCrary's three directorates (Energy & Infrastructure, Defense & National Security, and State & Local), and the COO on matters of strategy, sponsor partnerships, and program execution. Contributes to McCrary's mission to advance national security through applied cybersecurity research, operational capabilities, and trusted partnerships with federal agencies, the Department of Defense, the intelligence community, and critical infrastructure operators.

RESPONSIBILITIES

- Enterprise Technical Leadership
  - Serves as the senior technical executive of the McCrary Institute, accountable to the Associate Director and COO for all research, development, and operational technology capabilities.
  - Provides strategic direction for the Edge Lab across all capability pillars: HIL testbed operations, managed cybersecurity services, AI/ML defense research, and critical infrastructure resilience.
  - Defines and executes the Institute's technical capability roadmap in alignment with federal sponsor priorities, national cybersecurity strategy, and Auburn's research mission.
  - Represents McCrary's technical capabilities in external engagements with federal agencies, congressional stakeholders, national laboratory partners, and industry.
  - Possesses architecture-level understanding of artificial intelligence, autonomous agents, and agent workflows — with particular emphasis on how agents consume data and interact with APIs — and apply that understanding to McCrary's research agenda and technical capability development.
  - Participates in select hands-on software development and technology integration activities alongside students and staff, modeling a culture of applied technical leadership within the Edge Lab.
  - Works in close coordination with the Deputy Director for Business Development & Partnerships to align technical capabilities with capture strategy and sponsor engagement, and with the COO on resource allocation, operational priorities, and organizational planning.

RESPONSIBILITIES

- Supervisory Leadership — Edge Lab & Technical Staff
  - Provide supervisory and operational leadership over all Edge Lab personnel, including the Field Deployment and SOC Manager (ACIC), research engineers, senior cyber analysts, OT/ICS specialists, and all technical and cybersecurity operations staff.
  - Establishes team structure, define roles and responsibilities, and build the staffing plan required to execute McCrary's growing portfolio of federal contracts and sponsored research.
  - Leads hiring, onboarding, and performance management for all technical positions, in coordination with McCrary's operations staff and Auburn HR.
  - Develops and enforces lab operating procedures, security posture requirements, and quality standards across all Edge Lab environments.

- SERC3 / Critical Infrastructure Systems Laboratory (CISL)
  - Leads the design, build-out, and operational maturation of CISL — McCrary's multi-sector HIL testbed — ensuring it delivers repeatable, sponsor-grade research outcomes across power, water, telecom, data center, agriculture, and renewable energy domains.
  - Oversees execution of DOE CESER SERC3 program deliverables, including the cooperative agreement with coordinated research through Oak Ridge National Laboratory (ORNL) and integration with the CyTRICS program.
  - Collaborates closely with the Energy & Infrastructure and Defense & National Security Program Managers to ensure technical execution aligns with sponsor deliverables and contract requirements.
  - Maintains technical accountability for all OT/ICS research infrastructure, STIG hardening, zero-trust architecture requirements, and segmentation standards across CISL environments.
  - Drives field deployment of McCrary's DCEI capability and support Q2 operational unveiling milestones.

- ACIC — Cybersecurity Operations
  - Provides executive oversight of the Alabama Cybersecurity Intelligence Center (ACIC), including 24/7 MDR/SOC operations, EDR/SIEM platforms, and vCISO service delivery.
  - Ensures operational quality, service level compliance, and technical innovation across ACIC's managed cybersecurity service portfolio, including CrowdStrike, Splunk, and TekStream integrations.
  - Partners with the State & Local Program Manager to support ACIC's grant participant base, ensuring service delivery meets program and sponsor requirements.
  - Supports the Army ASA(ALT) Defense Industrial Base (DIB) Security pilot program and other emerging DoD engagements requiring operational cybersecurity delivery.

- Sponsored Research & Federal Contract Execution
  - Serves as technical authority for McCrary's sponsored research portfolio across active government sponsors including DOE, DoD, CISA, DHS, AOIT, and others.
  - Collaborates with the three directorate Program Managers (Energy & Infrastructure, Defense & National Security, and State & Local) to align technical capabilities with sponsor deliverables, ensuring on-time, on-budget execution with P&L accountability.
  - Partners with the Deputy Director for Business Development & Partnerships to support federal business development with technical content, capability demonstrations, and sponsor-facing briefings.
  - Coordinates with Auburn's Office of Sponsored Programs (OSP) on contract compliance, IP management, and grant administration requirements.

- Research & Technology Commercialization
  - Drive McCrary's applied research agenda from concept through delivery, including AI-enabled threat detection, OT/ICS security architecture, and critical infrastructure resilience methodologies.
  - Identify and develop pathways for commercialization of McCrary-developed technologies and methodologies, including technology transfer, licensing, and public-private partnership models.
  - Manage and grow partnerships with national laboratories (ORNL, INL, Sandia), industry technology providers, and defense research organizations.
  - Oversee development and maintenance of technical documentation, research publications, and capability briefing materials consistent with classification and IP requiremen

- Policy Integration & External Positioning
  - Collaborate with McCrary's policy and communications leadership to translate technical capabilities into policy-relevant insights and public-facing messaging.
  - Represent McCrary in conferences, congressional briefings, and interagency forums on critical infrastructure cybersecurity, OT/ICS security, and emerging technology threats.
  - Maintain and expand McCrary's network of federal sponsor relationships and cleared community partnerships.

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	Full supervisory responsibility for other employees is a major responsibility and includes training, evaluating, and making or recommending pay, promotion or other employment decisions.

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, Electrical Engineering, Cybersecurity, or a related technical field; advanced degree or equivalent professional experience strongly preferred.	and	10 years of	experience in cybersecurity, critical infrastructure security, OT/ICS, or related technical fields, including significant leadership roles.	Or

MINIMUM KNOWLEDGE, SKILLS, & ABILITIES

Knowledge in the intelligence community, national laboratories, or defense research organizations.	And
Deep OT/ICS security expertise, including STIG hardening, zero-trust architecture for operational technology, and ICS/SCADA vulnerability research.	And
Knowledge of FIPS 140-2/140-3 cryptographic standards and secure by design engineering for mission-critical systems.	And
Familiarity with DOE CESER, CISA, DHS, DARPA, or Army research programs and acquisition processes.	And
Knowledge of commercial platform delivery in classified or sensitive environments.	And
Record of technical publication, patent development, or technology commercialization.	And
Demonstrated knowledge of building and operating technical lab or testbed environments, including hardware-in-the-loop or cyber-physical systems.	And
Demonstrated knowledge of leading and supervising technical teams in a high-performance, mission-driven environment.	And
Demonstrated knowledge of federal agency partnerships, sponsored research contracts, or DoD/intelligence community program.	

MINIMUM LICENSES & CERTIFICATIONS

Licenses/Certifications	Licenses/Certification Details	Time Frame	Required/ Desired	
Other	Active Secret security clearance	Upon Hire	Required	

PHYSICAL DEMANDS & WORKING CONDITIONS

Physical Demands Category:	Other

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 cold		X			
Extreme heat		X			
Humidity		X			
Wet		X			
Noise		X			
Hazards		X			
Temperature Change		X			
Atmospheric Conditions		X			
Vibration		X			

Vision Requirements:

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