AUBURN
Human Resources

Chief Research Security Office

Job Description

JOB INFORMATION

Job Code	HC85
Job Description Title	Chief Research Security Office
Pay Grade	LC17
Range Minimum	$147,510
33rd %	$196,680
Range Midpoint	$221,260
67th %	$245,850
Range Maximum	$295,020
Exemption Status	Exempt
Approved Date:	5/25/2021 4:53:53 PM
Legacy Date Last Edited	1/26/2022

JOB FAMILY AND FUNCTION

Job Family:	Legal, Compliance & Audit
Job Function:	Research Security

JOB SUMMARY

The Chief Research Security Officer (CRSO) reports to the Vice President of Research & Economic Development and provides senior level direction, counsel, management, administrative and fiscal oversight for the Office of Research Security Compliance. Serves as the Facility Security Officer (FSO), Export Control Empowered Official, Contractor Special Security Officer (CSSO) and Insider Threat Senior Official for the University. Serves as a critical leader on the Research leadership team and at the University. Collaborates with Research leadership across campus to develop and execute research security.

RESPONSIBILITIES

- Provides overall management and proactive direction for the Office of Research Security Compliance to include providing leadership, development, and implementation of strategic plans, establishment of priorities for research security initiatives and administration and fiscal oversight. Provides day-to-day guidance to staff and makes decisions that ensure the effective operation of the Research Security Compliance Department.
- Provides advice and counsel to the Vice President of Research and Economic Development, Provost, Executive Vice President and President on strategic and operational issues as well as regulatory requirements related to research security protection and administration.
- Manages the facility security program to ensure compliance with federal security regulations as well as contractual agreements regarding the protection of classified, export control, proprietary, insider threat, controlled unclassified information and all other aspects the university research portfolio. Ensures full compliance with the National Industrial Security Program Operating Manual (NISPOM), Intelligence Community Directives (ICD), counterintelligence (CI), Cybersecurity laws, policies, and regulations, and all applicable federally funded government research activities.
- Implements and monitors the AU Insider Threat Program (ITP). Provides oversight to the Insider Threat Networking Group (ITNG). Responds to and investigates program security infractions and violations. Reports security infractions and violations to the appropriate government agencies.
- Conducts internal risk assessments of the AU classified, export control, insider threat, controlled unclassified information and research cybersecurity programs between scheduled government audits ensuring research information is being properly protected in accordance with government directives.
- Leads and directs Auburn’s counterintelligence program. Protects University assets from undue foreign influence and foreign interference and serves as AU’s primary point of contact with federal law enforcement and intelligence community agencies on research security related matters.
- Oversees the implementation and management of the University’s research cybersecurity program to include strategic planning, conducting risk assessments, COMSEC management and compliance with numerous cybersecurity directives and regulations.

RESPONSIBILITIES

- Serves as the Export Control Empowered Official ensuring compliance with export control laws and national security initiatives.
- May perform other duties as assigned by supervisor.

SUPERVISORY RESPONSIBILITIES

Supervisory Responsibility	Supervises others with full supervisory responsibility.

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	Degree in Cyber, Information Security, Engineering, Legal, International Studies, or related field.	And	12 years of	Direct relevant experience in intelligence, counterintelligence or information security; ten (10) years experience must be in management, training, compliance and protection of US Government-controlled information. Experience must show progressively increasing levels of responsibility and accountability.	Or
Master's Degree	Degree in Cyber, Information Security, Engineering, Legal, International Studies, or related field.	And	10 years of	Direct relevant experience in intelligence, counterintelligence or information security; ten (10) years experience must be in management, training, compliance and protection of US Government-controlled information. Experience must show progressively increasing levels of responsibility and accountability.	

MINIMUM KNOWLEDGE, SKILLS, & ABILITIES

Advanced knowledge and advanced understanding of US government security regulations and intelligence/counterintelligence operations to include the implementation and management of compliance processes, procedures, and best practices.	
Advanced written and verbal communication skills and the ability to present effectively to small and large audience of varying experience and operational backgrounds.	
Strong relationship building and negotiation skills.	
Demonstrated ability to identify problems, analyze courses of action and implement solutions.	
Demonstrated ability to expertly handle sensitive discussions with discretion, strong personal ethics commitment and sound judgment.	
Consistently models high standards of honesty, openness, and respect for the individual.	
Demonstrated ability to mentor and lead Research Security Compliance personnel.	
Experience working in an organization with integrated, cross-functional work teams is necessary.	
Demonstrated effectiveness in a operational environment with concurrent tasks and changing priorities and resources.	
Ability to conduct comprehensive risk assessments and identify security vulnerabilities related to information security, personnel security and physical security protocols.	

MINIMUM LICENSES & CERTIFICATIONS

Licenses/Certifications	Licenses/Certification Details	Time Frame	Required/ Desired	
	Must be a U.S. citizen with a current U.S. government Top Secret security clearance or have a current U.S. government Secret security clearance with the ability to obtain a U.S. government Top Secret security clearance.	Upon Hire	Required	And
	Completion of Defense Counterintelligence and Security Agencies Facility Security Officers Course for Possessing Facilities.	Upon Hire	Required	

REQUIRED PRE-EMPLOYMENT SCREENINGS

Security Clearance

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.