U.S. Senate Sergeant at Arms
Human Resources

Vacancy Announcement

When applying for this position, refer to "POSITION # 5271" on your application package.

POSITION:	Cybersecurity Supervisor (#5271)
DEPARTMENT:	Cybersecurity / Information Assurance / Awareness
REQUIREMENTS:	See attached Position Description
SALARY RANGE:	$98,953 - $148,424
CONTACT:	U.S. Senate Sergeant at Arms, Human Resources Senate Hart Building SH-142 Washington, DC 20510 Phone: (202) 224-2889 Fax: (202) 228-2965 Email: resumes@saa.senate.gov
POSTING DATE:	Thursday, September 20, 2018
DEADLINE FOR APPLICATIONS:	Thursday, October 04, 2018

All applicants must submit a U.S. Senate Sergeant at Arms Application for Employment with a cover letter and current resume to the Human Resources Department.

VETERANS EMPLOYMENT OPPORTUNITY ACT

Hiring for this position is governed by the Veterans Employment Opportunity Act of 1998 ("VEOA"), as made applicable by the Congressional Accountability Act of 1995 ("CAA"). Pursuant to the VEOA, qualified applicants who are not current employees of the Office of the Senate Sergeant at Arms and who are disabled or who have served on active duty in the Armed Forces during certain specified time periods or in certain military designated campaigns ("veterans") may be eligible to receive a preference over non-veterans in hiring decisions. Family members of veterans may also be eligible to receive a veterans' preference if the veteran cannot claim his or her veterans' preference.

To be eligible for a veterans' preference, applicants must meet all of the requirements set forth in the VEOA and applicable regulations. Those eligibility requirements are summarized in the Application for Veterans' Preference, which is available at www.senate.gov/saaemployment.

If claiming a veterans' preference, an applicant must indicate that he/she is preference eligible on the application or resume and must submit a completed copy of the Application for Veterans' Preference along with the supporting documentation specified on that form. If the Office of the Senate Sergeant at Arms does not receive the Application for Veterans' Preference and supporting documentation by the closing date, the applicant's claim for a veterans' preference may be denied.

Applicants may obtain a copy of the Office's Veterans' Preference In Appointments policy by submitting a written request to resumes@saa.senate.gov.

Individuals who are entitled to a veterans' preference are invited to self-identify voluntarily. This information is intended solely for use in connection with the obligations and efforts of the Office of the Senate Sergeant at Arms to provide veterans' preference to preference-eligible applicants in accordance with the VEOA. An applicant's status as a disabled veteran and any information regarding an applicant's disability, including the applicant's medical condition and history, will be kept confidential and will be collected, maintained and used in accordance with the Americans with Disabilities Act of 1990, as made applicable by section 102(a)(3) of the CAA, 2 U.S.C. §1302(a)(3). An applicant who declines to self-identify as a disabled veteran and/or to provide information and documentation regarding his/her disabled veteran's status will not be subjected to an adverse employment action, but the individual may be ruled ineligible for a veterans' preference.

CYBERSECURITY SUPERVISOR

NATURE OF WORK

This is professional and managerial work planning and managing the work of a small Cybersecurity team. Work may include supervising a combination of technical, professional and/or contract staff. Work also involves project management, providing input to the team's budget, providing forecasts, cost/benefit analysis and technical recommendations to senior management. This position is a managerial position under the direction of a Branch Manager and supports oversight and coordination of the cybersecurity program.

EXAMPLES OF WORK

(This list is not absolute or restrictive, but indicates approximate duties and responsibilities, which may be redefined pursuant to operational needs.)

- Supervises team staff by providing direction, setting priorities, assisting with problem resolution, reviewing and evaluating work, counseling staff, and conducting performance reviews.
- Establishes team goals, assigns team leaders, and administratively and technically directs the work of staff.
- Conducts annual reviews, assigning performance ratings, recommending awards, arranging training, and managing performance improvement plans.
- Identifies team training needs and conveys training recommendations to upper management.
- Develops team work plans and assigns projects, tasks, resources, deadlines and priorities to staff; monitors work progress, adjusts project schedules and updates status of work on a regular basis to the appropriate Branch Manager.
- Confers with other sections, divisions, departments, and vendors to gather and disseminate information; represents the SAA organization in discussions of projects; participates in organizational decision-making.
- Facilitates the creation and modification of all cybersecurity compliance policies and processes applicable to the Supervisor's team.
- Maintains a cybersecurity framework for conducting team services and/or operations to periodically assess the regulatory, commercial, organizational, inherent and residual level of compliance and risks.
- Identifies and resolves any issue of noncompliance with governing standards and frameworks applicable to the team.

PHYSICAL DEMANDS AND WORKING ENVIRONMENT

Work requires extended periods of confined sitting and hand-eye coordination working with computers. Expected to work unusual and perhaps unexpected hours during a Continuity of Operations.

MINIMUM QUALIFICATIONS

Work requires a Bachelor's Degree in computer science, telecommunications, or a related technical field, and seven to nine years of experience within a Certified Information Systems Security Professional (CISSP)-type environment, with at least two years of work in a supervisory capacity; or any equivalent combination of education and experience that provides the following knowledge, skills and abilities:

- Knowledge of laws, regulations, policies, and ethics as they relate to the cybersecurity area of expertise.
- Knowledge of current and emerging technologies and/or tools utilized in area of assigned cybersecurity discipline.
- Knowledge of cybersecurity concepts required.
- Skill in making processes more efficient.
- Ability to plan, supervise, assign and review the work of a combination of professional, technical and/or contract staff.
- Ability to apply critical thinking skills to identify strengths, weaknesses, alternative solutions, conclusions and approaches to problems.
- Ability to set goals, plans, and monitor projects.
- Ability to maintain proper documentation, relevant records and archives in an orderly, transparent fashion.
- Ability to display good judgment, work with a sense of urgency and demonstrate a commitment to high standards of ethics, regulatory compliance, customer service and business integrity.
- Ability to work well with a diverse client base.
- Ability to work in a heavily regulated and/or audited environment.
- Ability to communicate effectively, both orally and in writing.

LICENSES, CERTIFICATION AND OTHER REQUIREMENTS

Ability to obtain a security clearance.

Cybersecurity Supervisor Addendum

Information Assurance Branch - Awareness

Examples of Work:

- Assess effectiveness and efficiency of instruction according to ease of instructional technology use and student learning, knowledge transfer, and satisfaction
- Coordinate with internal and external subject matter experts to ensure existing qualification standards reflect organizational functional requirements and meet industry standards
- Create interactive learning exercises to create an effective learning environment
- Create training courses tailored to the audience and physical environment
- Develop the goals and objectives for cyber curriculum
- Establish and maintain communication channels with stakeholders
- Plan instructional strategies such as lectures, demonstrations, interactive exercises, multimedia presentations, video courses, web-based courses for most effective learning environment in conjunction with educators and trainers
- Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals
- Provide policy guidance to cyber management, staff, and users
- Review and apply organizational policies related to or influencing the cyber workforce
- Review existing and proposed policies with stakeholders
- Review, conduct, or participate in audits of cyber programs and projects
- Seek consensus on proposed policy changes from stakeholders
- Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce

Knowledge, Skills and Abilities:

- Knowledge of business or military operation plans, concept operation plans, orders, policies, and standing rules of engagement
- Knowledge of computer based training and e-learning services
- Knowledge of current and emerging threats/threat vectors
- Knowledge of enterprise incident response program, roles, and responsibilities
- Knowledge of media production, communication, and dissemination techniques and methods, including alternative ways to inform via written, oral, and visual media
- Knowledge of organization's risk tolerance and/or risk management approach
- Knowledge of privacy disclosure statements based on current laws
- Knowledge of the National Cybersecurity Workforce Framework, work roles, and associated tasks, knowledge, skills, and abilities
- Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure)
- Ability to conduct training and education needs assessment
- Ability to develop clear directions and instructional materials
- Ability to develop curriculum for use within a virtual environment
- Ability to develop curriculum that speaks to the topic at the appropriate level for the target audience
- Ability to leverage best practices and lessons learned of external organizations and academic institutions dealing with cyber issues
- Ability to monitor advancements in information privacy technologies to ensure organizational adaptation and compliance
- Ability to monitor and assess the potential impact of emerging technologies on laws, regulations, and/or policies