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.

INFORMATION TECHNOLOGY BRANCH MANAGER

NATURE OF WORK

This is managerial and administrative work planning, organizing and managing a major information technology branch within the SAA. Work includes planning, defining and prioritizing work of several units; directing and managing professional and technical staff; developing, in conjunction with other department management, branch policies and procedures; and developing and monitoring budgets. Position is responsible for assisting in the formulation of department strategic and tactical plans and participates in the Senate strategic planning effort. Work is performed with considerable latitude to establish and direct work to meet organizational objectives. Work is performed under the general supervision of the Director of Technology Development Services.

EXAMPLES OF WORK

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

- Manages the daily operations of the branch, including setting priorities, allocating resources, managing personnel and providing general oversight of projects.
- Manages and supervises staff recruitment, training, motivation and performance evaluation.
- Works with customers to develop new requirements, resolves complaints, provides information and responds to requests; serves as technical advisor to the Director on matters pertaining to the branch.
- Develops strategic and operational plans; provides project direction, coordination and resource allocation.
- Develops, implements and monitors the branch budget and budget expenditures; develops budget forecasts; provides input into budget testimony.
- Prepares and maintains status reports; approves purchases; and performs related administrative requirements.
- Develops standards for technical performance of information technology outsourcing; conducts regular reviews of vendor's contract performance.
- Represents the SAA in meetings and activities with senior management of other Senate or legislative branch organizations.
- Participates in user groups, task forces, and steering committee activities with other Senate or legislative branch organizations.
- Establishes policies and practices governing the operation, services and staff of the branch.
- Serve as the Director in his/her absence.

The statements contained herein reflect general details necessary to describe the principal functions of this class, knowledge and skill typically required and the physical demands and working conditions, but should not be considered an all-inclusive listing of work requirements.

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 COOP event.

MINIMUM QUALIFICATIONS

Work requires a Bachelor's Degree in Information Systems/Computer Science or a related technical field; and eight to ten years of experience in information technology management; or any equivalent combination of education and experience that provides the following knowledge, abilities and skills:

- Knowledge of current and emerging technologies and principles of information technology management.
- Knowledge of capabilities and requirements of various computer platforms in centralized, distributed, client server and stand alone operating environments.
- Knowledge of the current principles and practices of public administration, including governmental procurement, contracting, personnel, and capital project management.
- Knowledge of project life cycle methodologies.
- Ability to define strategic plans and objectives.
- Ability to analyze complex issues and make recommendations for action.
- Ability to plan, direct, manage, and supervise programs and activities of several technical units.
- Ability to plan, assign and review the work of technical, professional and managerial personnel.
- Ability to manage multi-million dollar annual budgets.
- Ability to establish and maintain effective working relationships with Senate office and committee staffs, the public, and SAA directors, managers, supervisors, and subordinates.
- Ability to communicate effectively.

LICENSES, CERTIFICATION AND OTHER REQUIREMENTS

None.

The statements contained herein reflect general details necessary to describe the principal functions of this class, knowledge and skill typically required and the physical demands and working conditions, but should not be considered an all-inclusive listing of work requirements.

INFORMATION TECHNOLOGY BRANCH MANAGER, IT SECURITY

This position plans, organizes and directs the activities of a small, experienced, and advanced professional and technical staff responsible for the delivery of high quality information and cyber security services to the U.S. Senate; develops, in conjunction with other department management, a work atmosphere of cooperation and collaboration; and participates in planning and development of annual goals and objectives for information and cyber security. Position is responsible for managing IT security systems, processes, and services including incident management, network security monitoring, vulnerability management, patch management; antivirus, and additional technologies to ensure maintenance of data confidentiality, integrity and systems availability within the Senate information technology infrastructure. More specifically, the position:

- Manages the daily operations of the branch, including setting priorities, allocating resources, managing personnel and providing general oversight of projects.
- Leads and participates in the development, maintenance, and publishing of security policies, standards and guidelines.
- Leads development and maintenance of information security and risk awareness programs for all employees, contractors and approved system users.
- Provides risk guidance for key projects and initiatives, including the evaluation and recommendation of technical controls and security measures.
- Understands the computing, access, data security concepts, and practices to work with the IT infrastructure, application development, and network engineering teams to ensure that the hardware, software, and practices employed within the environment are sound and appropriate.
- Provides leadership for design, deployment and operation of security management software and hardware devices including, but not limited to: antivirus defense, intrusion detection, authentication and access control systems, network scanning and vulnerability assessment, etc.
- Provides leadership, assistance, and subject matter expertise to address and mitigate security incidents.
- Liaises with various teams/departments across the organization to ensure alignment of IT Security with technology roadmaps and related activities.
- Serves as a Subject Matter Expert on current security threats and industry best practices.
- Leads development and implementation of measurable security metrics for projects and operations.
- Works to obtain support and acceptance of security policies and practices throughout the Senate.

A Bachelor's degree in Information Systems/Computer Science with an information security emphasis - preferred, or equivalent relevant experience – required; and eight to ten years of experience in information technology management; or any equivalent combination of education and experience. Masters degree in the field is a plus.

Position requires extensive experience in security architecture design, implementation and operations/maintenance. Demonstrated experience with a variety of IT security technologies including but not limited to: Intrusion Detection and Prevention; Security Event Management, Vulnerability Management, End Point Security, Anti-Virus, Firewalls, and Malware Analysis. Experience in developing security policies and procedures. Experience in performing security risk assessments and in assessing security of an IT environment.

Industry specific/professional certifications - helpful. Must obtain and maintain a clearance.