U.S. Senate Sergeant at Arms
Human Resources

Vacancy Announcement

POSITION:	**Principal Identity and Access Management Software Engineer #1001**
DEPARTMENT:	Process Management, and Innovation / Identity and Access Management
SUMMARY:	This is advanced professional work in a highly-specialized Information Technology discipline designing, implementing, and supporting identity and access management systems, including integration and provisioning of numerous Senate applications. The incumbent serves as the primary software engineer responsible for the functionality on Identity Access Management's (IAM) roadmap. Work includes researching and resolving issues escalated by other support groups, as well as recommending long-term strategic directions for Senate technology.
LICENSES AND CERTIFICATIONS:	Ability to obtain and maintain a security clearance.
SALARY RANGE:	$97,000 - $145,498
HOW TO APPLY:	All applicants must use the link below and follow instructions. https://sen.gov/YP4Z
POSTING DATE:	Monday, November 30, 2020 **(Until Filled)**

U.S. Senate Sergeant at Arms, Human Resources * Senate Hart Building SH-142, Washington, DC 20510 * Phone: 202-224-2889

PRINCIPAL IDENTITY AND ACCESS MANAGEMENT SOFTWARE ENGINEER

NATURE OF WORK

This is advanced professional work in a highly-specialized Information Technology discipline designing, implementing, and supporting identity and access management systems, including integration and provisioning of numerous Senate applications. The incumbent serves as the primary software engineer responsible for the functionality on Identity Access Management's (IAM) roadmap. Work includes researching and resolving issues escalated by other support groups, as well as recommending long-term strategic directions for Senate technology. Work is performed under the general direction of the manager.

EXAMPLES OF WORK

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

- Leads IIQ software development projects utilizing Java, JavaScript, C++, BeanShell, and out-of-box connectors
- Provides expert-level technical support for identity and access management systems to IAM, other technical staff, divisions and departments, and vendors.
- Works with the team to identify requirements, understand the impact on As-Is processes, facilitate effective design, configure IIQ to meet the requirements, preferably utilizing out-of-the-box (OOB) capabilities, and complete unit testing.
- Customizes, tests, recommends, and configures identity management system.
- Participates with the team to complete acceptance and integration testing; approves new IAM software releases; develops IAM installation plans; provides guidance in vendor oversight.
- Resolves critical and complex systems, applications or communications performance problems.
- Participates with the team to plan strategic direction for the Senate in the areas of IAM software and networking systems; monitors the impact of technological developments; and identifies emerging technologies.
- Participates in product evaluations and technical studies and task forces; works with the team to analyze new technology for its impact on the Senate environment; tests impact of new releases on Senate supported platforms; develops product configuration standards for use in the Senate environment.
- Works with the team to research, evaluate, and recommend software products for identity and access management.
- Provides expert technical guidance for system administration and maintenance on IAM systems.

REVISED: 11/4/2020 *CODE: 1969*

- Participates with the team to align roles and groups within the larger governance framework and unified provisioning of the IAM system.
- Provides Tier 3 support to the IAM support team.

PHYSICAL DEMANDS AND WORKING ENVIRONMENT

Work requires extended periods of confined sitting and hand-eye coordination working with computers. Work exposes the incumbent to a number of time-sensitive technical issues that require immediate resolution.

MINIMUM QUALIFICATIONS

Work requires a Bachelor's Degree in Business Administration, Engineering or in Computer Science or a related technical area with three years of experience configuring, deploying and maintaining IIQ in an enterprise setting, including experience with out-of-the-box connectors (for example, Active Directory), roles, certifications and workflows; three years of experience in IAM; five years of development experience using Java, JavaScript, C++; and three years of SQL experience.; three years of system, network, development, maintenance and support experience; or any equivalent combination of education and experience that provides the following knowledge, abilities and skills:

- Ability to troubleshoot and understand critical issues and bring appropriate resolution to complex problems.
- Ability to learn and adapt quickly to new circumstances.
- Ability to work collaboratively.
- Ability to communicate effectively.

LICENSES, CERTIFICATION AND OTHER REQUIREMENTS

Ability to obtain and maintain a security clearance.

Principal Identity and Access Management Software Engineer Addendum

Currently, the SAA-CIO’s pandemic posture authorizes the majority of its employees the privilege of full-time telework. This position may be eligible for full-time telework post-pandemic if the employee continues to meet SAA requirements and complies with the SAA’s Telework policy.

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.