



U.S. Senate Sergeant at Arms Human Resources

Vacancy Announcement

POSITION:

Cybersecurity Principal Specialist - Host #44

DEPARTMENT:

Cybersecurity / Systems Support / Host

SUMMARY:

This is advanced professional work coordinating, developing, evaluating, and implementing cybersecurity standards and procedures to protect centralized and distributed information systems, applications, and data. Work may include leading a team of employees responsible for providing a full range of cybersecurity support to Senators, Senate Committees and other Senate offices. Work includes coordinating and re-directing work assignments to ensure timelines and customer needs are met. The incumbent assists the supervisor in coordinating and directing staff work assignments. The incumbent may assign and inspect work and provide training to less experienced workers. Responsibilities include providing leadership, functional expertise, project management, coordination, support, and oversight of work efforts.

LICENSES AND CERTIFICATIONS:

Ability to obtain 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/Z35P>

POSTING DATE:

Tuesday, December 29, 2020 **(Until Filled)**

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

The SAA is an equal employment opportunity employer in accordance with the requirements of Senate Rules and regulations and applicable federal laws. It is the policy of the SAA that all employment actions will be administered without regard to an employee's or an applicant's race, color, national origin, religion, disability, genetic information, age, gender, sexual orientation or uniformed service.



CYBERSECURITY PRINCIPAL SPECIALIST

NATURE OF WORK

This is advanced professional work coordinating, developing, evaluating, and implementing cybersecurity standards and procedures to protect centralized and distributed information systems, applications, and data. Work may include leading a team of employees responsible for providing a full range of cybersecurity support to Senators, Senate Committees and other Senate offices. Work includes coordinating and re-directing work assignments to ensure timelines and customer needs are met. The incumbent assists the supervisor in coordinating and directing staff work assignments. The incumbent may assign and inspect work and provide training to less experienced workers. This work involves extensive interactions with customers, Sergeant at Arms (SAA) business units, other agencies, and vendors. Responsibilities include providing leadership, functional expertise, project management, coordination, support, and oversight of work efforts. This position is under the direction of a Supervisor 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.)

- As functional expert, the incumbent may be called upon to recommend short- and long-term strategic direction for Senate technology.
- As project manager, the incumbent may be assigned project management responsibilities to include the coordination and review of staff and contractor work efforts, budget monitoring, timetables and service level agreements.
- Work involves close cooperation with business owners to define, implement, and review effective cybersecurity requirements.
- Provides expert level functional support in the area of cybersecurity to SAA Cybersecurity Department staff and staff throughout the SAA organization.
- Administers key Cybersecurity service to Senate offices (ex: vulnerability assessments, cybersecurity defense operations, Information Assurance Audits and/or Awareness presentations).
- Assists the supervisor in coordinating all activities of the team; plans, coordinates and reviews work; provides feedback to supervisor for the purpose of evaluating subordinates.
- Provides advanced instruction to staff; trains, assigns and inspects work; schedules training.
- Serves as backup to supervisor, attending meetings and assisting in overseeing day-to-day operations; compiles weekly statistics and prepares necessary system reports and forms to assess workload.



- Leads advanced project teams and contractors; plans, assigns, directs, and coordinates work efforts; develops project plans, timetables and staff requirements.
- Serves as an authority on the interoperability, and system integration of operational security products which affect application systems, development initiatives, network efforts and computer acquisition plans of organizations within the Senate's automation architecture.
- Serves as primary or backup Contracting Officer's Representative (COR) for cybersecurity projects; helps coordinate activities of contractors, vendors, SAA customer support staff, and IT support staff; reviews vendor contracts for compliance and accuracy; assists in adjusting contract statement of work as business needs change; develops reporting mechanisms for evaluating contractor adherence to service level agreements; submits periodic reports on service level agreement compliance.
- Serves as team leader and/or project manager on assigned projects; plans, assigns, directs and coordinates work efforts; develops project plans, calculates level of effort and resource requirements, sets timetables.
- Promotes disaster recovery planning by assisting in identifying critical computer services and applications; develops and documents emergency responses and contingency plans; leads coordination role of planning and carrying out exercises.
- Works with Senate business owners to ensure appropriate logical, physical, management, and cybersecurity controls are employed in all applications; periodically reviews application controls for efficiency and effectiveness.
- Develops, reviews, maintains and recommends standards, policies, procedures, guidelines and security controls to protect Senate centralized and distributed computer operations from unauthorized access, use, disclosure and interruption of service.
- Assists in short- and long-range strategic planning activities for the Senate in the area of cybersecurity, monitors the impact of technological development; identifies, researches, and evaluates emerging IT security products; proposes solutions and countermeasures.

PHYSICAL DEMANDS AND WORKING ENVIRONMENT

Work requires extended periods of confined sitting and hand-eye coordination working with computers. Work is conducted in common office environments, secured spaces, and security operations centers. Occasional evening and weekend work may be required to resolve problems, handle incidents, participate in Continuity of Operations (COOP) exercises, or assist SAA staff in meeting critical deadlines. Expected to work unusual and perhaps unexpected hours during a (COOP) event.

MINIMUM QUALIFICATIONS

Work requires a Bachelor's Degree in computer science, telecommunications, or a related field, and eight to ten years of progressively responsible experience within a Certified Information Systems Security Professional (CISSP)-type environment or any equivalent combination of education and experience that provides the following knowledge, skills and abilities:



- Knowledge of project management principles and practices; ability to set goals and to plan, monitor and evaluate project or contract budgets; ability to organize and coordinate resources to achieve project and organizational goals and objectives efficiently and effectively.
- Skill in critical thinking to identify strengths, weaknesses, alternative solutions, conclusions and approaches to problems.
- Creates and leads interactive learning exercises that support an effective learning environment.
- Uses appropriate instructional strategies such as lectures, demonstrations, interactive exercises, multimedia presentations, video courses, and web-based courses to create an effective learning environment for the SAA cyber community.
- Designs instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to the relevant portion of the workforce.
- Skill in making processes more efficient.
- Ability to identify potential security events to the team; developing action plans, and carrying them out quickly and effectively.
- Ability to support the team Supervisor in interacting effectively with individuals at all levels of the organization, Member offices, external agencies and committees, and contractors.
- Ability to communicate effectively and possess excellent written, oral and presentation skills.
- Ability to handle sensitive information in compliance with established Senate standards and guidelines for managing sensitive data.

LICENSES, CERTIFICATION AND OTHER REQUIREMENTS

Ability to obtain a security clearance.

Cybersecurity Principal Specialist Addendum

Examples of Work:

- Translate functional requirements into technical solutions
- Build, install, configure, and test dedicated cyber defense hardware
- Check system hardware availability, functionality, integrity, and efficiency
- Identify, assess, and recommend cybersecurity or cybersecurity-enabled products for use within a system and ensure that recommended products are in compliance with organization's evaluation and validation requirements
- Identify information technology (IT) security program implications of new technologies or technology upgrades
- Conduct a market analysis to identify, assess, and recommend commercial, Government off-the-shelf, and open source products for use within a system and ensure recommended products are in compliance with organization's evaluation and validation requirement
- Analyze internal operational architecture, tools, and procedures for ways to improve performance
- Assist in identifying, prioritizing, and coordinating the protection of critical cyber defense infrastructure and key resources
- Identify potential conflicts with implementation of any cyber defense tools (e.g., tool and signature testing and optimization)
- Document and address organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle
- Employ secure configuration management processes
- Provide advice on project costs, design concepts, or design changes
- Participate in the acquisition process as necessary, following appropriate supply chain risk management practices
- Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, etc.)

Knowledge, Skills and Abilities:

- Knowledge of principles and methods for integrating system components

- Knowledge of capabilities and requirements analysis
- Knowledge of performance tuning tools and techniques
- Knowledge of the enterprise information technology (IT) architecture
- Knowledge of the type and frequency of routine hardware maintenance
- Knowledge of risk management processes (e.g., methods for assessing and mitigating risk)
- Knowledge of business continuity and disaster recovery continuity of operations plans
- Knowledge of access authentication methods
- Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation
- Ability to evaluate/ensure the trustworthiness of the supplier and/or product
- Ability to oversee the development and update of the life cycle cost estimate
- Ability to identify critical infrastructure systems with information communication technology that were designed without system security considerations

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.