



U.S. Senate Sergeant at Arms Human Resources

Vacancy Announcement

Reposting (Previous applicants need not reapply.)

POSITION:

Cybersecurity Principal Specialist #5358

DEPARTMENT:

Cybersecurity / Information Assurance / Audit

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. The incumbent leads efforts in maintaining deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions and leads efforts in maintaining knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing. This work involves making recommendations regarding the selection of cost-effective security controls to mitigate risk.

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/R5VN>

POSTING DATE:

Thursday, March 12, 2020 to **Thursday, March 26, 2020**

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:

- Lead efforts in maintaining deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions
- Lead efforts in maintaining knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing
- Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes)
- Perform an information security risk assessment
- Perform cybersecurity testing of developed applications and/or systems
- Perform technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, etc.)
- Lead efforts in preparing audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions
- Analyze computer-generated threats for counter intelligence or criminal activity
- Assess the effectiveness of security controls
- Lead efforts in conducting application vulnerability assessments
- Lead efforts in conducting required reviews as appropriate within environment (e.g., Technical Surveillance, Countermeasure Reviews [TSCM], TEMPEST countermeasure reviews)
- Determine the extent of threats and recommend courses of action or countermeasures to mitigate risks
- Develop procedures and test fail-over for system operations transfer to an alternate site based on system availability requirements
- Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, hash function checking)
- Ensure all systems security operations and maintenance activities are properly documented and updated as necessary

- Ensure the execution of disaster recovery and continuity of operations
- Examine recovered data for information of relevance to the issue at hand
- Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation

Knowledge, Skills and Abilities:

- Knowledge of organization's risk tolerance and/or risk management approach
- Knowledge of the judicial process, including the presentation of facts and evidence
- Knowledge of crisis management protocols, processes, and techniques
- Knowledge of current and emerging threats/threat vectors
- Knowledge of enterprise incident response program, roles, and responsibilities
- Knowledge of information security program management and project management principles and techniques
- Knowledge of organizational training policies
- Skill in identifying gaps in technical delivery capabilities
- Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system
- Skill in the use of penetration testing tools and techniques
- Skill in the use of social engineering techniques. (e.g., phishing, baiting, tailgating, etc.)
- Skill in using network analysis tools to identify vulnerabilities. (e.g., fuzzing, nmap, etc.)
- Skill to develop insights about the context of an organization's threat environment
- Skill to translate, track, and prioritize information needs and intelligence collection requirements across the extended enterprise
- Ability to assist in designing valid and reliable assessments

- Ability to assist in monitoring advancements in information privacy technologies to ensure organizational adaptation and compliance
- Ability to assist in monitoring and assessing the potential impact of emerging technologies on laws, regulations, and/or policies

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.