U.S. Senate Sergeant at Arms
Human Resources

Vacancy Announcement

POSITION:	**Cybersecurity Technical Director #5382**
DEPARTMENT:	Cybersecurity / Cybersecurity Operations Branch
SUMMARY:	This is advanced professional work providing technical expertise to a team in the Cybersecurity Department. Work includes providing subject matter expert review of team processes/procedures to ensure optimal efficiency and effectiveness; recommending and optimizing architecture of applicable team technologies and/or tools to achieve maximum effectiveness and efficiency in accomplishing team goals and objectives. Work is performed under the direction of the team Supervisor.
LICENSES AND CERTIFICATIONS:	Ability to obtain a security clearance.
SALARY RANGE:	$104,761 - $157,136
HOW TO APPLY:	All applicants must use the link below and follow instructions. https://sen.gov/O2NW
POSTING DATE:	Wednesday, October 21, 2020 **(Until Filled)**

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

CYBERSECURITY TECHNICAL DIRECTOR

NATURE OF WORK

This is advanced professional work providing technical expertise to the assigned team supervisor in the Cybersecurity Department. Work includes providing subject matter expert review of team processes/procedures to ensure optimal efficiency and effectiveness; recommending and optimizing architecture of applicable team technologies and/or tools to achieve maximum effectiveness and efficiency in accomplishing team goals and objectives. Work is performed under the direction of the team Supervisor. This position supports technical and/or functional oversight and coordination of the cybersecurity program for the respective branch.

EXAMPLES OF WORK

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

- Serves as an internal consultant and advisor in own area of expertise (e.g., technology, tools, standards, best practices, processes, etc.).
- Supports assigned supervisor on overall enterprise information security architecture with the organization's overall security strategy.
- Advises supervisor on risk levels and security posture.
- Interprets and advises the assigned supervisor on appropriate application of laws, regulations, policies, standards, or procedures to specific issues.
- Interprets patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the team's cybersecurity mission and objectives.
- Provides support to the assigned supervisor in the development of cyber operations specific indicators measuring success and attainment of team goals and objectives.
- Provides support to the team for planning/developmental forums and working groups as appropriate.
- Develops short-term and strategic training events for the assigned team in conjunction with Supervisor's/Branch Manager's approval.

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 event.

MINIMUM QUALIFICATIONS

Work requires a Bachelor's Degree in computer science, telecommunications, or a related technical field, and Eight to ten years of experience within a Certified Information Systems Security Professional (CISSP)-type

environment or any equivalent combination of education and experience that provides the following knowledge, abilities and skills:

- Knowledge of laws, regulations, policies, and ethics as they relate to the cybersecurity area of expertise.
- Knowledge of cyber threats and vulnerabilities as they relate to the cybersecurity area of expertise.
- Knowledge of specific operational impacts of cybersecurity lapses as they relate to the cybersecurity area of expertise.
- Knowledge of operations testing and evaluation methods as they relate to the cybersecurity area of expertise.
- Skill in integrating the team's goals and objectives into the team's technical and/or functional architecture.
- Skill in making processes more efficient.
- Skill in written, oral and presentation skills, especially in conducting cross-training events for other cybersecurity teams.
- Ability to apply an organization's goals and objectives to develop and maintain the team's operations architecture.
- Ability to optimize systems and/or tools to meet enterprise performance requirements.
- Ability to execute technology and/or tool automation processes.
- Ability to work well with a diverse staff base.
- Ability to work in heavily regulated and/or audited environment.

LICENSES, CERTIFICATION AND OTHER REQUIREMENTS

Ability to obtain a security clearance.

Cybersecurity Technical Director Addendum

Examples of Work:

· Evaluate Operations Team process, procedures and tools for improving effectiveness and efficiency in detect, react and recover mission.

· Establish standards and procedures to track Operations Team Detect , React and Recovery Mission

· Devise and establish policies and systems to support the implementation of cyber defense strategies set by Cybersecurity Department Leadership

· Assist in identifying, prioritizing, and coordinating the protection of critical cyber defense infrastructure and key resources

· Analyze Operations mission requirements against technical solutions to identify gaps within the Cybersecurity Departments defense-in-depth capabilities

· Identify potential conflicts with implementation of any cyber defense tools (e.g., tool and signature testing and optimization)

· 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

· Develop reliable metrics for Operations Branch requirement for logging of data within its security information and event management (SIEM) tool

· Work with Operations Branch Manager to oversee the completion of Proof of Concepts/Product Evaluations of products to ensure all technical requirements are met

· Document and address organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle

· Oversee Cybersecurity Content Review Program for continuous monitoring support for the Cyber Security Operations Center

· Ensure acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines

· Provide technical support for production and development systems

· Provide input on security requirements to be included in statements of work and other appropriate procurement documents

· Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment.

· Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements

· Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents

· Determine the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately

Knowledge, Skills and Abilities:

· Knowledge of computer networking concepts and protocols, and network security methodologies

· Knowledge of risk management processes (e.g., methods for assessing and mitigating risk)

· Knowledge of capabilities and applications of network equipment including routers, switches, bridges, servers, transmission media, and related hardware

· Knowledge of capabilities and requirements analysis

· Knowledge of business continuity and disaster recovery continuity of operations plans

· Knowledge of information security systems engineering principles (NIST SP 800-160)

· Knowledge of access authentication methods

· Knowledge of encryption algorithms

· Knowledge of auditing and logging procedures (including server-based logging)

· Skill in analyzing network traffic capacity and performance characteristics

· Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation

· Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate)

· Ability to apply network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth)

· Ability to apply secure system design tools, methods and techniques

· Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation)

· Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute)

· 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.