U.S. Senate Sergeant at Arms
Human Resources

Vacancy Announcement

When applying for this position, refer to "POSITION #5358" on your application package.

POSITION:	Cybersecurity Senior Specialist (#5358)
DEPARTMENT:	Cybersecurity / Information Assurance Branch / Audit
REQUIREMENTS:	See attached Position Description
SALARY RANGE:	$84,840 - $127,252
CONTACT:	U.S. Senate Sergeant at Arms, Human Resources Senate Hart Building SH-142 Washington, DC 20510 Phone: (202) 224-2889 Fax: (202) 228-2965 Email: resumes@saa.senate.gov
POSTING DATE:	Tuesday, September 11, 2018
DEADLINE FOR APPLICATIONS:	Tuesday, September 25, 2018

All applicants must submit a U.S. Senate Sergeant at Arms Application for Employment with a cover letter and current resume to the Human Resources Department.

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.

CYBERSECURITY SENIOR SPECIALIST

NATURE OF WORK

This is professional work coordinating, implementing and maintaining technologies and processes to protect the confidentiality, integrity, and availability of Senate information systems. Work includes promoting system cybersecurity to safeguard information systems from unauthorized access, use, disclosure, or tampering. Incumbent utilizes all the security tools available to prevent system compromise and detect, react and respond to indicators of intrusion activity in the Senate's data/voice networks. Work also involves working closely with other Sergeant at Arms (SAA) departments and the Senate user community to define security requirements, cybersecurity plans to address disaster recovery, recommend mitigation strategies, and encourage adoption of best practices. Work is performed under the direction of a Cybersecurity Supervisor and is peer-reviewed for accuracy and effectiveness.

EXAMPLES OF WORK

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

- Responds to potential localized or widespread security events; uses various reports to help track and isolate user access problems and potential security incidents; creates daily situational reports while manning and supporting the Cyber Security Operations Center.
- Coordinates and performs automated vulnerability assessments; advises Senate office staff on effective remediation techniques.
- Coordinates and performs the critical security patch evaluation and certification process for supported Microsoft and non-Microsoft software.
- Promotes cybersecurity awareness and assists with developing security awareness materials; provides security reviews for Senate Office Cybersecurity operational environments; and assists in providing security training and awareness briefings.
- Assesses the impact of new cybersecurity threats and identifies and evaluates vulnerabilities within new technology and changes to Senate IT infrastructure.
- Researches, evaluates, tests, and recommends cybersecurity solutions and controls.
- Develops, implements, and maintains scripts and other automated tools to identify indicators of intrusion activity and to support effective cybersecurity workflow processes.

- Performs cybersecurity systems administration tasks and services for Senate employees and vendor maintenance access.

- Updates management as required on Cybersecurity related issues.

PHYSICAL DEMANDS AND WORKING ENVIRONMENT

Work is essentially sedentary with occasional walking, standing, and bending; occasional lifting and carrying desktop computers, computer components, and/or packages of software media. Work is conducted in common office environments 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 three to five 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:

- Understanding of computer operating systems, applications, and networking; understanding of key principles of information protection; knowledge of data security and access control systems, encryption, firewalls, network- and host-based security technologies and processes.

- Working knowledge of TCP/IP communications protocols and standards.

- Ability to identify potential security breaches and implement action plans in conjunction with diverse groups of stakeholders.

- Ability to interface with individuals at all levels of the organization in a dynamic, fast-paced environment.

- Ability to communicate functional issues and solutions effectively, both orally and in writing, to individuals possessing a broad range of functional knowledge, skills, and abilities.

- Ability to re-focus work activities rapidly in response to changing requirements and priorities.

- Ability to handle sensitive information.

- Proficiency with office productivity tools including, but not limited to, spreadsheets, word processors, databases, and presentation software.

- Proficiency with one or more scripting language and/or integrated development environments.

LICENSES, CERTIFICATION AND OTHER REQUIREMENTS

Ability to obtain and maintain a security clearance.

Cybersecurity Senior Specialist Addendum

Cybersecurity Information Assurance Branch - Audit

Examples of Work:

- Update deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions
- Update knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing
- Support implementing recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes)
- Contribute to information security risk assessment
- Contribute to testing of cybersecurity developed applications and/or systems
- Contribute to 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.)
- Senior contributor to audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions
- Contribute to analysis of computer-generated threats for counter intelligence or criminal activity
- Contribute to analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion or other crimes
- Support team Lead as required in conducting required reviews as appropriate within environment (e.g., Technical Surveillance, Countermeasure Reviews [TSCM], TEMPEST countermeasure reviews)
- Contribute to development of procedures and test fail-over for system operations transfer to an alternate site based on system availability requirements
- Contribute to documentation of original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, hash function checking)
- Provide technical leadership employing information technology (IT) systems and digital storage media to solve, investigate, and/or prosecute cybercrimes and fraud committed against people and property
- Support systems security operations and maintenance activities are properly documented and updated as necessary
- Contribute to integration and implementation of Cross-Domain Solutions (CDS) in a secure environment
- Examine recovered data for information of relevance to the issue at hand
- Senior contributor to identification and/or determination of whether a security incident is indicative of a violation of law that requires specific legal action
- Senior contributor identifying digital evidence for examination and analysis in such a way as to avoid unintentional alteration.
- Senior contributor implementing system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation

Knowledge, Skills and Abilities:

- Ability to support the design of valid and reliable assessments
- Strong knowledge of organization's risk tolerance and/or risk management approach
- Skill in contributing to application vulnerability assessments
- 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
- Strong skill in reviewing logs to identify evidence of past intrusions
- Knowledge of penetration testing tools and techniques
- Knowledge of 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
- Knowledge of advancements in information privacy technologies to ensure organizational adaptation and compliance
- Knowledge of crisis management protocols, processes, and techniques
- 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
- Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation)
- Knowledge of network traffic analysis methods.
- Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL])
- Knowledge of packet-level analysis

- Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- Knowledge of basic system, network, and OS hardening techniques.
- Knowledge of test procedures, principles, and methodologies (e.g., Capabilities and Maturity Model Integration (CMMI)).
- Knowledge of transmission records (e.g., Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wireless Fidelity (Wi-Fi). paging, Voice over Internet Protocol (VoIP)), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly.
- Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.
- Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
- Knowledge of network traffic analysis (tools, methodologies, processes).

Certification:

Demonstrated by providing artifacts such as: a diploma/degree, cybersecurity certifications, or other relevant items demonstrating the participation of other cybersecurity activities like Cyber Patriot or other similar programs.