U.S. Senate Sergeant at Arms

Human Resources

# Vacancy Announcement

***When applying for this position, refer to “POSITION # 5364” on your application package.***

| | |
|---|---|
| **POSITION:** | Cybersecurity Specialist - Hunt (#5364) |
| **LOCATION/HOURS:** | Swing Shift (2:00 p.m. - 11:00 p.m.) |
| **DEPARTMENT:** | Cybersecurity / Cybersecurity Operations Branch / Hunt Operations Center |
| **REQUIREMENTS:** | See attached Position Description |
| **SALARY RANGE:** | $85,856 - $124,877 (Includes Night Shift Differential) |
| **CONTACT:** | U.S. Senate Sergeant at Arms, Human Resources<br>Senate Hart Building SH-142<br>Washington, DC 20510<br>Phone: (202) 224-2889<br>Fax: (202) 228-2965<br>Email: resumes@saa.senate.gov |
| **POSTING DATE:** | Thursday, September 20, 2018 |
| **DEADLINE FOR APPLICATIONS:** | Thursday, October 04, 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.

**OFFICE OF THE SERGEANT AT ARMS AND DOORKEEPER**
**UNITED STATES SENATE**

# CYBERSECURITY SPECIALIST

## NATURE OF WORK

This is professional work supporting the mission of a specific cybersecurity team to protect centralized and distributed information systems, applications, and data. The incumbent will have responsibility for competently contributing to the proper implementation of the team's adopted standards and practices. This position is responsible for supporting the execution and coordination of mission essential services. Work is performed under the general supervision of a Supervisor.

## EXAMPLES OF WORK

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

- Provides functional and/or technical skills for the assigned cybersecurity unit.

- Supports the unit's work effort as required in preparing materials for collaborating with other sections, divisions, departments, and vendors to gather and disseminate information.

- Contributes to the unit's work effort as required in preparing analysis and materials for providing expert level support in the assigned area of cybersecurity to SAA IT security branch staff, other SAA technical staff, SAA procurement staff, and other division or departments; and for identifying and resolving critical and complex issues in the assigned unit.

- Supports the unit's work effort as directed in providing leadership to the unit's project teams and contractors. Work includes helping to develop plans, assignments, and coordination of work efforts.

- Supports the unit's work effort to develop governing policies, standards and procedures.

## 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.

## MINIMUM QUALIFICATIONS

Work requires an Associate's Degree, or greater, in computer science, telecommunications, or a related technical field, and one to two years of experience within a CISSP-type environment or any equivalent combination of education and experience that provides the following knowledge, skills and abilities:

- Knowledge with a variety of concepts, practices and procedures used by the assigned cybersecurity unit.

- Knowledge of current technologies and/or tools in use by the assigned unit.

*The statements contained herein reflect general details necessary to describe the principal functions of this class, knowledge and skill typically required and the physical demands and working conditions, but should not be considered an all-inclusive listing of work requirements.*

- Skill in critical thinking to identify strengths, weaknesses, alternative solutions, conclusions and approaches to unit problems.
- Skill in making processes more efficient.
- Ability to logically analyze systems and/or processes in use by the assigned unit.
- Ability to support unit work effort in setting team goals, plans, and monitoring projects.
- General command of applicable standards and processes.
- Ability in oral communication skills.

## LICENSES, CERTIFICATION AND OTHER REQUIREMENTS

Ability to obtain a security clearance.

*The statements contained herein reflect general details necessary to describe the principal functions of this class, knowledge and skill typically required and the physical demands and working conditions, but should not be considered an all-inclusive listing of work requirements.*

# Cybersecurity Specialist Addendum

Cybersecurity Operations Branch - Hunt Operations Center – Swing Shift (2:00 p.m. - 11:00 p.m.)

**Examples of Work:**

- Contribute technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents
- Assist with implementation of updating defense tools' rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists, etc.) for specialized cyber defense applications
- Analyze log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security
- Assist with the triage cyber defense incidents, including determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation
- Assist with trend analysis and reporting to ensure quality of cyber defense.
- Assist with modifications or adjustments to technical platform, processes, environment, etc., based on cybersecurity capability assessments (Blue Team, Read Team, audits, etc.)
- Assist with development of cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies
- Assist with collection of intrusion artifacts (e.g., source code, malware, Trojans) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise

**Knowledge, Skills and Abilities:**

- Knowledge of cybersecurity and privacy principles
- Knowledge of cyber threats and vulnerabilities
- Knowledge of authentication, authorization, and access control methods
- Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins)
- Knowledge of incident categories, incident responses, and timelines for responses
- Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions
- Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities
- Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations
- Knowledge of adversarial tactics, techniques, and procedures
- Knowledge of collection management processes, capabilities, and limitations
- Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks)
- Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures
- Knowledge of cyber-attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks)
- Knowledge of encryption methodologies
- Knowledge of signature implementation impact for viruses, malware, and attacks
- Knowledge of cloud service models and how those models can limit incident response
- Knowledge of malware analysis concepts and methodologies
- Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump)
- Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications
- Knowledge of penetration testing principles, tools, and techniques
- Knowledge of intrusion detection and prevention system tools and applications
- Knowledge of common adversary capabilities, tactics, techniques, and procedures in assigned area of responsibility
- Knowledge of general attack stages
- Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes
- Skill in preserving evidence integrity according to standard operating procedures or national standards
- Skill in using incident handling methodologies
- Skill in conducting investigations and developing comprehensive reports
- Skill in collecting data from a variety of cyber defense resources
- Skill in securing network communications
- Skill in recognizing and categorizing types of vulnerabilities and associated attacks
- Skill in protecting a network against malware. (e.g., NIPS, anti-malware, restrict/prevent external devices, spam filters)
- Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation)
- Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies
- Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute