U.S. Senate Sergeant at Arms
Human Resources

# Vacancy Announcement

| | |
|---|---|
| **POSITION:** | **Cybersecurity Specialist - (#5287)** |
| **DEPARTMENT:** | Cybersecurity / Cyber Operations Branch / Threat Intelligence Analyst |
| **SUMMARY:** | 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. |
| **SALARY RANGE:** | $79,823 - $119,730 |
| **HOW TO APPLY:** | All applicants must use the link below and follow instructions. https://sen.gov/MO54 |
| **POSTING DATE:** | Friday, May 10, 2019 **to Friday, May 31, 2019** |

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

# 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.

- 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.

# Cybersecurity Specialist Addendum

Cybersecurity Specialist Addendum

Cybersecurity Operations Branch – Threat Intelligence Analyst

Examples of Work:

Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion or other crimes.

Develop a trend analysis and impact report.

Examine recovered data for information of relevance to the issue at hand.

Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information.

Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.

Identify and analyze anomalies in network traffic using metadata (e.g., CENTAUR).

Determine the extent of threats and recommend courses of action or countermeasures to mitigate risks.

Employ information technology (IT) systems and digital storage media to solve, investigate, and/or prosecute cybercrimes and fraud committed against people and property.

Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings).

Reconstruct a malicious attack or activity based off network traffic.

Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration.

Read, interpret, write, modify, and execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems (e.g., those that perform tasks such as: parsing large data files, automating manual tasks, and fetching/ processing remote data).

Implement data mining and data warehousing applications.

Manage the compilation, cataloging, caching, distribution, and retrieval of data.

Assist in the construction of signatures which can be implemented on cyber defense network tools in response to new or observed threats within the network environment or enclave.

Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cyber incidents and articulate the event's history, status, and potential impact for further action in accordance with the organization's cybersecurity policies and procedures

Identify data or intelligence of evidentiary value to support counterintelligence and criminal investigations.

Fuse computer network attack analyses with criminal and counterintelligence investigations and operations.

Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions.

Knowledge, Skills and Abilities:

Knowledge of the factors of threat that could impact collection operations.

Knowledge of data mining techniques.

Knowledge of collection management tools.

Knowledge of database access application programming interfaces (e.g., Java Database Connectivity [JDBC]).

Knowledge of available databases and tools necessary to assess appropriate collection tasking.

Knowledge of database management systems, query languages, table relationships, and views.

Knowledge of the characteristics of physical and virtual data storage media.

Skill in conducting queries and developing algorithms to analyze data structures.

Knowledge of data classification standards and methodologies based on sensitivity and other risk factors.

Knowledge of taxonomy and semantic ontology theory.

Skill in reviewing logs to identify evidence of past intrusions.

Skill in mimicking threat behaviors.

Skill in collecting data from a variety of cyber defense resources.

Skill in performing impact/risk assessments.

Ability to evaluate, analyze, and synthesize large quantities of data (which may be fragmented and contradictory) into high quality, fused targeting/ intelligence products.

Ability to evaluate information for reliability, validity, and relevance.

Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.

Ability to coordinate and collaborate with analysts regarding surveillance requirements and essential information development.

Ability to maintain databases. (i.e., backup, restore, delete data, transaction log files, etc.).

# 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.