U.S. Senate Sergeant at Arms
Human Resources

Vacancy Announcement

POSITION:	**Cybersecurity Senior Specialist - Hunt (#139)**
DEPARTMENT:	Cybersecurity / Cyber Operations Branch, Hunt Operations Center / Hunt Analyst
SUMMARY:	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.
SALARY RANGE:	$86,766 - $130,141
HOW TO APPLY:	All applicants must use the link below and follow instructions. https://sen.gov/OJ5W
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 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 Senior Specialist Addendum

Cybersecurity Operations Branch, Hunt Operations Center – Hunt Analyst-Day Shift

Examples of Work:

Contribute senior technical skills for analyzing log files, evidence, and other information to determine. best methods for identifying the perpetrator(s) of a network intrusion or other crimes

Assist with monitoring files and registries on the running system after identifying intrusion via dynamic analysis

Provide assistance in examining intercept-related metadata and content with an understanding of targeting significance

Serve as technical resource for compiling, integrating, and/or interpreting all-source data for intelligence or vulnerability value with respect to specific targets

Provide technical support for collaborating across internal and/or external organizational lines to enhance collection, analysis and dissemination

Assist in evaluating and interpreting metadata to look for patterns, anomalies, or events, thereby optimizing targeting, analysis and processing

Contribute technical leadership for identifying data or intelligence of evidentiary value to support counterintelligence and criminal investigations

Assist a technical team in operating specialized hardware/software and implementing industry best practices for cataloging, documenting, extracting, collecting, packaging and preserving digital evidence

Knowledge, Skills and Abilities:

Knowledge of encryption algorithms and cyber capabilities/tools (e.g., SSL, PGP)

Knowledge of obfuscation techniques (e.g., TOR/Onion/anonymizers, VPN/ VPS, encryption).

Knowledge of collateral damage and estimating impact(s)

Knowledge of file type abuse by adversaries for anomalous behavior

Knowledge of network traffic analysis (tools, methodologies, processes)

Skill in using multiple analytic tools, databases, and techniques (e.g., Analyst’s Notebook, A-Space, Anchory, M3, divergent/convergent thinking, link charts, matrices, etc.)

Skill in creating and extracting important information from packet captures

Skill in interpreting metadata and content as applied by collection systems

Skill in recognizing and interpreting malicious network activity in traffic

Skill in reading and interpreting signatures (e.g., snort)

Skill in reviewing logs to identify evidence of past intrusions

Ability to contribute senior technical leadership in evaluating, analyzing and synthesizing large quantities of data (which may be fragmented and contradictory) into high quality, fused targeting/intelligence products

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

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.