U.S. Senate Sergeant at Arms
Human Resources

Vacancy Announcement

POSITION:	**Chief Privacy Officer #5359**
DEPARTMENT:	Executive Office - Office of General Counsel
SUMMARY:	The Chief Privacy Officer will establish and maintain the SAA vision, strategy, and program to ensure information assets and technologies are adequately safeguarded in order to protect the privacy of the Senators and their staff. The Chief Privacy Officer will develop privacy policies for internal use cases and privacy statements for external use cases. The incumbent will identify, develop, implement, maintain, assess and test processes across the enterprise to reduce information risks. The Chief Privacy Officer will coordinate a response to incidents, establish appropriate standards and controls, manage security technologies, and direct the establishment and implementation of policies and procedures. In addition, the Chief Privacy Officer represents the SAA with internal and external stakeholders.
LICENSES AND CERTIFICATIONS:	Position requires the ability to obtain a top-secret security clearance.
SALARY RANGE:	$143,387 - $173,900
HOW TO APPLY:	All applicants must use the link below and follow instructions. https://sen.gov/25LL
POSTING DATE:	Friday, July 30, 2021 **to Friday, August 20, 2021**

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

CHIEF PRIVACY OFFICER

NATURE OF WORK

Working as part of the Office of General Counsel, the Chief Privacy Officer will establish and maintain the SAA vision, strategy, and program to ensure information assets and technologies are adequately safeguarded in order to protect the privacy of the Senators and their staff. The Chief Privacy Officer will develop privacy policies for internal use cases, and privacy statements for external use cases, and describe privacy requirements for business partners and service providers. The Chief Privacy Officer will closely collaborate with business stakeholders to control risk from potential procedural or technology changes that affect privacy. In addition, the Chief Privacy Officer represents the SAA with internal and external stakeholders.

The Chief Privacy Officer conducts privacy risk assessments, focused on end-to-end business processes or applications. The Chief Privacy Officer will identify, develop, implement, maintain, assess and test processes across the enterprise to reduce information risks. The Chief Privacy Officer will coordinate a response to incidents, establish appropriate standards and controls, manage security technologies, and direct the establishment and implementation of policies and procedures through analysis of end-to-end business process mapping.

This position will identify key controls (to include major IT programs, macro programs, and non-IT related information) and identify strengths and material weaknesses. In coordination with the business process owners, the Chief Privacy Officer will exploit opportunities and weigh risks. The Chief Privacy Officer will coordinate the development of corrective action plans for risks deemed unacceptable and track them until mitigated. He or she will identify and suggest priorities for the organization, as well as determine how to maintain and improve adherence to Senate policies.

EXAMPLES OF WORK

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

- Working across the divisions of the SAA, maintains, develops and implements SAA's privacy management program and the resulting privacy policies, procedures and documentation for the processing of personal data in coordination with SAA leadership.
- Devises and updates policies and procedures for customers, employees and data breach incident responses, ensuring alignment with the actual implementation of personal data processing activities.
- Works to ensure the organization maintains the appropriate privacy and confidentiality consent procedures, authorization forms, and information notices.
- Works with procurement, vendor management and the legal departments to ensure that contracts and operating-level agreements meet the Senate's privacy requirements.
- In coordination with the SAA Internal Controls Program, implements and maintains an internal reporting mechanism for intended (new or changed) personal data processing activities, to which

business unit/process owners must adhere.

- Determines the SAA's specific privacy-related requirements and potential vulnerabilities.
- Receives and manages internal reports from business stakeholders to maintain control over all project and innovation initiatives, including change management, to ensure timely attention for privacy bottlenecks and hiatuses.
- Manages the privacy risk assessment process in close collaboration with business stakeholders.
- Conducts regular privacy policy compliance assessments to ensure that SAA's privacy policies are being adhered to.
- Ensures that business units, technology teams and third parties (service providers) follow SAA's privacy management program, meet privacy policy requirements and address privacy concerns.
- Coordinates with business process owners to ensure they establish adequate segregation of duties, rigorous change management procedures, access procedures, incident and problem management procedures, and configuration, installation & testing procedures.
- Collaborates with and assists business units and technology areas to develop corrective action plans for identified privacy compliance issues.
- Continuously monitors the status and effectiveness of privacy controls across service offerings, ensuring that privacy-related key risk indicators are effectively monitored to prevent an unacceptable impact on business objectives and reputation.
- Conducts frequent compliance report monitoring activities on collaborating partners, third-party service providers' and other data processors' levels of privacy compliance.
- Develops a testing methodology and report findings in a structural, transparent and business-relevant manner in coordination with SAA leadership, to the SAA to recommend, decide and instruct on adequate and appropriate mitigating measures.
- Supports the creation of an inventory that documents how and why SAA collects, shares and uses personal data.
- Continuously updates and re-evaluates the extent to which customer, constituent and employee information is collected and shared internally and externally.
- Monitors the data request and usage processes, purpose-based authorized use and prevention mechanisms' effectiveness against unauthorized use and cross-border data transfer matters for personal data across SAA.
- Works with business owners to help them maintain registries of all personal data stores and processing activities.

- Serves as the internal advisor to the CIO to interpret privacy/policy-related questions.
- Ensures that data security practices, in particular, logging, monitoring and auditing practices, do not conflict with privacy requirements.
- Works closely with the CIO to anticipate potential privacy problems embedded in the use of emerging technologies.
- Liaises with SAA's CIO and Director of Cybersecurity in matters relating to data breaches (including preparedness, prevention, impact mitigation and integral management of breaches).
- Identifies trends in privacy requirements and compliance enforcement, and accounts for the necessary changes in the privacy management program, updating information only to the stakeholder audiences affected in their respective activities.
- Develops new and innovative strategies to address privacy requirements in new computing paradigms, such as hybrid cloud computing, social media analytics, and surveillance technologies.

PHYSICAL DEMANDS AND WORKING ENVIRONMENT

Work is primarily in an office environment with no exceptional physical demands.

MINIMUM QUALIFICATIONS

The ideal candidate will have a combination of a legal or business degree with a technical or computer science degree. Work requires a Bachelor's Degree or higher in business administration, law, finance, accounting, computer science or a related discipline and at least 7 years of senior or executive management experience; or any equivalent combination of education and experience that provides the following knowledge, skills, and abilities:

- Familiarity and experience with cloud computing, online services, web and enterprise applications, and data analytics.
- Ability to understand business process flows and to provide recommendations for operationalizing compliance requirements.
- Strong analytical and problem resolution skills. Sound business judgment, with the ability to think strategically and give practical advice by balancing business needs with legal risks.
- Strong written and verbal communication skills, as well as the ability to work well with a diverse client base.
- Willingness to be available for incident and emergency handling outside standard office hours, where necessary.

- Knowledge of the privacy aspects of the product development life cycle, data handling and asset classification, and knowledge of the role of a privacy professional in ensuring that customer data is properly managed.

- Ability to articulate the importance of customer privacy. Comfort with promoting privacy up and down the management chain, including audiences who have varying levels of familiarity with the topic.

- Ability to maintain proper documentation, relevant records and archives in an orderly, transparent fashion.

LICENSES, CERTIFICATION AND OTHER REQUIREMENTS

- Position requires the ability to obtain a top-secret security clearance.

- An advanced degree in law (JD), business (MBA), information science (MIS), information security or a related field is preferred.

- The preferred candidate has obtained two or more of the following certifications: one or more of: Certified Information Privacy Professional (CIPP), Certified Information Privacy Management (CIPM), and/or Certified Information Privacy Technologist (CIPT), and one or more of: Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Certified Information Systems Auditor (CISA).

U.S. Senate Sergeant at Arms
Human Resources

INFORMATION FOR PROSPECTIVE SERGEANT AT ARMS (SAA) EMPLOYEES

The United States Senate Sergeant at Arms (SAA) is the largest in size of staff and budget in the Senate. It is responsible for all Senate computers and technology support services, recording and photographic services, printing and graphics services, and telecommunications services. The SAA also provides assistance to all Senate offices with their staffing, mailing, purchasing, and financial needs. The offices of the SAA that are responsible for providing these and other services include Capitol Facilities, the Operations Division, Financial Operations, and Human Resources. The SAA also shares responsibility for the Senate Page Program, the Senate Office of Training and Development, and the Capitol Telephone Exchange.

This summary of Employment Policies and Benefits is not comprehensive; it highlights major benefits that may be of interest to prospective employees. Policies and benefits are subject to change at the discretion of the Sergeant at Arms.

EMPLOYMENT POLICIES

All jobs at the Senate jobs are considered “excepted service” and are accordingly not part of the federal government’s "competitive service” process. SAA employees are considered at-will employees under the jurisdiction of the U.S. Senate Sergeant at Arms. Prospective employees will be fingerprinted and undergo a criminal background investigation. All employment offers are contingent upon successful completion of the background check.

Evaluations: Employees enter service under a six-month probationary period. After six-months of employment, a performance appraisal is conducted to determine if the employee meets job requirements, or to remain in the employment of the SAA. On the first anniversary of completing probation, and annually thereafter on that anniversary date, performance appraisals are conducted.

Pay: Salary reviews occur at the same time as performance appraisals. Merit increases are not automatic; they are based on meritorious performance and subject to approval by management of the department and the SAA. If approved by the Senate, SAA employees may also receive cost-of-living adjustments (COLAs). Senate pay days are the 5th and 20th of each month. If these days fall on a weekend or holiday, the last working day before the 5th and the 20th becomes the pay day.

HEALTH/WELLNESS BENEFITS

The Sergeant at Arms offers the full range of Federal benefits to employees:
- Federal Employees Health Benefits (FEHB)
- Federal Employees Dental and Vision Program (FEDVIP)
- Flexible Spending Accounts (FSA)
- Federal Long-Term Care Insurance (FLTCIP)
- Federal Employees Group Life Insurance (FEGLI)

RETIREMENT PLANS

Most new employees are automatically covered under the Federal Employees Retirement System - Further Revised Annuity Employees (FERSFRAE). Employees with prior Federal service may be eligible to continue to participate in the Civil Service Retirement System (CSRS), Federal Employees Retirement System (FERS) or the Federal Employees Retirement System – Revised Annuity Employees (FERS-RAE). For information on the TSP, visit www.tsp.gov.

HOLIDAY & LEAVE ACCRUALS

We offer paid time off benefits including: Annual, Sick, Long-Term Medical leave, and ten holidays. Annual and Sick leave are accrued on the 15th and last day of the month. Annual leave is accrued at rates dependent upon length of Federal Service.

Holidays: New Year's Day, Martin Luther King, Jr. Day, Presidents Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veterans Day, Thanksgiving Day, and Christmas Day.

Full -Time Employee **Annual** Leave Accrual Rates:

- Less than 3 years of federal service – 120 hours/year, 5 hours/pay day
- 3 - 15 years of federal service – 160 hours/year, 6.67 hours/pay day
- 15+ years of federal service – 200 hours/year, 8.33 hours/pay day

Year-end balances of no more than 240 hours carry over for future use

Full -Time Employee **Sick** Leave Accrual Rate:

- Sick leave can be used for either personal or immediate family medical needs
- 96 hours/year, 4 hours/pay period

Year-end balances carry over for future use

OTHER BENEFITS

Transportation Subsidy: The SAA offers a Transit subsidy of up to $270.00 for employees who use mass transit, including Metro, Commuter Buses, VRE, MARC trains and Van Pools.

Parking: Parking is provided without cost to regular SAA employees who do not participate in the transit subsidy program.

Student Loan Repayment Program: The SAA offers Student Loan Repayment for employees of up to $833.00 a month for Qualifying Federal Student Loans.

Training & Development: The SAA offers training and development to advance professional skills including live classes, online learning and leadership coaching.

The SAA is an equal opportunity employer in accordance with the requirements of Senate rules, regulations, and applicable Federal Laws.