DISTRICT OF COLUMBIA RETIREMENT BOARD
Position Vacancy Announcement

ANNOUNCEMENT NO: 20200103	POSITION: Information Systems Security Officer
OPENING DATE: January 3, 2020	CLOSING DATE: Open Until Filled
TOUR OF DUTY: 9:00 a.m. – 5:30 p.m., Monday – Friday	STARTING RANGE: $84,748 - $105,936 DOQ (Grade 09) (Career Service) Entire Range: $84,748 - $137,562
LOCATION: 900 7th Street, NW, 2nd Floor Washington, DC 20001	AREA OF CONSIDERATION: Open to all applicants
NUMBER OF VACANCIES: One (1)	TYPE OF APPOINTMENT: Probationary to Regular
This position is NOT in a collective bargaining unit.	

*** *Successful pre-employment criminal, financial, educational and certification background check required* ***

ABOUT THE D.C. RETIREMENT BOARD: The District of Columbia Retirement Board (DCRB) is an independent agency of the District of Columbia Government. Our mission is to manage and control the assets of the D.C. Police Officers' and Firefighters' Retirement Fund and the D.C. Teachers' Retirement Fund as well as to administer benefits for the members of the of the D.C. Police Officers' and Firefighters' Retirement Plan and the D.C. Teachers' Retirement Plan.

POSITION SUMMARY

Under the direction of the Information Technology Director, the Information Systems Security Officer (ISSO) ensures the secure operation of the agency's information systems and services including servers, network connections, storage devices, appliances, PCs, mobile devices, applications, databases, and data transfer devices and technologies, The ISSO will design the agency's data loss protection (DLP) policies and procedures, check server and firewall logs, scrutinize network traffic, establish and update virus scans, and troubleshoot.

ESSENTIAL DUTIES AND RESPONSIBILITIES

Information Security (InfoSec) Operations—

Has the knowledge of the technical solutions to create value, and in alignment with agency standards and industry best practices. Even in the most difficult situations, ensures that Information Assurance and Compliance tools and processes occur based on the needs of the project or the task in consideration.

- Develops, implements, maintains, and oversees enforcement of policies, procedures and associated plans for system security administration and user system access based on industry-standard best practices.
- Leads and has the ability to perform vulnerability scans of applications, servers, and databases.
- Provides analysis and reports to senior management on the status of software security assurance-related weaknesses.
- Directs risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.
- Participates in the processes to obtain ISO 20000 certification for the agency, meet FIPS-140- 2, FIPS-199, NIST800-53, and moderate secure environment compliance.

- Designs, implements, and maintains cyber security strategies for the agency to minimize the risks of security breaches.
- Participates in the design and implementation of disaster recovery plans and strategies for the agency with a goal of fault tolerance and disaster avoidance, to include telephone and telecommunications services, operating systems, databases, networks, servers, and software applications.
- Conducts research on emerging products, services, protocols, and standards in support of security enhancement and development efforts. Recommends, schedules, and performs security improvements, upgrades, and/or purchases.
- Deploys, manages and maintains all security systems and their corresponding or associated software, including firewalls, intrusion prevention and detection systems, cryptography systems, and anti-virus software. Manages connection security for local area networks, agency websites both internal and external, and e-mail communications. Manages and ensures the security of databases and data transferred both internally and externally, and data maintained on agency devices.
- Designs, performs, and/or oversees penetration testing of all systems in order to identify system vulnerabilities. Designs, implements, and reports on security system and end user activity audits.
- Monitors server logs, firewall logs, intrusion detection logs, and network traffic for unusual or suspicious activity. Interprets activity and make recommendations for resolution.
- Administers and maintains end user accounts, permissions, and access rights to PCs, systems, appliances, and devices. Provides on-call security support to end-users.

Technical Leadership—
Leads the design, planning, execution and support of major initiatives to enhance IT service delivery following best practices in Change Management, Enterprise Architecture and Project Management

- Influences change management on an ongoing basis, taking steps to remove barriers, accelerate its pace, and supports others through the change.
- Ensures enterprise-level IT specifications align with the agency's business requirements. Documents all design and analysis work in an integrated repository for enterprise access and reuse.
- Has the knowledge of information safeguarding principles to use appropriate privacy management techniques for accomplishing tasks and objectives.
- Prepares and implements plans utilizing a variety of project management templates for a given initiative both short and long term to quality, cost, and time constraints.

FUNCTIONAL COMPETENCIES

- Broad hands-on knowledge of firewalls, intrusion prevention and detection systems, anti-virus software, data encryption, and related industry-standard techniques and practices.
- In-depth technical knowledge of network, end computing devices, and operating systems, including Cisco, Microsoft, and VMware products.
- Strong knowledge of TCP/IP and network administration/protocols, including Software Defined Network (SDN)
- Hands-on experience with devices such as hubs, switches, and routers.
- Advanced knowledge of applicable practices and laws relating to data privacy and protection.
- Demonstrated knowledge of federal security standards such as FIPS-199, FIPS-140-2, and NIST-800-53.

REQUIRED EDUCATION & PROFESSIONAL CERTIFICATIONS

- Bachelor's Degree in computer science or closely related field.

- Certifications in information security such as CISSP, Security+, SSCP, and GSEC are a plus.
- Certifications in information systems network and infrastructure management such as MCSE, ITIL and CCNP are a plus.

JOB EXPERIENCE (Years & Type)

- Seven years' experience in the field of information technology and systems security operations.

DCRB is an Equal Opportunity Employer. In compliance with the Americans with Disabilities Act, the employer will provide reasonable accommodations to qualified individuals with disabilities and encourage both prospective employees and incumbents to discuss potential accommodations with the employer.

WORKING CONDITIONS:

- Normal office environment

COMPENSATION LEVEL: DCRB Grade 09

This job description indicates the general nature and level of work to be performed by an employee in this job. It is not intended to be an exhaustive list of all tasks, duties, and qualifications of an employee assigned to this job. The employee may be asked to perform other duties as assigned.

RANKING FACTORS: NONE

HOW TO APPLY: Applicants must submit a completed DC2000 Employment Application form, letter of interest discussing eligibility and qualifications, and resume. The DC2000 Employment Application is available as a fillable file document on the "Working at DCRB" page on DCRB's website. You may view the page here: http://dcrb.dc.gov/service/working-dcrb

Applicants claiming Veterans Preference must submit official proof with application.

All educational and experience requirements used to determine eligibility for this position must be officially verified at the time of appointment. No offer of employment will be deemed fulfilled without such verification(s).

WHERE TO APPLY:

Via Fax to: (202) 343-3302
Attention: HR Director

Via Email to: dcrb.vacancies@dc.gov

NOTE: It is imperative that all information on the DC2000, resume and supporting documents be both accurate and truthful and is subject to verification. Misrepresentations of any kind may be grounds for disqualification for this position or termination.

NOTICE OF NON-DISCRIMINATION: In accordance with the DC Human Rights Act of 1977, as amended, DC Official Code, §2-1401.01, et seq. (Act), the District of Columbia Public Schools does not discriminate in its programs and activities on the basis of actual or perceived race, color, religion, national origin, sex, age, marital status, personal appearance, sexual orientation, family status, family responsibilities, matriculation, political affiliation, disability, source of income or place of residence or business. Sexual harassment is a form of sex discrimination, which is prohibited by the Act. In addition, harassment based on any of the above protected categories is prohibited by the Act. Discrimination in violation of the Act will not be tolerated. Violators will be subject to disciplinary action.

NOTICE OF BACKGROUND INVESTIGATION AND PENALTIES FOR FALSE STATEMENTS: An offer of employment with the DCRB in contingent upon the completion and satisfactory results of a criminal, education and financial background investigation conducted by the DCRB or authorized agent prior to commencement of duty. In addition, an offer of employment for a position with specified education and certification qualification requirement(s) is contingent upon the completion and satisfactory result of an educational and/or certification background investigation conducted by the DCRB or authorized agent prior to commencement of duty (Pursuant to DCRB Policy No. DCRB-09-1-01).

Applicant understands that a false statement on any part of your application, including materials submitted with the application, may be grounds for not hiring you, or for firing you after you begin work (D.C. Official Code, section 1- 616.51 *et seq.*) (2001). Applicant understands that the making of a false statement on the application or on materials submitted with the application is punishable by criminal penalties pursuant to D.C. Official Code, section 22-2405 *et seq*. (2001).

DRUG-FREE WORK PLACE ACT OF 1988: "PURSUANT TO THE REQUIREMENTS OF THE DRUG-FREE WORKPLACE ACT OF 1988, THE INDIVIDUAL SELECTED TO FILL THIS POSITION WILL, AS A CONDITION OF EMPLOYMENT, BE REQUIRED TO NOTIFY HIS OR HER IMMEDIATE SUPERVISOR, IN WRITING, NO LATER THAN FIVE (5) DAYS AFTER CONVICTION OF OR A PLEA OF GUILTY TO A VIOLATION OF ANY CRIMINAL DRUG STATUTE OCCURRING IN THE WORKPLACE."

OFFICIAL JOB OFFERS ARE MADE ONLY BY THE DCRB HUMAN RESOURCES