POSTAL REGULATORY COMMISSION
JOB VACANCY NOTICE
VACANCY NUMBER: PRC 05-23
OPEN: January 13, 2023
CLOSE: February 3, 2023

POSITION TITLE:	**CYBERSECURITY SPECIALIST**
GRADE:	**PRC- 6**
SALARY RANGE:	**$132,368 – $176,458**
LOCATION:	**POSTAL REGULATORY COMMISSION** **OFFICE OF THE SECRETARY AND ADMINISTRATION** **901 NEW YORK AVENUE, NW, SUITE 200** **WASHINGTON, DC 20268-0001**
TELEWORK ELIGIBLE:	**YES – REMOTE WORK POTENTIAL**
APPOINTMENT TYPE:	**PERMANENT**
SECURITY CLEARANCE:	**PUBLIC TRUST BACKGROUND INVESTIGATION**
INFORMATION:	**ONE POSITION MAY BE FILLED UNDER THIS VACANCY ANNOUNCEMENT**
WHO MAY BE CONSIDERED:	**OPEN TO ALL US CITIZENS**
APPLICATION PERIOD:	**3 WEEKS**

INTRODUCTION

The Postal Regulatory Commission is seeking a talented and dynamic Cybersecurity Specialist to join its Office of the Secretary and Administration to support the Chief Information Security Officer in building a secure and modern cybersecurity program for the agency. This position is a unique opportunity for a cybersecurity professional who wants to make a positive impact at a small Federal agency while continually enhancing their technical capabilities and expertise.

LEARN MORE ABOUT THIS AGENCY

The Postal Regulatory Commission is an independent establishment of the executive branch created by the Postal Accountability and Enhancement Act (PAEA) to provide strengthened oversight of the Postal Service. The five-member bipartisan Commission promotes high quality universal mail service for the American people by ensuring Postal Service transparency, accountability, and compliance with the law. The Commission is the primary regulator of the Postal Service and works to provide appropriate insight into postal rates, finances, and service to stakeholders and the public.

WORK ENVIRONMENT

This position is in the Office of the Secretary and Administration (OSA) which handles all Commission operations, including Administrative Services, Information Technology, Finance (Budget, Accounting, Procurement), Human Resources, Data Management, Strategic Planning, Facilities, Health and Safety, Records Management, Privacy, and more. As a result of these expansive responsibilities and small number of staff, OSA team members tend to possess entrepreneurial spirits, wear multiple hats, and engage in high levels of cooperation to ensure the Commission operates effectively and efficiently. This position is eligible for remote work.

MAJOR DUTIES AND RESPONSIBILITIES

The major duties of this position fall under multiple core Cybersecurity functional areas: Cybersecurity Compliance, Cybersecurity Operations, Cybersecurity Policy, and Training. This position is responsible for governance, risk, and cybersecurity compliance directly pertaining to network security monitoring, cybersecurity architecture planning, research and development, vulnerability management, incident handling, and a cybersecurity program oversight to meet Commission regulatory compliance and Federal Information Security Modernization Act (FISMA) mandates. This non-supervisory position works under the direction of the Chief Information Security Officer (CISO).

Compliance

- Manages, plans, and executes annual security assessments following the PRC Security Assessment and Authorization (SA&A) process for all PRC systems including FedRamp Authorized services and recommend efficiencies as needed.
- Advises, assists, and supports the CISO is developing, overseeing, maintaining, and improving the Commission's Cybersecurity Program.
- Responsible for monitoring and maintaining an up-to-date Plan of Action and Milestone (POA&M) repository, enter new POA&Ms as needed, and send a monthly POA&M report to the CISO and Authorizing Official.
- Manages and applies all updates to ensure the Commission's National Institute of Standards and Technology (NIST) 800-53 worksheets algins with current NIST Revision.
- Monitors, conducts research, recommends action, and responds to developments in cybersecurity, including directives through Executive Order, Office of Management and Budget (OMB), Cybersecurity and Infrastructure Security Agency (CISA), and any other applicable guidance. Assists with data entry and assessment for all Cyber compliance reporting, including input into CyberScope.
- Conducts comprehensive research, develops, and updates comprehensive information security system and application policies, guidelines, standards, requirements, and procedures. Recommends ways to protect the organization's information and information systems.

Cybersecurity Operations

- Attains and maintains technical expertise of Commission's cybersecurity tools, including CrowdStrike, Microsoft SCCM Patch Manager (SCCM). Shall attain proficiency with the QualysGuard Cloud Platform including Vulnerability Management, Detection and Response (VMDR), Hardware Asset Management (HWAM), Software Asset Management (SWAM), Continuous Monitoring, and Policy modules within one year.
- Manages vulnerability reporting, monitors, and generates security vulnerability reports, and assists the support team to remediate software flaws within Commission timeframes.
- Manages logging solution that complies with Federal directives and investigates, analyzes, and provides notification for security events.
- Serves as a member of the Incident Response Team. Assists with investigation, analysis, and response to vulnerabilities and cyber incidents.
- Reviews secure baselines using Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS) or other baselines as needed for full compliance, excluding exceptions that are approved by the CISO for operational reasons.
- Responsible for monitoring all accounts, configurations, and systems for policy compliance, including but not limited to Change Requests, adherence to the concept of Least Privilege, password policies, and rules of behavior.

- Serves as member of Contingency team, assists with testing, log capture, recommendations, and assists with continuity of operations planning and execution by implementing, configuring, and ensuring availability of an alternate processing site in the event of a contingency. Monitors and ensures backup data is available to the Commission in the event of a loss of data.
- Understands, recommends, and applies rules for data security standards, including encryption algorithms, (e.g., ensure all communication in transit is protected by Federal Information Processing Standards (FIPS) 140-2 validated encryption modules), host/network access control mechanisms, rules for ports, service, and firewall rules, sanitization of data, personally identifiable information (PII) and controlled unclassified information (CUI) data security standards.
- Develops and maintains current diagrams, flow charts, and system procedures as directed by the CISO.
- Monitors and responds to its internal security reports and notifications through the Commission's external Vulnerability Disclosure Policy.

QUALIFICATIONS AND EVALUATION

You will be evaluated by a screening panel based on evidence of your ability to successfully perform the duties of the position according to the qualifications outlined in this announcement. The panel will forward the appropriate candidates to the Secretary and Chief Administrative Officer for further consideration and possible interview.

EDUCATION AND EXPERIENCE

This position requires experience in Cybersecurity Compliance, Cybersecurity Data Analysis, vulnerabilities mitigation and Cybersecurity Policy/Training.

Special qualification requirements include extensive experience in NIST guidance with working knowledge in performing SA&A as defined in NIST SP 800-37 and 800-53. The candidate must have experience in the field of Security Operations. Highly-qualified candidates will have experience with Continuous Diagnostics and Mitigation Program (CDM) provided security tools such as QualysGuard and CrowdStrike and understand how to use these tools for network vulnerability scanning, malware, HWAM/SWAM, application scanner, configuration monitoring, and continuous monitoring. Experience in developing cybersecurity policy and providing security training, incident training, and contingency training.

Highly-qualified candidates will have specialized experience in cloud technology, architectures, and service levels, as well as Microsoft 365 services such as SharePoint, PowerBI, and Teams.

Generally accepted industry certifications such as Information Systems Audit and Control Association (ISACA), International Information System Security Certification Consortium (ISC2) are preferred but not required.

ETHICS REQUIREMENTS

The Commission is committed to government ethics. As a Commission employee, you will be subject to the Standards of Ethical Conduct for Employees of the Executive Branch and the criminal conflict of interest statutes. Commission employees are also subject to Commission-specific ethics rules (39 C.F.R. subpart A of part 3001 and supplemental standards of ethical conduct [5 C.F.R. part 5601]). The supplemental standards prohibit Commission employees, as well as their spouses and dependent children, from owning any securities issued by entities that are identified on the Commission's annually published prohibited securities list. As an employee of the Commission, you must complete initial ethics training within three months of your appointment and, depending on your position, complete required financial disclosure forms within 30 days of your appointment.

BENEFITS

A career with the U.S. Government provides employees with a comprehensive benefits package. As a federal employee,

you and your family will have access to a range of benefits that are designed to make your federal career very rewarding.

For more information, visit either https://www.opm.gov/healthcare-insurance/Guide-Me/New-Prospective-Employees/ **or** https://www.opm.gov/healthcare-insurance/Guide-Me/Federal-Employees/

You will earn annual **vacation leave**. More info: http://www.opm.gov/policy-data-oversight/pay-leave/leave-administration/fact-sheets/annual-leave/.

You will earn **sick leave**. More info: http://www.opm.gov/policy-data-oversight/pay-leave/leave-administration/fact-sheets/sick-leave-general-information/.

You will be paid for **Federal holidays** that fall within your regularly scheduled tour of duty. More info: https://www.opm.gov/policy-data-oversight/pay-leave/federal-holidays/#url%3D2023

If you are a current Federal employee, you can boost your retirement savings by participating in the Thrift Savings Plan(TSP). The TSP offers the same types of savings and tax benefits as a 401(k) plan.

If you use public transportation, part of your **transportation costs** may be subsidized. Our human resources office can provide additional information on how this program is run.

You may participate in the **Flexible Spending Account (FSA)** program for expenses that are tax-deductible, but not reimbursed by any other source, including out-of-pocket expenses and non-covered benefits under their FEHB plans.

CONDITIONS OF EMPLOYMENT

- You will be required to serve a probationary period of 1 year.
- Relocation expenses are not authorized.
- You will be required to participate in direct deposit.
- **Fair Labor Standards Act (FLSA) Status:** Exempt
- You must be a **U.S. citizen or national** to be eligible for this position.
- You must successfully pass a background investigation.
- This position may require you to submit a Public Financial Disclosure Report (OGE 278) upon entry and annually thereafter.
- The Postal Regulatory Commission uses e-Verify, an Internet-based system, to confirm the eligibility of all newly hired employees to work in the United States. Learn more about E-Verify, including your rights and responsibilities.

REASONABLE ACCOMMODATION

If you need reasonable accommodation for a disability, please contact the Commission's HR office at HR@prc.gov or Sherri Proctor at 202-789-6869. If you have a hearing impairment, you may call the Federal Information Relay Service at 1-800-877-8339 for assistance in contacting the person named above.

EEO POLICY STATEMENT

The U.S. Postal Regulatory Commission is an Equal Opportunity Employer. The United States Government does not discriminate in employment on the basis of race, color, religion, sex (including pregnancy and gender identity), national origin, political affiliation, sexual orientation, marital status, disability, genetic information, age, membership in an employee organization, parental status, military service, or other non-merit factor.

VETERAN INFORMATION

If you are claiming veterans' preference, you must submit a copy of your DD-214 (Member 4 copy), or other official documentation from a branch of the Armed Forces or the Department of Veterans Affairs showing dates of service and type of discharge. Ten-point preference eligibles must also submit an application for 10-point Veteran Preference, SF-15, along with the required documentation listed on the back of the SF-15 form. For more information on veterans' preference

view Feds Hire Vets.

LEGAL AND REGULATORY GUIDANCE

Social Security Number–Your Social Security Number is requested under the authority of Executive Order 9397 to uniquely identify your records from those of other applicants who may have the same name. As allowed by law or Presidential directive, your Social Security Number is used to seek information about you from employers, schools, banks, and others who may know you. Failure to provide your Social Security Number when requested will result in your application not being processed.

Privacy Act–Privacy Act Notice (PL 93-579): The information requested here is used to determine qualifications for employment and is authorized under 5 U.S.C. §§ 3302 and 3361.

Signature–Before you are hired, you will be required to sign and certify the accuracy of the information in your application.

False Statements–If you make a false statement in any part of your application, you may not be hired; you may be fired after you begin work; or you may be subject to fine, imprisonment, or other disciplinary action.

Selective Service–If you are a male applicant born after December 31, 1959, on request you must certify that you have registered with the Selective Service System or are exempt from having to do so under the Selective Service Law.

ADDITIONAL INFORMATION

Receiving Service Credit or Earning Annual (Vacation) Leave: Federal Employees earn annual leave at a rate (4, 6 or 8 hours per pay period) which is based on the number of years they have served as a federal employee. The Commission may offer Federal employee's credit for their job-related non-federal experience or active-duty uniformed military service. This credited service can be used in determining the rate at which they earn annual leave. Such credit must be requestedand approved prior to the appointment date and is not guaranteed.

WHAT TO EXPECT NEXT

Once your online application is submitted you will receive a confirmation notification by email. After we receive application package (including all required documents) and the vacancy announcement closes, we will review applications to ensure qualification and eligibility requirements are met. Please ensure that your application includes all required documents as we will not process applications missing a cover letter, etc. After the review is complete, the best qualified candidates will be referred to the hiring manager for further consideration and possible interview. Applicants will be notified of their status by email, referred applicants will be notified as such and may be contacted directly by the hiring office for an interview. All referred applicants will receive a final notification once a selection decision has been made.

HOW TO APPLY

Applicants must apply through the online application system USAJOBS.gov. Follow the prompts to register, answer a few questions and submit all required documents.

If you already have a USAJOBS account, click "*Apply Online*" and follow the prompts to attach any additional documents that may be required.

In order for your application to be considered complete, the following documents *must* be submitted:

1. Cover Letter (no more than two pages)
2. Resume must contain the following information:
    a. name
    b. address
    c. contact information

d. *If you are claiming veteran's preference, you must indicate the type of veteran's preference you are claiming on your resume*
e. detailed work experience related to this position as described in the major duties including:
    i. dates of employment
    ii. title
    iii. grade (for Federal employment)
f. education

3. Current and former Federal employees must submit a copy of your last or most recent SF-50, "Notice of Personnel Action" to indicate your current federal status. If the most recent SF-50 has an effective date within the past year, it may not clearly demonstrate that you possess the years of experience required for this vacancy. You must provide additional SF-50s that clearly demonstrate that you meet the years of experience required for this vacancy. (The SF-50 must show your tenure, grade and step, and type of position occupied. [i.e., Excepted or Competitive])
    a. Performance award, Realignment, and Detail SF-50's **will not be accepted** as proof of grade or tenure.
4. Five-point veterans must submit a DD214 (member 4 copy)

Failure to provide this documentation will result in your application not receiving 5-point preference.

5. Ten-point veterans ***must*** submit the following:
    a. A copy of your DD214
    b. Application for 10-point Veteran's preference, SF-15 http://www.opm.gov/forms/pdf_fill/sf15.pdf
    c. A copy of the official letter from VA, dated 1991 or later, certifying the service-connected disability and indicating the percentage of disability
    d. If you're currently serving on Active Duty: submit a letter from your unit identifying the branch of service, period(s) of service, campaign badges or expeditionary medals earned, type of discharge, character of service, and the date you will be separated or be on approved terminal leave. If you supply a statement of service at this stage, your preference/eligibility will be verified by a DD214 (Member 4 Copy) upon separation from the military.

Failure to provide this documentation will result in your application not receiving 10-point preference.

To gain access to your DD214 online, please visit: http://www.archives.gov/veterans/military-service-records/

Application packages will NOT be accepted via email, mail or fax. All applications must be received by 11:59 pm on the closing date.

This vacancy announcement will be open from January 13, 2023, through February 3, 2023. Complete application packages must be submitted at the time that you apply to receive consideration. Additional documents will not be accepted after the vacancy closes.

For More Information
You can obtain forms and additional information by contacting Kerry Grega at 202-789-6834 or hr@prc.gov.