IA-25-45A-PC (Internal)
Information Technology Security Specialist

The agency will review up to 100 application packages for this position. Applications must be submitted via email and only the first 100 received will be considered.

Overview

Open & Closing Dates

6/24/2025 to 7/9/2025

Service

Excepted

Pay Scale & Grade

GG-14

Salary

$142,488.00 to $ 185,234.00 / Per Year

Appointment Type

Permanent

Work Schedule

Full-time

Location

Arlington, Virginia

Relocation Expenses Reimbursed

No

Telework Eligible

Yes - as determined by the agency policy.

Security Clearance

Moderate Background Investigation

Application Count

100

Job family (Series)

2210 Information Technology Management

Drug Test

Yes

This Job Is Open To

Hiring Path

Internal to an agency

Hiring Paths Clarification Text

Current United States Postal Service Office of Inspector General, United States Postal Service and United States Postal Inspection Service and Postal Regulatory Commission Employees only.

Summary

***PLEASE NOTE THAT THIS VACANCY ANNOUNCEMENT IS ONLY OPEN TO CURRENT UNITED STATES POSTAL SERVICE OFFICE OF INSPECTOR GENERAL, UNITED STATES POSTAL SERVICE, UNITED STATES POSTAL INSPECTION SERVICE AND POSTAL REGULATORY COMMISSION EMPLOYEES. OTHER APPLICANTS WILL NOT BE CONSIDERED.**

This announcement provides a reassignment/promotion opportunity to fill our Information Technology Security Specialist position in the Office of Chief Information Officer (CIO) located in Arlington, VA. Bring your skills and voice to our team!

Duties

The successful candidate will be a technical expert authority responsible for the application security function and for information technology security (Cybersecurity/InfoSec) engineering, and design. Responsibilities include solving significant problems complicated by interfaces and inter-relationships between and among programs, systems, functions, applications, and numerous critical issues for agency-wide information technology solutions, operations, and maintenance supporting the security of agency infrastructure, systems, and information.

Candidates will be evaluated on the skills that they possess that are directly related to the duties of the position and the experience, education and training that indicate the applicant's ability to acquire the particular knowledge and skills needed to perform the duties of the position. Only those candidates who meet all qualification and eligibility requirements and who submit the required information by 11:59 PM EST on 7/9/2025 will be considered.

The USPS OIG uses a Pay Banding system, which is equivalent to the Federal GS scale. Grade and salary determinations will be made based upon a candidate's education and professional experience.

This position is being advertised at the Specialist Band level, equivalent to a GS-14. The salary range for this position is $142,488.00 - $185,234.00. The salary figures include locality pay.

Please note that the duties and responsibilities associated with this position may vary based upon the agency's needs at the time of hire. The following description of major duties and responsibilities is only intended to give applicants a general overview of the expectations.

- Establishes, implements, and interprets the requirements for agency compliance with policy directives governing cybersecurity protection.

- Performs thorough security operations center analysis of potentially malicious or suspicious threats.
- Effectively administers and sustains enterprise level application security scanning tools for all COTS, GOTS, Web Applications, and internally developed cloud-based applications.
- Conducts risk and vulnerability assessments of planned and installed information systems applications to identify vulnerabilities, risks, and protection needs.
- Conducts systems security evaluations, audits, and reviews.
- Develops cybersecurity plans, processes, and procedures.
- Participates in network and system design to ensure implementation of appropriate cybersecurity policies as they relate to application security.
- Facilitates the gathering, analysis, and preservation of evident used in the prosecution of cybercrimes.
- Updates or establishes new application security requirements.
- Assesses security events to determine impact and implementing corrective actions.
- Ensures the rigorous application of information security/cybersecurity policies, principles, and practices in the delivery of all IT services.
- Identifies current and potential problem areas.
- Monitors agency compliance with application cybersecurity protection requirements across IT programs.
- Ability to handle multiple tasks and work independently as well as in a team.

Requirements

Conditions of Employment

- Must be a U.S. citizen.
- Must be able to pass a drug screening.
- Must be able to pass a background investigation.
- Must be able to obtain and maintain Moderate Background Investigation security clearance.
- Must be able to obtain and maintain a government-issued credit card.
- May be required to successfully complete a 12-month probationary period.

MINIMUM QUALIFICATIONS

You must meet ALL of the minimum qualifications listed below.

- Bachelor's Degree in Computer Science, Computer Engineering, Cybersecurity/Information Technology Security or related field of study from an accredited college or university

OR

- Must have at least 5 years of specialized hands-on experience in application security testing

AND

- Must have at least 5 years of specialized experience with hands-on skills in performing application security assessments
- Must have at least 5 years of specialized experience in Secure SDLC and Source Code Analysis (Manual &Tools) on Web-based Applications
- Must have hands-on experience with Static and Dynamic Application Security Testing using tools like HP Fortify, HP WebInspect, HCL Appscan, Snyk, Checkmarx, Synopsys, and Veracode
- Must have specialized experience in Continuous Integration (CI) and Continuous Deployment (CD) practices
- Must have specialized experience in manual code review with the ability to identify potential vulnerabilities and best coding practices
- Must have specialized experience in application vulnerability and security assessments using various tools like Burp Suite Pro, OWASP Zap Proxy, DirBuster, Kali Linux, Metasploit Pro, Accunetix, Insight AppSec, GitLab, Coverity, Fortify, and GitHub Enterprise
- Must have specialized experience in assessing application vulnerabilities and bugs in various applications
- Must have specialized experience creating security testing pipelines and test plans
- Must have specialized experience in implementing and deploying an organization-wide Application Security program (DAST and SAST) at the enterprise level to identify, report and remediate security vulnerabilities in development and production environments
- Must have knowledge of coding languages such as Java, .NET, Python, PHP, C++, C#
- Must have extensive experience in preparing test Plans, writing test Cases, test Execution and follow up remediation efforts

DESIRABLE QUALIFICATIONS

- Microsoft 365 Certified Security Administrator Associate
- Microsoft Certified Azure Security Engineer Associate
- Advanced degree in Cybersecurity or related field
- Current Industry Certifications in one or more of the following (or equivalent)
    - Certified Secure Software Lifecyle Professional (CCSP)
    - Certified Cloud Security Professional (CSSLP)
    - Offensive Security Certified Professional (OSCP)
    - EC-Council Certified Application Security Engineer (CASE)
    - GIAC Certified Web Application Defender (GWEB)
    - Azure Developer Associate

EVALUATION FACTORS

You must have the experience, knowledge and skills as listed in EACH of the evaluation factors. Failure to demonstrate that you meet all the evaluation factor requirements as listed below will result in a score of zero (0); an ineligible status, and you will not be referred for further consideration. Include your major accomplishments relevant to the position requirements in your resume.

- Demonstrated expertise in configuring, deploying and utilizing both dynamic and static application security testing tools.
- Demonstrated knowledge of application-based, host-based, and network-based security best practices.
- Knowledge in applying advanced information technology principles, concepts, methods, standards, and practices sufficient to develop and interpret policies, procedures, and strategies governing the planning and delivery of services throughout the agency.
- Demonstrated ability to cultivate relationships across multiple teams to effectively implement security recommendations.
- Demonstrated ability to communicate effectively both orally and in writing with audiences of various levels of technical understanding.

You will no longer be considered for this position if you receive a zero (0) rating on any evaluation factor.

Failure to demonstrate that you meet all evaluation factor requirements will result in a score of zero (0). Upon receipt of a zero score, you will be deemed "not minimally qualified," and you will not be referred for further consideration.

Education

Education must be accredited by an institution recognized by the U.S. Department of Education. Applicants can verify accreditation here: www.ed.gov.

Special Instructions for Candidates with Foreign Education:
Education completed outside the United States must be deemed equivalent to that gained in U.S. education programs. You must submit all necessary documents to a private U.S. credential evaluation service to interpret equivalency of your education against courses given in U.S. accredited colleges and universities. For further information visit: https://sites.ed.gov/international/recognition-of-foreign-qualifications.

Additional information

Pay is only part of the compensation you will earn working for the USPS OIG. We offer a broad array of benefits programs:

As a result of the passage of the Postal Service Reform Act of 2022 (PSRA), USPS employees (including USPS OIG) and retirees will transition from the Federal Employees Health Benefits (FEHB) Program to the Postal Service Health Benefits (PSHB) Program effective January 1, 2025.

Detailed information about eligibility and enrollment will be provided upon hiring. For more information, visit the Postal Service Health Benefits (PSHB) Program website at https://www.opm.gov/healthcare-insurance/pshb/#url=Overview

We offer Health, Dental, Vision, Life and Long-Term Care Insurances with Flexible Spending options as well. For more information about these programs visit: https://www.opm.gov/healthcare-insurance/Guide-Me/Federal-Employees/

Retirement and Thrift Savings. For more information about these programs see https://www.opm.gov/retirement-center/ and tsp.gov/.

Flexible Work Schedules. USPS OIG offers a range of family-friendly flexibilities including flexible work schedules, telework and employee assistance programs.

Leave and Holidays. In addition to eleven (11) paid holidays each year, you will earn thirteen (13) days of paid sick leave and thirteen (13) to twenty-six (26) paid vacation days each year depending on your years of service.

Fair Labor Standards Act (FLSA) Status: EXEMPT. (Nonexempt employees are entitled to overtime pay; Exempt employees are not).

Our agency provides Reasonable Accommodations for applicants with disabilities. If you require accommodations during any part of the application and/or hiring process, please contact us by sending an email to SupportHiring@uspsoig.gov. The decision on granting an accommodation request will be made on a case-by-case basis.

How You Will Be Evaluated

You will be evaluated for this job based on how well you meet the qualifications above.

The Human Resources Office will review your resume and supporting documentation to ensure that you meet the minimum qualifications required for this position. You will no longer be considered for this position if you: receive a zero (0) rating on any evaluation factor; fail to attach all required documentation; if your application materials indicate that you are not minimally qualified for this position; or if you fail to qualify on the interview.

Only the top-rated candidates will be referred to a review official or the selecting official for further consideration. Top-rated applicants may be required to participate in an interview. Your rating may be further adjusted or rated as ineligible by the review official or the selecting official based on your interview performance. Once all applicant scores are finalized, the selecting official will make a final decision.

NOTE: If you receive a zero (0) rating on any evaluation factor or on the interview, you will be considered NOT MINIMALLY QUALIFIED for the position and rated ineligible.

Applicants for this position may be interviewed one or more times as part of the hiring process. During interviews, applicants may not use any AI tool or virtual assistant (such as ChatGPT) to help them answer questions, except for accessibility tools used as part of a reasonable accommodation. Applicants who fail to follow these rules will be disqualified from the hiring process.

Required Documents

You must submit all required documents by 11:59 PM EST on the closing date of this announcement. Make sure you include the vacancy announcement number in the subject line when submitting your application package. For information on submitting application packages, please review the ‘How to Apply’ section. This announcement number for this vacancy is: EX-25-45B-PC.

1. RESUME. Required. It is essential that your resume and supporting documentation provide sufficient information to substantiate your qualifications for the announced position.

2. COMPLETE APPLICATION QUESTIONNAIRE. **Required.** Download the Application Questionnaire (PDF), complete the form, and include it in the application package.

3. SF-50: Required, if applicable. If you are or have been a federal employee. This is to demonstrate tenure and competitive/excepted service for eligibility purposes. (**Required:** Name the file as **"SF-50"** or **"Form 50"**).

4. SUPPORTING DOCUMENTS: Required, if applicable. Degrees, Certificates, and Licenses. If there is an education, certification, and/or license requirement for this vacancy, relevant documents must be included in the application package.

If you are relying on your education to meet qualification requirements:

Education must be accredited by an accrediting institution recognized by the U.S. Department of Education in order for it to be credited towards qualifications. Therefore, provide only the attendance and/or degrees from www.ed.gov.

Failure to provide all the required information as stated in this vacancy announcement may result in an ineligible rating or may affect the overall rating.

How to Apply

To apply for this position, you must submit an application package containing all required documents, e.g., resume, application questionnaire, performance appraisals, SF-50, Veterans' preference documents, transcripts, and/or supporting documents, etc. The application questionnaire is available as a PDF in the vacancy announcement. The complete application package must be submitted via email at SupportHiring@uspsoig.gov by 11:59 PM (EST) on the closing date, Wednesday July 9, 2025, to receive consideration**.**

Please include the vacancy number in the subject line when you are submitting your application package and all email communications pertaining to this vacancy announcement.

For any questions on this vacancy announcement, please contact SupportHiring@uspsoig.gov.