**VACANCY ID #** **189919** **EMPLOYMENT ANNOUNCEMENT**

A picture containing text, outdoor, sign

Description automatically generated

**TITLE: INFORMATION TECHNOLOGY SPECIALIST 3 (INFORMATION SECURITY)**

**STATUS: PERMANENT NON-COMPETITVE**

**BUREAU: INFORMATION TECHNOLOGY**

**LOCATION: LATHAM**

**SALARY: PEF SG23 ($86,681 – $109,650)**

**MINIMUM QUALIFICATIONS:**

Bachelor’s degree with at least 15 credit hours in cyber security, information assurance, or information technology; and two years of information technology experience, at least one year of which is information security or information assurance experience.

OR

A bachelor's degree in any field with at least three years of information technology experience, at least one year of which is information security or information assurance experience.

OR

An associate's degree in any field with five years of general information technology experience at least one of which is information security or information assurance experience.

OR

At least seven years of information security or information assurance experience.

**PREFERRED QUALIFICATIONS:**

* 2+ years of infrastructure security or security operations experience
* 5+ years of information technology administration experience or equivalent combination of work and educational experiences
* In-depth knowledge of network protocols, network security principles, and firewall management
* Knowledge of vulnerability management processes, including patching, remediation, and system hardening
* Proven knowledge of security (preferred - CISSP, CISA, CISM, GPEN, GWAPT, GCIH, other GIAC certifications, OSCP, CEH, Security+, etc.)
* Understanding of CIS Benchmarks and implementation procedures in order to bring infrastructure and systems into compliance through hardening
* Experience utilizing various vulnerability and SIEM tools such as CrowdStrike, Splunk, Arctic Wolf, Tenable (Nessus)

**JOB SUMMARY:**

Under the direction of the Manager of Information Technology Services (Information Security) 1 of the Security Operations Unit, the Information Technology Specialist 3 (Information Security) will serve as an

Infrastructure Security Specialist, responsible for securing IT infrastructure, including firewalls, network security, and system hardening. This role requires expertise in both on-premises and cloud infrastructure, performing vulnerability assessments and responding to security incidents. This position will ensure that the OAG’s infrastructure remains resilient against cyber threats through the implementation of robust security policies and practices that safeguard critical systems and data. This role plays a crucial part in protecting the agency's infrastructure from vulnerabilities, reducing risk and ensuring the security of sensitive data across the organization.

**DUTIES:**

* Conduct network monitoring and intrusion detection analysis using various computer network defense tools, such as intrusion detection/prevention systems, firewalls, and host-based security systems.
* Conduct log-based and endpoint-based threat detection to detect and protect against threats coming from multiple sources.
* Correlate activity across assets (endpoint, network, apps) and environments (on-premises, cloud) to identify patterns of anomalous activity.
* Monitor and defend infrastructure environments, including physical data centers, virtualized environments, and cloud services.
* Conduct regular vulnerability assessments on infrastructure elements (servers, firewalls, network devices, etc.).
* Maintain and update infrastructure vulnerability management program to address newly discovered threats.
* Implement and enforce strict access control policies for infrastructure components; focused on RBAC, least-privileged, and zero trust architecture.
* Develop, implement, and enforce infrastructure security policies, procedures and standards that align with industry best practices (NIST, CIS).
* Participate in infrastructure design and reviews with various teams throughout the bureau to ensure new systems and services are designed and implemented with security.
* Participate in tabletop and actual exercises to validate the agency’s infrastructure security.
* Other duties as assigned.

**HOURS OF WORK:**

The agency's hours of operation are Monday through Friday, between 8:30 a.m. and 5:00 p.m. (37.5 hours/week). Scheduling determinations are dependent upon the needs of each bureau and will be communicated during interviews.

**HOW TO APPLY**

In your submission, you must provide sufficient information to determine from your resume and/or cover letter that you meet the minimum qualifications stated above. If a certificate or degree is required to demonstrate that you meet the minimum qualifications, you must provide proof that you hold the required certificate or degree. To apply, please send your resume, cover letter, and a copy of your degree/transcript (if applicable) to [HR.Recruitment@ag.ny.gov](mailto:HR.Recruitment@ag.ny.gov). Be sure to include Vacancy # 189919 and Title of the position in the subject heading of your email.

*Candidates from diverse backgrounds are encouraged to apply.*

*The OAG is an equal opportunity employer and is committed to workplace diversity.*

**Posted** June 10, 2025