NYC OFFICE OF THE COMPTROLLER

JOB VACANCY NOTICE

Title:	**IT Security Specialist - Security Audits (2 positions)**
Salary:	**$75,000 - $90,000**
Bureau/Division:	**Bureau of Audit / IT Audits**
Period:	**January 2, 2019 – Until Filled**

JOB DESCRIPTION

The New York City Comptroller's Office seeks a creative, detail-oriented, and hands-on IT and Information Security Specialist to assist with specialized IT and cybersecurity audits and act as subject matter expert in analyzing complex information systems, IT architectures, platforms, operating systems, storage & database solutions, virtualization configuration, encryption, digital certificates, directory services, communication components, networks, network security appliances, and servers.

The Audit Bureau's IT Division plans and executes a wide variety of information technology and cybersecurity audits of New York City government IT systems, projects, and contracts, in accordance with the New York City Charter and generally accepted government auditing standards. Under the supervision of the Manager of IT and Security Audits and the general direction of the Director, the IT Security Specialist's responsibilities include, but are not limited to, the following:

- Conducts research and analysis of City agencies' IT systems and cybersecurity posture, including software, hardware architecture and overall IT infrastructure to determine risks to the agency and report findings; reviews measures and controls, and provide a technical assessment; assess digital files and information systems against established City and industry standards, and latest security best practices;

- Conducts tests of internal controls for audits and investigations of IT, cybersecurity, telecommunications, and other projects involving technical services; performs audit procedures and security tests necessary to meet audit objectives or assigned tasks in compliance with Generally Accepted Government Auditing Standards including Information Technology and Security standards; assists the IT Auditors and supervisors during audits by providing specialized technical and IT cyber security training or orientation, as required;

- Prepares audit work papers, drafts audit findings and recommendations and discusses them with auditors and supervisors; assists in the development, updating, revising, and improving of IT audit testing procedures and programs and assists in creating technical cyber security audit programs;

- Reviews internal and external security controls including from outside vendors; reviews network, intrusion detection and prevention configuration systems, and vulnerability reports; analyzes weaknesses and deviations from best practices or published standards and recommends countermeasures;

- Acts as the IT Audit Division's representative in the field and as liaison between the Comptroller's Office and the agency/entity being audited, and,

- Performs other related work or special studies as may be required.

MINIMUM QUALIFICATION REQUIREMENTS

A baccalaureate degree from an accredited college, preferably in Computer Science, or a related field and four (4) or more years of progressively responsible experience in the field of IT/Cyber Security.

PREFERRED SKILLS IN ADDITION TO MINIMUM QUALIFICATIONS

- Demonstrated experience with IT security audits, IT security controls assessment, information security and cybersecurity, systems implementation and systems architecture in addition to working knowledge of NIST Special Publication 800-53 and Cybersecurity Framework;

- Familiarity with programming/scripting languages such as Java, C/C++, Ruby, Python, Perl, etc.;

- Demonstrated understanding of common cybersecurity tools such as Nessus, Nmap, Wireshark, Splunk, NetSparker, Snort or similar tools and in-depth knowledge of the current cyber threat landscape, with a specific focus on the technical aspects of adversarial Tactics, Techniques and Procedures (TTPs) and their relation to the cyber kill chain and other analytical models;

- Security audit expertise in Unix/Linix, Windows, distributed databases, web technologies, enterprise architecture, virtualization and technology infrastructure;

- Understanding of Web Application Firewalls (WAF), Network Access Control (NAC) systems on wired and wireless, Intrusion Detection/Prevention Systems (IDS/IPS), Distributed Denial of Service (DDOS) mitigation and Software Defined Networking (SDN) and Network Virtualization;

- Experience with networking security and configuration including Layer 2 and 3, spanning tree, VLANs, remote VPN software, IPSec, and network control protocols such as; QoS, PoE, DHCP, FTP, TFTP, SNMP, and security protocols such as; SSH, HTTPS, AAA and others;

- Experience with NIST, PCI-DSS, HIPAA, Sarbanes-Oxley, PII, ITIL, ISO 27001 and 27002, COSO principles and others standards and information security frameworks;

- Experience with backend storage systems SAN/NAS, virtual machine platforms, Windows/UNIX/Linux Server configuration, and Microsoft Active Directory/LDAP;

- Experience with security logs and the daily operational support of network appliances/firewalls, Security Information Event Management (SIEM), network DLP, vulnerability scanning, enterprise full disk encryption, database encryption and employee and vendor remote access security controls;

- Related industry certifications such as CCNA, MCSA, MCSE, VCP and CISSP or a closely related designation is desirable; and,

- Excellent interpersonal, communication, writing and organizational skills.

TO APPLY, GO TO: Employment Opportunities at www.comptroller.nyc.gov

Certain residency requirements may apply. We appreciate every applicant's interest; however, only those under consideration will be contacted.

Note: Vacancy notices listed as "Until Filled" will be posted for at least five workdays.

POSTING DATE:	POST UNTIL:	JVN:
January 2, 2019	**Until Filled**	**015/019/052**

The NYC Comptroller's Office is an Equal Opportunity Employer