

**City of New York  
Department of Information Technology & Telecommunications  
Job Posting Notice**

<b>Civil Service Title:</b> Computer Systems Manager	<b>Level:</b> M6
<b>Title Code No:</b> 10050	<b>Salary:</b> \$88,417/\$95,350 - \$202,000
<b>Business Title:</b> Citywide Chief Security Officer	<b>Work Location:</b> Brooklyn, NY
<b>Division/Work Unit:</b> Commissioner's Office	<b>Number of Positions:</b> 1
<b>Job ID:</b> 221905	<b>Hours/Shift:</b> Day - Due to the necessary technical management duties of this position in a 24/7 operation, candidate may be required to be on call and/or work various shifts such as weekends and/or evenings.

**Job Description**

**WHO WE ARE:**

The NYC Department of Information Technology & Telecommunication (DoITT) is New York City government's technology leader. Our mission is to modernize IT infrastructure and service delivery in government; implement state-of-the-art information technology solutions to improve public services; make government more transparent and accountable; and employ cutting-edge tools, methods, and partnerships to empower New Yorkers. Our services touch every aspect of City life: from public safety to human services, from education to economic development, our services cross the full spectrum of governmental operations.

To fulfill our mission, we develop and support applications, maintain efficient and reliable computing and network platforms, develop sophisticated security tools and policies, and ensure the reliability of IT infrastructure and enterprise systems through redundancy and disaster recovery planning. We also negotiate service agreements with telecommunications providers doing business with City agencies, and administer franchise agreements with telecommunications and cable television providers that serve NYC residents.

**THE OPPORTUNITY:**

As the City's IT security leader, DoITT is responsible for ensuring the protection of the City's IT systems and information. We have an opportunity for a Citywide Chief Security Officer to oversee development and delivery of a comprehensive information security strategy to optimize the security posture of the City's infrastructure. The Citywide Chief Security Officer will advise City leadership on proactive and progressive strategies to mitigate current and future cyber risks, and will be responsible for creation and delivery of regular security updates to City Executives. The incumbent will drive collaboration with State, Federal and private partners and will manage coordination across all sectors in case of a security incident.

**WHAT YOU WILL DO:**

Reporting directly to the DoITT Commissioner, with significant interaction with City agency IT security officers, the Mayor's Office, and State and Federal partners, the Citywide Chief Security Officer will:

- Oversee the Information Security Unit and the Citywide Security Operations Center within DoITT, managing a large team of employees and consultants;
- Work with City leadership to oversee the formation and operations of a city-wide information security program that is organized toward common goals in information security;
- Provide strategic leadership of the City's information security programs;
- Establish annual and long-range security and compliance goals, define security strategies, metrics, reporting mechanisms and program services; and create maturity models and a roadmap for continual program improvements;
- Review and approve the City's security architectures; including but not limited to network, application, data center and cloud security;
- Provide guidance and counsel to IT security managers at DoITT, NYPD, NYC Emergency Management, City Hall and City agencies in defining objectives and strategies for information security;
- Manage institution-wide information security governance, and chair an Information Security Advisory Committee which will include, at a minimum, City Hall, DoITT, Law, NYPD and NYCEM;
- Direct the development, dissemination of, and modifications of information security policies. Monitor compliance with and review the effectiveness of information security policies and procedures;
- Review and evaluate the information security aspects of the City's relationships with third-party technology providers and other vendors who have access to City and customer information and systems, including reviewing contracts to ensure they contain appropriate non-disclosure language and security commitments;
- Stay abreast of information security technologies, issues, and regulatory changes affecting government and participate in local, national and international policy and practice discussions;
- Represent the City in forums and on committees and boards in national and regional conferences, consortiums and collaborations;
- Coordinate and track all information technology and security related audits including scope of audits, timelines, auditing agencies and outcomes;
- Act as an internal information security consultant to the City's business and technology units, advising on risks, vulnerabilities and control practices on new and existing products and services, current and proposed changes to business processes and existing or planned technology systems;
- Keep abreast of security incidents and act as primary control point during significant information security incidents. Convene a Security Incident Response as needed, or requested, in addressing and investigating security incidences that arise;
- Oversee the development of and manage a citywide cyber security training program.

The position's responsibilities include commitment to and compliance with the City's EEO policy.

### Minimum Qualification Requirements

1. A master's degree in computer science from an accredited college and three years of progressively more responsible, full-time, satisfactory experience using information technology in computer applications programming, systems programming, computer systems development, data telecommunications, database administration, planning of data/information processing, user services, or area networks at least 18 months of this experience must have been in an administrative, managerial or executive capacity in the areas of computer applications programming, systems programming, computer systems development, data telecommunications, data base administration, or planning of data processing or in the supervision of staff performing these duties;  
or
2. A baccalaureate degree from an accredited college and four years of experience as described in "1" above;  
or
3. A four-year high school diploma or its educational equivalent approved by a State's department of education or recognized accrediting organization and six years of experience as described in "1" above;  
or
4. A satisfactory combination of education and experience equivalent to "1", "2" or "3" above. However, all candidates must have at least a four-year high school diploma or its educational equivalent approved by a State's department of education or recognized accrediting organization and must possess at least three years of experience as described in "1" above, including the 18 months of administrative, managerial, executive or supervisory experience as described in "1" above.

NOTE: The following types of experience are not acceptable: superficial use of preprogrammed software without complex programming, design, implementation or management of the product; use of word processing packages; use of a hand held calculator; primarily the entering or updating of data in a system; the operation of data processing hardware or consoles.

### Preferred Skills

We are looking for candidates who not only have the required experience and skills, but can demonstrate a high level of professionalism and customer service. If you are an IT professional who combines high business acumen with technical expertise and team collaboration, you are strongly encouraged to apply. Our ideal candidate possesses the following experience and skills:

- Five years of executive level experience overseeing IT security at a large corporation or institution;
- Competent management skills overseeing a highly technical staff of employees and consultants;
- Experience briefing executive level stakeholders on complicated security issues;
- Ability to navigate and collaborate among numerous stakeholders, including City agencies, State and Federal agencies, and private sector partners;
- A broad knowledge of information technology, including networking, data center, cloud, SCADA systems and some exposure to application and systems development;
- A good working knowledge of information security tools, procedures and best practices;
- Education - The incumbent should have a BA or BS in one of the following fields of study: Computer Science, Information Security, Management Information Systems, or Computer Information Systems;
- Professional Certification - Professional certification is not required for this position, however, industry recognized certifications such as CISSP, CNA or CISA, are desirable;
- This position requires strong written and oral communication skills as the incumbent will be required to summarize the results of their work, comments and recommendations in written reports, and also in presentations to City executives.

### To Apply

For City employees, please go to Employee Self Service (ESS), click on Recruiting Activities > Careers, and search for Job ID #221905  
For all other applicants, please go to [www.nyc.gov/jobs/search](http://www.nyc.gov/jobs/search) and search for Job ID #221905

-or-

If you do not have access to a computer, please mail resume indicating Job ID # to:  
Department of Information Technology and Telecommunications (DoITT)  
Recruitment Office - 255 Greenwich Street - 9th Floor - New York, NY 10007

SUBMISSION OF A RESUME IS NOT A GUARANTEE THAT YOU WILL RECEIVE AN INTERVIEW  
APPOINTMENTS ARE SUBJECT TO OVERSIGHT

**Posting Date:** November 6, 2015

**Post Until:** Filled

The Department of Information Technology & Telecommunications and the City of New York are equal opportunity employers.