DEPARTMENT OF INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS TESTIMONY
BEFORE THE NEW YORK CITY COUNCIL COMMITTEE ON TECHNOLOGY
RE: INTRO. 664-11 – PERSONAL INFORMATION SECURITY
THURSDAY, JANUARY 19, 2012

Good morning Chair Cabrera and members of the Council Committee on Technology. My name is Daniel Srebnick, Associate Commissioner for IT Security at the Department of Information Technology and Telecommunications, or DoITT, and New York City's Chief Information Security Officer. Thank you for the opportunity to testify today on Introduction 664, in relation to the security of personal information.

With the maturing of the digital age and the explosion of attendant data, the management of citywide information security is as important as any of DoITT's responsibilities. Accordingly, we have crafted citywide information security policies and standards that are as strong and dynamic as the city we serve. Pursuant to the New York City Charter, DoITT is empowered to plan, formulate, coordinate and advance information technology, which includes ensuring the security for data and other information stored in the City's IT infrastructure, i.e., the data centers, networks, and web portals that support critical City agency functions.

In 2006, DoITT assumed primary responsibility for review of and, as necessary, the promulgation of new policies and standards to ensure the confidentiality, integrity and controlled accessibility of all electronic information processed through the City of New York. DoITT also assumed primary responsibility for information security auditing – to assist agencies in minimizing internal exposures that could compromise sensitive data, disrupt agency operations, cause liability, or diminish public trust.

In 2010, this role was further reinforced by Executive Order 140, which empowered DoITT to establish and enforce citywide IT policies and for ensuring that such policies are aligned with the City's business needs and investments, as well as the individual business needs of each agency. Included in this authority is the provision of Citywide Information Security Polices and Standards, a collection of directives which together provide the basis for the City's IT Security governance.

Pursuant to this authority, DoITT's IT Security division ensures the overall security of the City's data and information technology assets. Security services are centrally-managed by DoITT for use by City agencies, including perimeter firewalls, intrusion detection, an industry-standard, three-tier hosting model for Internet applications with layered security and citywide malware/spyware protection. And we work constantly to build a consciousness about information security matters by issuing a regular Citywide Information Security Awareness Newsletter to all City employees, on topics ranging from identify theft to protecting portable devices, and from rogue anti-virus software to security and privacy on social networking sites. These, as well as a comprehensive listing of the all citywide information security policies and the appropriate DoITT contacts for IT security issues of all types are available through Cityshare, the City's employee intranet portal.

DoITT's work has led to New York City being viewed as a municipal leader in the information security field. In 2009, New York was the first city in the country to participate in the Department of Homeland Security's biennial "Cyber Storm" exercise series, which simulates large-scale cyber events and attacks on the government and the nation's critical infrastructure and key resources – so that collective cyber preparedness and response capabilities can be measured against realistic and credible national-level events.

More recently, the Information Security Executive program, which holds annual awards to recognize information security directors and teams who demonstrate outstanding leadership in IT Security management, recognized DoITT IT's Security Team for its work with McAfee to deploy an integrated network, host, and cloud solution, and leverage threat analytics to support 180,000 users from 52 City agencies.

As result of these and other efforts, for more than a decade now there have been no reported breaches of DoITT managed infrastructure, or on any applications where security accreditation has been successfully completed.

As successful as we've been, there is always the opportunity to further improve upon the job we do – and in an area as vital as IT security, it is imperative to do so. Because the thrust of Intro. 664 would help codify in local law much of what our Citywide Information Security Polices and Standards already requires of agencies, we welcome the opportunity to discuss with the Council how the bill can be crafted to ensure it meets these goals, as well as the high standards New Yorkers expect and deserve when entrusting the City with their personal information.

While we support the spirit of Intro. 664 and the emphasis it places on comprehensive citywide information security, the proposal will, however, require further examination in some areas to assure feasibility of implementation and standardization across City agencies. I will outline some of these considerations as follows.

The bill as currently drafted would require each agency to develop, implement, and maintain a comprehensive security program for their systems of records containing personal information. Better, we believe, to have the City – through DoITT – continue to review existing and promulgate new citywide information security polices and standards, with certain baseline criteria, which can be applied to all agencies. This approach, as is the current practice, would of course still allow agencies that opt for additional security measures to implement them as appropriate, while avoiding the duplicative effort and unnecessary expense that would accompany an agency-by agency mandate.

Next, the bill as currently drafted places substantial – and appropriate – focus on securing the files, records, and systems in and on which personal information is stored. But information security can be compromised through application flaws as well as infrastructural flaws, so it is as important to secure the digital and paper-based records that applications draw data from and run upon, as it is to secure the applications themselves.

Application security is addressed today by way of DoITT's Security Accreditation Process, which is required of all applications that are either multiagency or public facing in nature. The process is designed to determine whether the data contained within the system has been appropriately classified, and whether the system itself has been constructed with security controls appropriate to that data classification. The process also includes automated scans that check the hosting platform and the application for security vulnerabilities that could be leveraged to steal or change data. Moreover, as part of the accreditation process, DoITT confirms that all private data is appropriately protected by encryption and access controls.

In 2011, for instance, 25 major applications were accredited through our accreditation process. These include major citywide initiatives such as eHire, the September 11th Tenth Anniversary Website, and the first accreditation of an externally-hosted cloud application, the Department of Transportation's Feedback Portal. Additionally, more than 1,500 vulnerabilities that could have led to the compromise of private data were uncovered last year, and remediated before the applications went live.

Finally, the bill as currently drafted requires employing some fairly specific user authentication protocols, which if codified in law could unintentionally prevent the City from implementing the latest tools and security measures. As technology continues to advance, passwords, for instance, may no longer be the primary means by which user access is controlled several years hence. It would be preferable, therefore, to legislate the establishment of and compliance with an overarching identity management program, which would have the flexibility necessary to keep pace with coming technological advancements.

These are but a few topics for further discussion in a bill otherwise rightly aimed at addressing a constant imperative of the digital world: information security. By not confining the City to the parameters of specific technological tools, but rather acknowledging its need – within a standard framework of current best practices – to develop policies nimble enough for all agencies to adapt to the ever-evolving and sophisticated means of technological attack, we can pursue a considered approach to ensuring the continued privacy and security of all New Yorkers. We look forward to working with you in that regard.

This concludes my prepared testimony, and I will now be pleased to address any questions.

Thank you.

THE COUNCIL
THE CITY OF NEW YORK

Appearance Card

I intend to appear and speak on Int. No. 664 Res. No. _____

☑ in favor ☐ in opposition

Date: 1/19/11

(PLEASE PRINT)

Name: DANIEL L. SLEBNICK

Address: 2 METROTECH CENTER BKLYN NY

I represent: DOITT

Address: SAME

Please complete this card and return to the Sergeant-at-Arms