Department of Information Technology and Telecommunications
Testimony before the City Council Committee on Technology in Government
Oversight Hearing on Data Security and Privacy – Protecting Personal Information
Wednesday, December 13, 2006

Good afternoon Chair Brewer and members of the City Council Committee on Technology in Government. My name is Paul Cosgrave, and I am Commissioner of the Department of Information Technology and Telecommunications, or DoITT, and the New York City CIO. Thank you for the opportunity to testify today regarding the subjects of Citywide Data Security and Privacy, and some of our current initiatives to enhance the ways we protect the City's electronic information, and that of its clients. Joining me today is Daniel Srebnick, DoITT's Associate Commissioner for Citywide IT Security and Chief Information Security Officer. The responsibility for establishing and overseeing the City's IT Security Policies, as I will soon describe, has been recently transferred to DoITT, and Dan is the person now responsible for that function.

The related topics of IT privacy and security, for an entity the size of New York City, are understandably complex and multi-faceted. As technology becomes more commonplace, and we utilize the Internet to reach more people and facilitate their basic interactions with the City, these topics take on even greater importance. Accordingly, the City is embarking upon a series of initiatives to ensure that the security, reliability, and availability of data in its manifold systems are second-to-none, and that we are protecting the privacy of our constituents to the greatest extent possible.

I would like to speak today about my background in IT privacy and security, discuss some of the citywide measures being undertaken to enhance the City's efforts in these areas, and detail some significant accomplishments in this regard.

While I am relatively new to the Bloomberg Administration, I am quite mindful of the importance of strong privacy policies and top-notch systems security, having had significant practical experience in the area. From 1998 to 2001, I served as CIO at the Internal Revenue Service, an organization responsible for collecting over $2 trillion per year for the federal government. I need not emphasize the importance of privacy and security for an organization with such reach and impact. Furthermore, we were charged by Congress to expand the percentage of our electronic transactions to at least 80% by 2007, a program I set in motion during my tenure.

While at the IRS, I also led a major restructuring and centralization of information systems, and put in place the technology and policies enabling us to become an organization that, literally, ran on the Internet. I worked on designing a multi-billion dollar strategic modernization program aimed at improving core processing capabilities, streamlining operations, and introducing a number of new e-commerce services to taxpayers. Finally, I created a new "Privacy Advocate" position, and significantly expanded our IT Security organization.

As you can imagine, implementing these new systems, policies and procedures, and effecting these changes for an organization of 100,000 people provided me with valuable insights for the challenges now before us in New York City.

The management of electronic data can effectively be described as the interplay between privacy and security. Privacy is the setting of rules about what needs to happen with the data over which the City has stewardship; security consists of putting the appropriate technologies in place to make that policy possible. I would like to start this discussion by describing, in general, some of the policies and practices we already have in place.

Mayor Bloomberg has made it clear that he wants his legacy to be a City government that is transparent, accountable and accessible to its residents, businesses, visitors and employees. Two cornerstones of that legacy are the 311 Citizen Service Center and *NYC.gov*. Both provide a simple, direct means by which our constituents can reach the government that serves them, and we, in exchange, have a responsibility to protect their personal information on these media.

The confidentiality of callers to 3-1-1 is safeguarded by the 3-1-1 Client Information Privacy Policy. This policy consists of principles and procedures relating to the personal information of callers—how it is to be collected, how long it is to be retained, and how clients may access that information upon request. Generally speaking, 3-1-1 limits the collection of personal information only to those instances where necessary to address callers' needs, conduct and improve City services, provide emergency assistance, or as required by law. When 3-1-1 does collect personal information, its disclosure is also limited to the instances I just described. Of course, personal information collected by 3-1-1 is never sold to third parties for marketing purposes.

The privacy policy was established to ensure that 3-1-1 callers may expect a certain level of privacy regarding the information they convey when making a complaint. DoITT is quite mindful of the consequences of personal information being inadequately protected—not only could it discourage citizens from making complaints, but it may also provoke retaliation against the constituents filing them.

To ensure client confidentiality, 3-1-1 provides a Service Request number each time a caller lodges a request to be tracked and addressed by a particular City agency. This number can be used by the caller to later retrieve a record of their call. Individuals cannot access information related to calls without providing a Service Request number, except by operation of law, i.e., a court order. In addition, 3-1-1 Call Center Representatives are trained on the privacy policy, and are subject to disciplinary action should they fail to adhere to it.

We also protect personal information at 3-1-1 by limiting its retention. For instance, voice recordings of calls are kept for 14 days, and then erased. Exceptions to this rule include calls kept for quality assurance purposes (in which case personal information is redacted), calls subject to subpoenas or Freedom of Information Law requests, or calls material to an ongoing law enforcement investigation.

DoITT's other interactive, public-facing enterprise is *NYC.gov*, the City's official website. When visiting *NYC.gov*, certain information is automatically collected about the user, including the Internet Service Provider's IP address and domain name, type of browser, date and time of visit, and the pages viewed while on the site. The City uses this information to identify site performance needs, ensure the compatibility with the technology used by visitors, and to generally add and improve services offered. As is the case with 3-1-1, this data is never collected, sold, or otherwise distributed for commercial or marketing purposes.

Visitors to *NYC.gov* may affirmatively submit information to the City via online forms or by registering to receive emails about City-specific news, services, and information. All such information is stored in a secure environment, and is used by the City only to meet its duties and obligations to constituents. The City does not sell any personally identifiable information, and does not disclose credit card or other personal financial information except as necessary to complete the transaction for which it was submitted. In certain instances, a user may have the opportunity to use a password to obtain or submit personally identifiable information—ACCESS NYC, which I will discuss later, is an example of this. The City will never ask a user for a password in a telephone call, fax, email or any other form of unsolicited communication.

We have integrated industry-standard or better security measures and systems into the design, implementation, and day-to-day operation of *NYC.gov*, and its underlying servers and networks. Furthermore, we maintain ongoing efforts to identify and/or block unauthorized intrusions, and any attempts to upload, change, or otherwise cause damage to *NYC.gov* or the information provided on or submitted to it.

None of this is to suggest that we cannot still improve, as IT privacy measures are constantly evolving. DoITT is currently examining additional ways to limit the retention of personal information, and will continue to explore ways to improve upon existing polices as the City expands the services it offers the public.

I would like to shift the focus now from privacy to security. We have set out to enhance the City's IT security posture to consolidate and centralize certain enterprise-wide roles, pursuant to DoITT's mandate to oversee the use of existing and emerging technologies in government operations, and its delivery of services to the public. Specifically, DoITT has recently assumed primary responsibility for reviewing security procedures and standards, and, as appropriate, for developing new security procedures and standards to ensure the confidentiality, integrity, and controlled accessibility of electronic information processed through the City of New York.

DoITT will also be assisting City agencies in reviewing their IT resources to assess compliance with Citywide Information Security Standards and Directives. This role includes working with agencies to review their IT plans to ensure adequate controls; collaboration with City agencies to determine citywide technology infrastructure protections; and the coordination of actions to eradicate potential technological attacks against the City. In concert with the Mayor's Office of Operations, we are now at the beginning of an information-gathering process to highlight how each agency is reporting on citywide goals and initiatives. IT privacy and security measures will be high on the list of metrics we will be tracking.

We have also taken steps to ensure that the progress we make in this effort is institutionalized in the consciousness of City government. Since my appointment, DoITT has embarked upon development and implementation of a Citywide IT Strategy, or an overall approach for leveraging technology to accomplish the City's business goals and objectives. Figuring prominently in that strategy, of course, are the topics of privacy and security. We will measure our success by surveying the City's constituents and employees, to ensure their confidence in our ability to protect their personal data and information.

To support the City's IT Strategic Direction, a new citywide IT governance structure has been developed. The Technology Steering Committee, or TSC—composed of Deputy Mayors with operational responsibilities and representatives from the Offices of Operations, Management and Budget, and DoITT—is the decision-making authority for implementing and monitoring key citywide IT initiatives. Three advisory councils have been established under the TSC: an Executive CIO Council, a Portfolio Management Advisory Council, and an Enterprise Architecture Committee.

As an example of how these committees are working, the Executive CIO Council last week agreed on a new Password Identification Policy. This policy is the first step in a much broader initiative to authenticate all citywide employees, contractors, and other users of our systems with one consistent method. The first phase will entail rolling this policy out to all users of DoITT's systems, then to all City employees, and finally expanding to the individuals who access our systems from outside the City. This last phase will be critical to informing how we manage privacy and ensure security for all our constituents.

Responsible for facilitating inter-agency IT collaboration and communication, the Executive CIO Council approaches technology issues from a citywide perspective. Part of the council is the IT Security/Identity Management Subcommittee, consisting of agency Chief Information Security Officers. This subcommittee is charged with reviewing the City's IT security policies, establishing processes to support agency compliance with these policies, and developing a citywide strategy for identity management, including the use of digital and electronic signatures.

While the security changes I have just described are largely new initiatives, I would now like to discuss some of the ways the City, and DoITT, have already been contributing to the enhancement of IT privacy and security.

The City's wide area network, known as *CityNet*, is monitored 24/7/365 through a security operations vendor, and has intrusion detection sensors at critical points within its infrastructure. Should any anomalies requiring immediate attention be detected, there is an escalation procedure followed, with the citywide IT HelpDesk as the first point of contact. There are also systems deployed, monitored by DoITT staff, which model network traffic and seek out any patterns dissimilar from what is normally expected. Work orders, or what we call "trouble tickets," are opened based upon observations of these systems, and DoITT Security and HelpDesk staff work with agency personnel to resolve problems as they arise.

As you know, DoITT has also pioneered the development of citywide contracts, enabling the City to leverage its considerable size and purchasing power to ensure significant cost savings for goods and services. Among the citywide contracts DoITT has recently established are those specifically focused on IT security services. Available to any City agency, these contracts are divided into three classes of service: Response and Restoration Services; Assessment, Planning, Design and Implementation Services; and Ongoing Managed Security Services.

The Response and Restoration Services class was established to provide onsite and/or remote response, remediation and restoration services when an adverse situation exists—for instance, if systems are compromised as a result of a malicious attack. The contract provides for rapid restoration of client devices, LAN/WAN environments, and both custom-developed and commercial applications.

The Assessment, Planning, Design and Implementation Services class, the broadest of the three, is intended to help City agencies plan and implement IT security in their own organizations. Assessment services include evaluating technical environments and applications for security risks, determining the level of vulnerability, and providing recommendations—and actual fixes—for weaknesses discovered. Planning services include developing security strategies and policies for wired and wireless infrastructure, software, applications and data. Design services include wired and wireless infrastructure, software applications, and identity management; and implementation services include validating, procuring, installing, configuring, testing, and documenting security solutions.

The Ongoing Managed Security Services class covers subscription-based services for ongoing monitoring, maintenance, and enhancement of *CityNet* security on a 24/7/365 basis—including intrusion detection, prevention, management, and monitoring services, and regular electronic verification of the Internet security profile.

Finally, I would like to detail two of the City's most recent IT initiatives, and the privacy and security considerations inherent in both.

The first is ACCESS NYC. Under the leadership of Deputy Mayor Linda Gibbs, we have worked for the past year to take related information from the universe of health and human service programs available to New Yorkers and bring it together in an intuitive, user-friendly way. ACCESS NYC takes a transformative, client-centered approach to explaining the many services offered, and allows New Yorkers most in need to pre-screen—anonymously if they like—for their eligibility for programs offered by more than 20 different City, state and federal programs, in any of seven different languages.

Obviously, protecting the personal information of New Yorkers using ACCESS NYC was of paramount concern from the start. Security in ACCESS NYC is controlled via numerous security features, as well as custom code to ensure the data and privacy of users is maintained at all times. Function Level Security is used extensively throughout the system, to ensure users can only access those pages for which they are authorized.

The second project is the Citywide Mobile Wireless Network, or CMWN, which will be operational throughout lower Manhattan by January, and implemented throughout the five boroughs over the next 18 months. When complete, this network will represent an historic enhancement to public safety communications in New York City.

The CMWN will give first responders from the Police and Fire Departments high-speed data access to support large file transfers, fingerprints, mug shots, city maps, and full-motion, streaming video. The CMWN will also support a host of other public service applications that will provide a significant improvement over existing technologies, by enabling data transfer rates 50 times faster than what we are using today. We testified before you regarding the CMWN last month, and Council Members Brewer and Vallone, along with members of the Council staff, have toured the system's Network Operating Center (NOC). The invitation remains open for the Council to tour the NOC at their convenience.

Due to the mobile, open nature of wireless technology, this next-generation public safety network—the first of its kind in the country—was imbued from its initial conception, through the design and piloting processes, and now in its implementation, with a significant focus on the security of the data to be transmitted over it. The vendor is now building the network in compliance with Citywide Information Security Policy, Directives, and Standards, to ensure the system is protected from misuse and provides a safe and secure operational environment.

There are three main security objectives that drive our work on the system:

- Authentication, as previously discussed;
- System Monitoring and Intrusion Detection, which is critical to protecting any network environment; and
- Encryption, or a higher-level security protocol applicable to this level of data transfer.

For security reasons, I will not be discussing the specific techniques we are using for each of these projects, but you may rest assured we are employing state-of-the-art measures to ensure the integrity of the data processed in ACCESS NYC, and transmitted via the Citywide Mobile Wireless Network.

In sum, New York City has made a substantial commitment to protecting the privacy of its constituents by making many improvements in IT security over the course of the Bloomberg Administration, and will continue with these enhancements through the series of initiatives I described above. By consolidating citywide IT security policy-making, establishing an auditing practice with agencies to analyze successes and diagnose potential issues, and working to instill these practices into the common administration of City government, we are confident these improvements will endure throughout this Administration and beyond, to the benefit of New Yorkers and the agencies that serve them. As always, we welcome your feedback and comments, and would now be pleased to address any questions you have.

Thank you.