DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS TESTIMONY
BEFORE THE NEW YORK CITY COUNCIL COMMITTEE ON TECHNOLOGY
RE: INTRO. 626-2015 / PERSONAL INFORMATION SECURITY &
INTRO. 1052-2016 / CITY AGENCY ELECTRONICS DISPOSAL
MONDAY, FEBRUARY 1, 2016

Good afternoon Chair Vacca and members of the Council Committee on Technology. My name is Anne Roest, New York City Chief Information Officer and Commissioner of the Department of Information Technology and Telecommunications, or DoITT. Thank you for the opportunity to testify today on Intro. 626, in relation to the security of personal information; and Intro. 1052, in relation to the disposal of electronics for City agencies. Taken together, these bills aim at addressing a constant imperative of the digital world – information security – and I thank the Committee for its focus on such a vital area of City operations. I am joined today by Mindy Tarlow, Director of the Mayor's Office of Operations, who will speak to Intro. 627.

In a connected city our IT security posture is only as good as the weakest link, and a weak link successfully exploited in one agency can have significant consequences on other agencies – and on the lives of the New Yorkers they serve. Accordingly, DoITT maintains and promulgates a range of Citywide Information Security Policies and Standards as strong and dynamic as the city we serve, to which every agency must adhere.

Our robust IT Security Division also manages the overall security of the City's shared data and information technology assets through the management of an integrated security network, consolidating desktop and server security on a single, citywide platform. DoITT also maintains email, intrusion prevention systems, next generation firewall protection, and security monitoring. In this way, New York City maintains the ability to keep pace with rapidly-evolving threats by centrally implementing and enforcing citywide policies and standards – with the ability to update them dynamically.

There is always the opportunity to further improve upon the job we do – and in an area as vital as IT security, it is essential to do so. New York City is an incredibly inviting target for our cyber adversaries the world over, and these parties are constantly developing new and increasingly complex means of attack. The City, in turn, must have the ability to keep pace with these rapidly-evolving threats by centrally implementing and enforcing citywide policies and standards, and by continuing to update them as necessary.

To that end, the de Blasio Administration has been aggressive and progressive in its support of a strong cyber security program. Since the start of the Administration we have increased our security headcount and invested tens of millions of additional dollars in new training and technologies to improve our security posture and to keep pace with the ever-evolving threat landscape.

Together these measures reflect the great emphasis we place on protecting the security of New Yorkers' information against the many thousands of daily attempts to improperly access City systems and data. The spirit and aim of **Intro. 626** align with these efforts, and with the high standards New Yorkers expect and deserve when entrusting the City with their personal information. I very much appreciated the opportunity to discuss with the Council last week my concerns on the bill as drafted, and look forward to continuing our dialogue about the City's cyber security program. Our interest, and the Council's, in protecting sensitive information could not be more closely aligned.

Next, **Intro. 1052**, would require City agencies to ensure erasure of all information when disposing of electronics. The City recognizes the importance of such a practice, and our Citywide Information Security Policy on Digital Media Re-use and Disposal, established in 2011, requires that all digital media undergo a data sanitization process prior to disposal, or reuse, to protect against unauthorized access to information. Not only is this a policy to which all City employees must adhere, but it is also one that any vendor handling any of our equipment must adhere to as well. We will continue updating this policy as new electronic tools become available, and are happy to keep the Council apprised of our progress.

I appreciate the opportunity to testify today. And I thank the Council for highlighting the vital issue of information security. By developing policies nimble enough to adapt to the ever-evolving and sophisticated means of technological attack, within a centralized framework of current best practices, we can continue successfully protecting the information of New Yorkers.

I look forward to working with you.

Thank you.