

**OFFICE OF TECHNOLOGY AND INNOVATION TESTIMONY BEFORE THE NEW
YORK CITY COUNCIL COMMITTEE OF THE WHOLE**

October 5, 2026

Good morning, Speaker Menin, Chair De La Rosa, and Council Members. My name is Sarah Milstein and I am the Deputy Commissioner for Strategic Advisory Services for the Office of Technology and Innovation (OTI). I am joined here today by my colleague, CJ Dixon, OTI's Deputy Commissioner of NYC Cyber Command and New York City's Chief Information Security Officer. I am also joined by Samuel Levine, Commissioner of the Department of Consumer Affairs and Worker Protection (DCWP), Carlos Ortiz, DCWP's Chief of Staff and Deputy Commissioner of External Affairs, and Benjamin Krakauer, First Deputy Commissioner for NYC Emergency Management (NYCEM).

In my role at OTI, I oversee both the Office of Algorithmic Accountability (OAA) and NYC Cyber Command. We appreciate that the Council is holding this timely hearing about the risks of AI technology. Thank you, Speaker, for getting representatives of the companies that develop, deploy, and sell AI tools to the general public to speak to the capabilities, limits, and risks associated with these systems, at this hearing. As a representative of OTI, I am here today to provide information to the Committee of the Whole about how we serve the City's technology and cyber-defense needs, and to address the proposed legislation that potentially impacts the administration.

For those unfamiliar with our work, OTI's core mission is to use technology, data and design to make the City work better for New Yorkers. We achieve this through a wide range of digital products, infrastructure, data systems, and shared expertise. In other words, we use technology to help agencies make every New Yorker's experience of City government better. For our discussion today, we can speak to the work we're doing around agency use of algorithmic tools, and our cybersecurity program.

To touch briefly on the AI arm of OTI, I'm pleased to share that the Office of Algorithmic Accountability (OAA) has been formally established and six new positions have been created in the FY27 Adopted Budget to staff it up. The hiring process for those roles is actively underway. The OAA's duties include:

- Analyzing algorithmic tools submitted by agencies to determine whether there is risk that the proposed tool could result in discriminatory decision-making;
- Conducting and publicly reporting on pre-deployment assessments;
- Creating and maintaining a public-facing platform for submission of comments;
- Establishing a protocol with the Department of Investigation for receiving complaints from the public;
- Promulgating rules establishing basic compliance standards that all agencies must meet in developing, procuring, deploying, and using public-impacting artificial intelligence; and

- Reporting the results of pre-deployment assessments and audits conducted by the Office.

Overall, the Office is progressing as planned, and we remain focused on building the capacity needed to carry out this work effectively.

I will now turn to the legislation on today's docket that would impact OTI.

Introduction 161-2026 would amend annual reporting on algorithmic tools to include their impact on city employment, with a focus on potential changes to funded agency positions, salaries, and duties. OTI is currently undertaking a study on the impact of algorithmic tools on municipal employees pursuant to Local Law 25 of 2026. This study will provide insights into the extent to which algorithmic tools, including artificial intelligence, impact city employees and the administration of their duties, including their hiring and work functions. While we agree that it is important to examine the impact of AI on our workforce, the bill as written would not produce new insights beyond those in the larger, more expansive directive of Local Law 25.

The next three bills involve New York City Cyber Command. This office plays a vital role in protecting and defending the City and its residents from the impacts of cyber attacks. On a day-to-day basis, we provide 24/7 security services and assist agencies in bolstering their cyber maturity. We work collaboratively with agency partners, as well as state, federal, and private entities, to safeguard the essential services and data that New Yorkers depend upon daily.

Our core mission is to make New York City the most cyber resilient city in the world, and we take this extremely seriously. NYC is a target for cyber attacks with a technology landscape that is unparalleled among other cities and states. This requires a unified, comprehensive defense against constant cyber threats. Our key duties include:

- Setting information security policies and standards for the City
- Directing the City's citywide cyber defense and incident response
- Deploying defensive technical and administrative controls; and
- Providing guidance to City Hall and agencies on cyber defense.

In my fairly new role at OTI, it is a privilege to work with our staff and our agency partners in furtherance of this critical mission. New York City Cyber Command's alignment within OTI has placed the team in a strong position to monitor and respond to wide-ranging cyber threats.

Cybersecurity is continuous work. In my role, I'm confident we can continue to adapt to a constantly evolving threat landscape. Simply put, New York City Cyber Command has a 24/7 apparatus in place to defend the City's systems from malicious attacks – regardless of the origin.

With that in mind, **Preconsidered Introduction T2026-2602** would make it unlawful to market, offer for sale, sell, or deploy an artificial intelligence (AI) model in New York City that has not received third-party validation or does not have a technical capability to be shut down by a

human operator. The bill would require the director of the Office of Cyber Command to promulgate rules regarding what the third-party validation, assessments, certifications and disclosure would entail, and the qualifications for third-party validators.

To be clear, Cyber Command's core mission is to defend the City of New York's infrastructure from cyber attacks. We are not subject matter experts on the qualifications for an entity to be considered a third-party validator. Further, neither OTI nor Cyber Command have experience regulating the private sector in the way that this legislation would require and neither would be the best choice to lead this regulatory regime for consumer products. We defer to DCWP to speak about the private sector policy and enforcement piece.

To that end, DCWP supports the intent of this legislation. They recommend including robust record keeping requirements to better allow the agency to conduct affirmative enforcement. They also note based on conversations with advocates and sister agencies, that the administration is not certain about the availability or ability of such businesses. We look forward to hearing from those stakeholders today including on whether initiatives like this one could help spur a market for such services.

Preconsidered Introduction T2026-2601 would require the Office of Cyber Command to establish standards and procedures for contractors to identify the occurrence of a reportable AI safety incident. To take a step back, I'd like to lay out how AI Risk and Incidents are categorized according to National Institute for Standards and Technology (NIST):

- **AI-Under-Attack (AI Cybersecurity Incidents)** are traditional cybersecurity compromises where the AI system is the target (for example, data poisoning or jailbreaks).
- **Misuse or Malfunction (AI-Induced Incidents)** would be harms resulting from the use or failure of AI aside from a cyber compromise. In this category, the AI system itself behaves exactly as it was built or trained, but the real-world outcome causes harm. These incidents are not cyber attacks.

We understand the Council's intent here, given the publicized instances of AI systems operating outside the bounds of their intended use. As I noted earlier, the risk landscape is constantly evolving, and we are continuing to evolve our strategies to keep the City's infrastructure safe. But not all threats related to AI systems are necessarily cyber attacks – and the legislation as written does not address that. Cyber Command would be a critical stakeholder in this discussion, but it is important to emphasize that we need to work with our state and federal partners to address these issues holistically.

I also want to provide further context on breaches of security generally. Agency disclosure of a breach of security – in any form – is governed by § 10-502 of the administrative code. There are extensive protocols for interagency coordination in the event of any breach of security. These

protocols are aligned with the New York State “Stop Hacks and Improve Electronic Data Security” (SHIELD) Act. Current law, policies, and protocols are in place for incidents described in this legislation. Further, the threshold of 24-hour public notice is inconsistent with current law and would compromise the City’s investigation of a cyber-incident.

Preconsidered Introduction T2026-2606 would require the Office of Cyber Command, in coordination with NYCEM, to develop or update an emergency response plan concerning AI system-related threats to NYC’s infrastructure, operations, public health and welfare. I’d once again like to emphasize that there are laws, policies, and protocols in place for breaches in security, regardless of actor. However, we are happy to discuss more broadly with Council how we already coordinate with NYCEM to coordinate and engage with partners to restore services.

Finally, I will provide DCWP’s feedback on the remaining legislation that would impact the administration.

Preconsidered T2026-2605 would allow any person to submit a complaint to DCWP alleging that a person or entity has violated certain provisions of law related to artificial intelligence. DCWP strongly supports the intent of this bill to establish a civilian enforcement structure for AI violations, especially given widespread reporting that concerns being raised by AI companies’ employees are being ignored. However, there are fiscal and operational concerns with the volume of complaints that the agency would receive, and the resources and expertise required to handle each individual complaint. Therefore, the administration believes it would be important to coordinate closely with mission-aligned enforcement agencies at the state level. The NYS Attorney General just recently announced its secure whistleblower portal for New Yorkers to report unsafe and illegal conduct related to AI technology. This could be an opportunity to partner on this existing program to more effectively enforce complaints on behalf of New Yorkers.

Preconsidered T2026-2599 would impose requirements and restrictions on companies that provide chatbots, including requirements related to data security and privacy, the right of chatbot users to access their own data, and restrictions on how chatbot providers can use chatbot user data. DCWP has concerns about this bill. While we support Council’s goal to better regulate company’s deployment of AI chatbots, and believe the approach taken by this bill is sound, the implementation and enforcement of this bill’s data security and privacy requirements would require a deep technical understanding and investigative ability that is outside of the agency’s scope. To be clear, DCWP is committed to regulating harmful practices, including relating to chatbots, that fall within the agency’s investigative ability. To that end, the administration is working on rules related to the use of AI chatbots to better regulate this space for consumers. The Administration is also invested in supporting the New York Attorney General in their efforts to rein in data abuses, for which this bill may serve as a model.

Preconsidered T2026-2603 would require any advertisement that promotes an artificial intelligence (“AI”) model in the City to disclose whether such model has undergone validation

by a third-party. It also would prohibit any such advertisement from including any materially false or misleading statement regarding the safety of an AI model. DCWP supports this bill to require disclosure of third-party validation on any advertisement of an AI model. However, as mentioned above, the administration is not certain about the availability or abilities of such businesses. And, we want to be clear that any advertising that uses false or misleading statements is currently prohibited under the City's Consumer Protection Law, and will be enforced with the full scope of DCWP's authority. We look forward to working with Council to ensure the law includes effective enforcement mechanisms, and to continue addressing issues within DCWP's scope of work as it relates to AI.

Thank you for your time. This panel will now take questions.

###

Additional testimony from the Administration below:

Intro 0504-2026 would permit elected officials and candidates for elected office to notify, in writing, owners of generative AI systems that they do not authorize those systems to produce manipulated audio, photos, or videos with their likeness. The administration supports the intent of this bill. The administration would like to discuss how best to accomplish its goals and we defer to our colleagues at the Law Department for further details.

Intro T2026-2600 would create a private right of action against companies that make artificial intelligence models available for commercial or public use when third parties cause harm by misuse or malicious use of artificial intelligence models. The administration supports holding companies accountable for harms they or their products cause, including through the use of private rights of action, and looks forward to further discussion.