CITY COUNCIL
CITY OF NEW YORK

---------- X

TRANSCRIPT OF THE MINUTES

Of the

COMMITTEE ON TECHNOLOGY

---------- X

DECEMBER 13, 2018
Start: 1:15 P.M.
Recess: 1:58 P.M.

HELD AT: COMMITTEE ROOM – CITY HALL

B E F O R E: PETER A. KOO

COUNCIL MEMBERS: ROBERT F. HOLDEN
BRAD S. LANDER
ERIC A. ULRICH
KALMAN YEGER

A P P E A R A N C E S (CONTINUED)

JEFF BROWN, New York City Chief Information Security and Head of Cybercommand

SARGEANT AT ARMS: Sound check for the Committee on Technology. Taking place Committee Room City Hall, scheduled for 1 p.m. uhm December 13, 2018, being recorded by Israel Martinez.

CHAIR PETER KOO: (gavel pounding). Good afternoon. I am Council Member Peter Koo. I am the chair of the Committee on Technology and I want to welcome all of you to our hearing. At today's hearing will focus on four Bills, Intro 1152, a local law in relation to requiring an online payment grace period in the event of an electronic system security breech. Intro 1153, a local law in relationship, in relation to be requiring a penetration testing protocol. Intro 1154, a local law in relation to encrypting website exchange or transfers and then lastly Intro 1297, a local law in relation to codifying an office of cyber command. Ensuring the security in Cyberspace to our promoting prosperity and protecting your City's critical infrastructure and the privacy of our residents. The internet has become an important component of all aspects of lives. The internet has changed businesses paths, education, Government, healthcare and even the ways in which we interact with each other. We now use the

internet to transfer of funds from bank accounts, check bus time tables, book car service, pay parking tickets, check weather and remote in regular room temperatures in our homes and even it to upload to get medications. All of this requires providing personal and private information and really to make sure that the information is secure. Therefore, both our critical infrastructures and our daily lives rely on computer driver interkinetic information technologies. It is the fact that in Cyberspaces new vulnerabilities have been revealed and new tracks continue to emerge. It is part of our mission to keep our Cyberspace safe and secure and these four Bills hope to accomplish just that. Okay. I look forward to hearing from the panels today and I would like to thank the Technology Committee Staff for putting together this hearing. I would like to recognize the Technology Committee Members which they are on the way and thank you and I look forward to hearing on the testimony on these Bills today and we have Mr. Jeff Brown, New York City Chief Information Security and Head of Cybercommand. Welcome to our Committee.

COUNSEL: Do you affirm to tell the truth, the whole truth and nothing but the truth and answer honestly to Committee questions?

JEFF BROWN: I do.

COUNSEL: Thank you.

CHAIR PETER KOO: Thank you. Okay.

COUNSEL: You can start.

CHAIR PETER KOO: Yeah, you can start now.

JEFF BROWN: Good afternoon, good afternoon Chair Koo and members of the Committee on Technology. My name is Jeff Brown and I am New York City's Chief Information Security Officer and Head of New York City Cybercommand. I am here today to speak with you about the important issue of Cybersecurity. Specifically, with respect to issues associated with the Committee's consideration of four distinct pieces of proposed Legislation. Intro 1152, Intro 1153, Intro 1154 and Intro 1297. At New York City Cybercommand we believe that thoughtful Legislation and regulation at the Federal, State and local levels plays a critical role to enhance our collective and increasingly interdependent Cybersecurity posture. This is our first time to appear before the Committee

and we see today as a welcome opportunity. Before we turn to the proposed Legislation, I would like to take a moment to provide some context on New York City Cybercommand and the perspective we offer today. I would be remiss if I did not mention at the onset the important work protecting the City from Cyber threats that pre-dates the creation of New York City Cybercommand. This work was performed by the Department of Information Technology and Telecommunications as well as Technology and Security Teams within the Agencies themselves. These teams continue today and are our strongest partners. Recognizing the importance of Cybersecurity to the City and its residents, visitors and businesses. The Mayor built a distinct standalone Cybersecurity function that would have the appropriate responsibilities and authorities to apply uniform consistent approach to Cybersecurity across all City Agencies including Do It as a core technology services Agency. Our planned foundation rested on the premise that it continued to be the world's leading City, New York must remain the safest and most security City. As a first step, we needed to establish a mechanism for the City to have a

Cybersecurity conversation as it appeared to be Technology conversation and with the Agencies delivering critical services each and every day to New Yorkers. In support of this effort, the Mayor signed Executive Order 28 on July 11, 2017. It is a concise but thorough document that sets for the intent, direction and authority of the City's unique approach to Cybersecurity with a clear mission to make New York City a Cyber secure place to live, visit and do business. Under the Executive Order, we are charged to undertake the following activities with regard to City-owned and managed systems, ensure compliance with information security policy and standards, mitigation Cyber threats and direct incident response, mandate deployment of technical and administrative controls, review Cyber-related spending and collaborate with Federal and State Government Agencies and private-sector organizations. In addition to Cybercommand specific mandates under the Executive Order I would also like to highlight just one example of how New York City Cybercommand help define the role of City Government in Cyberspace, the New York City Security Initiative. NYC Secure re-conventionalizes the role of the City

in Cyberspace under the principal that Cybersecurity is a public safety issue and an essential need of all New Yorkers and Cybersecurity for New Yorkers should protect and respect New Yorkers Privacy. I am proud to remind the Council that in support of the NYC Secure Initiative, New York City Cybercommand released a free mobile threat detection app. This App embodies our NYC Secure Principals. It reduced the risk of malicious activity when it is sought on mobile devices and it was built under the concept of Privacy by Design. We developed the App to ensure that privacy principals were embedded into the Apps code. Similarly, New York City Cybercommand is also working with the Agencies to deploy a privacy centric Wi-Fi Security Solution in the locations where the City provides free Wi-Fi. The creation of New York City Cybercommand was a critical step to protect our City and prepare in its future. It is a future in which New Yorkers expect our City to rapidly adapt to new ways in engaging in commerce and culture through technology and this future must be secure. The complexity of Cybersecurity coupled with the challenge of preparing to defend against future unknowns is daunting. This Committee knows that

Cyber threats have evolved and are evolving in concerning ways. Cyberthreats do not respect international boundaries. Cyberthreats do not respect national boundaries. Cyberthreats do not respect state boundaries and cyberthreats do not respect local boundaries and since the inception of New York City Cybercommand, we have routinely dealt with and are currently handing a variety of Cybersecurity matters related to the City Government Ecosystem. But I say with confidence that New York City is setting a new standard on how a City addresses these threats. We cannot eliminate cyberthreats but we can take decisive action to mitigate the risks that these threats will harm the ability of City Agencies to deliver critical services and we can respond quickly to minimize their impact if they do. Accordingly, today presents an opportunity to work together as a City on additional measures to assist our City's preparation. We welcome this and all opportunities to work with the Committee on thoughtful Legislation that will advance our shared objections for a safer City. We appreciate the overall objective of the proposed Legislation to enhance the Cybersecurity of our City.

I make the following brief observations with respect to each of the proposed Bills and will be delighted to discuss them further and in greater detail following the hearing today. Intro 1152, we agree with the premise that people should not incur late fees associated with a system outage. We will work with Council to identify the appropriate agencies that should also be a part of this discussion. Intro 1153, this proposed Legislation outlines four important Cybersecurity objectives. The first, NYC Cybercommand referred to as voting management. The second we will refer to it as education awareness. The third we would refer to as compliance and the fourth we would refer to as incident response reporting. While we will continue to support strengthening, education and awareness throughout the City's workforce we are concerned about certain aspects of the proposed Legislation, particularly the concept of an immediate reporting requirement during incident response. As currently written, the Bill would require us to divert resources from responding to an attack to brief the City Council in a matter outside of the traditional hearing and oversight processes outlined in the Charter and it may force

the public exposure of information that would make the City an easier target of Cyberattack. Intro 1154, website encryption is important and our partners at Do It have made significant progress toward this end. HTTPS has already been implemented on NYC.gov and we support the Committee in moving more City-maintained websites to HTTPS. Intro 1297, we support centralization of authority within City Government to manage Cyberthreats. Our organization with the authority to salvage technical controls with oversight ability and the resources to engage and educate across City-government is the most effective approach to address the Cyberthreats that we face. Executive Order 28 clearly defines the powers and duties of New York City Cybercommand, acknowledges the unique importance of Cybersecurity of critical infrastructure and underscores the need to organize around this important issue in a way that best protects all New Yorkers and the services that they rely on each day. Today's Committee hearing is a signal to New Yorkers that our Government is in firm agreement about the critical importance of Cybersecurity. It is a signal to New Yorkers that their government recognizes that partnership can

strengthen New York City and that New York City can set an example for others to follow. In the spirit of our shared responsibility to protect and defend the people of New York City I want to once more thank Chair Koo and the Committee on Technology for the opportunity to speak today and I welcome the discussion.

CHAIR PETER KOO: Thank you very much, Mr. Mr. uhm before we start questioning it should be one to acknowledge uhm our Committee Members who would just join us, Council Member Ulrich, Council Member Holden and Council Member Yeger. So, thank you for your testimony. Uhm first all, I want to congratulate you on your success in monitoring NYC Secure to have. I am sure that we all would like to learn more about your success in protecting New York City and our residents from Cyberattacks. So, uhm Executive Order 28 requires New York City Cybercommand to set Security Policies and Standards. How is the process going?

JEFF BROWN: Thank you for the question Chair Koo. The process is going quite well. I would reiterate to the Committee that the Department of Information Technology and Telecommunications

predating the creation of NYC Cybercommand has a standard of policies and associated standards for the security of IT systems. New York City Cybercommand has been working diligently with the Department of Information Technology Telecommunications and Agencies, learning from those Agencies, experiences with the existing policy has begun the process of rolling out new policies. Those new policies include incident response and others to come in coming months. Uhm these policies are meant to make sure that the authority of NYC Cybercommand to do things like deploy defenses and conduct incident response is in tight, tight coordination with the Agencies themselves and is also making sure that our City has the standards that are industry standard and industry leading to protect our systems from any type of Cyber event.

CHAIR PETER KOO: Thank you, can you put the mic a little bit closer to you.

JEFF BROWN: I'm sorry, yeah. Thanks. Better?

CHAIR PETER KOO: Yeah, yeah.

JEFF BROWN: Okay.

CHAIR PETER KOO: Yeah thank you. So, these policies tailor to a specific agency or uhm they are applied to all City Agencies?

JEFF BROWN: The policies are meant as an umbrella for all City Agencies. The policies are followed, will be followed by standards and are followed by standards that give more precise guidance on technical controls but I would like to highlight is agencies themselves have different functions and different technical environments so we are very, very mindful in working with the agencies to make sure that the umbrella applies appropriately and helps guide them into a better standard but then we need ot be mindful of the different technical environments and associate guidance to them on how to best to defend their individual systems.

CHAIR PETER KOO: Okay, thank you. Uhm Executive Order 28 also required New York City Cybercommand to ensure compliance with the policies, is there a mechanism in place to ensure compliance?

JEFF BROWN: There are mechanisms to ensure compliance. Some mechanisms are technical and some mechanisms are Administrative. New York City Cybercommand is working with the Agencies to make

sure that they take advantage of the most secure ways of, uhm of building and maintaining their technical systems.

CHAIR PETER KOO: What other consequence Agencies didn't comply with the Executive Order?

JEFF BROWN: We are in an active conversation with the Agencies about what is really the intent of our Cybersecurity conversation today and that intent is to make sure that we defend those systems against what really is the consequence of concern and that is the disruption of a system or the stewing of data and that is the, are the consequences that we are always are mindful about protecting against.

CHAIR PETER KOO: Uhm in general, can you tell us what are the targets of Cyberattacks?

JEFF BROWN: So, in general, the, if you think about New York City's City Government Systems. They are not necessarily unlike a highly complicated but very large enterprise environment. So, the types of threats that we see today are not unlike the type of threats that enterprises have to deal with each and every day. That is something that our team is incredibly focused on. Some of those threats that

are the most common are things like fishing events uhm that I think is a prevail and attack factor but there are many others so we have a defense in-depth strategy to make sure that we are taking a look at things that happen at other enterprises. Learning how to take those learning from the events of those other enterprises and learning to apply that learning against our own defenses to make sure they are enriched each and every day.

CHAIR PETER KOO: Not, yeah. Okay. So, you had mentioned in your testimony a privacy sensitive Wi-Fi Security Solution. Uhm what are the risks associated with using public Wi-Fi, so if I use Wi-Fi in this room, is it safe?

JEFF BROWN: No, so the Wi-Fi in public spaces, uhm there are two components of the NYC Secure Approach. One of the components is in any place where the City Government in New York is providing public Wi-Fi. We are configuring that Wi-Fi to take advantage of a non-for-profit what is called DNS Security Solution. The reason why we chose this DNS Security Solution it is just like the app, privacy by design. This solution, if a user connects to that public Wi-Fi terminal will only

prevent the user from connecting to a website that is specifically on the internet, placed by the internet to steal something from that user. It doesn't collect any of the browser information from, from that connection. So, we wanted to provide a very strong security solution to take a major piece of the attack factor off of the table when someone connects to a Wi-Fi, uhm that's one of the measures that we brought to bear the NYC Secure Initiative. The other is app, I'm happy to speak to that measure as well.

CHAIR PETER KOO: So, uhm, will any information be collected from the users. Are you collecting any information from there?

JEFF BROWN: No, no it doesn't, for the Wi-Fi solution, again it is a DNS security solution. The name of it is Quad 9. The thing that I find very interesting about the solution is that isn't just something that can be deployed at the places where the New York City Government provides public Wi-Fi, any individual who wants to education themselves about this initiative could take this home and configure their home advice to use the same piece of protection. It does not collect the browser history, it only interacts with uhm the domain name system in

a way so that the internet connection is successful. Uhm what is, what is very important to know is that the only thing it will block are sites that are only put there by criminal and advisories in order to compromise the device. It is the only thing, it's the only action it takes. And again, I think that this is a wonderful opportunity to speak with the Council about this, about this initiative because in many ways we want to inform New Yorkers, educate New Yorkers because this is a tool, they can bring home. They can use this tool in the day-to-day life and they would be safer and it would not be invasive in their privacy.

CHAIR PETER KOO: So, uhm so is the Wi-Fi use in all agencies the same? Or say is in library we have Wi-Fi too. In the New York City Public Library…

JEFF BROWN: So…

CHAIR PETER KOO: So, are they using the same systems as yours?

JEFF BROWN: Different Agencies, the Library and other Wi-Fi providers in the City, from a technical perspective they are all different systems. Uhm we've been working with the Agency to make sure

where they are providing public Wi-Fi, this solution is enabled. We are also working with other places in New York City that provide public Wi-Fi to enable the solution as well, like the Libraries. Uhm I don't have the Data right in front of me but I know my team has had many conversations with the public Wi-Fi… uhm with the public libraries and some of the have availed themselves of the solution to protect New Yorkers when they access their, their free Wi-Fi.

CHAIR PETER KOO: So, uhm, recently I ride on the subway, I see ads on the new NYC Secure App in the subways.

JEFF BROWN: That's right.

CHAIR PETER KOO: You are advertising for it, yeah, so, can you tell us something about it? Is it available for both Apple and Android uhm systems?

JEFF BROWN: That is correct, Chair Koo. It is available for both the Apple and the Android systems, uhm this app, the NYC Secure App the important note is that we built this app with Privacy by Design. So, at the code level this app does not collect any provide data from a New Yorkers Device. It is not capable of collecting that data. My organization does not receive data, any organization

does not receive data. It does not send the data from the device. The thing that the ad does is really in two categories, one we spoken a little bit about Wi-Fi security. It could give you a Wi-Fi alert. What the Wi-Fi alert is saying is that your device is connecting to an unsecure Wi-Fi. Uhm, as we know, the internet itself is in many ways not a secure place, so what we are reminding you in New York or what we are trying to educate a New Yorker to do is be mindful when you have those connections with your device to steer away from sites where you might want to conduct activity that would be of a private nature for you. It could be banking, it could be etc. as we are reminding New Yorkers to steer away from that and if you do want to conduct that activity to look for the connection to the HTTPS. That guidance is given right there for the New Yorkers. So that's a Wi-Fi we consider that a network type alert. It is not going to take action on the device, it is just going to let the New Yorker know. The other type of alert that comes off the NYCC app is called a device alert. A device alert might indicate that unfortunately you may… on a, on a link in a phishing email, etc. Unfortunately, your device has

come across a threat that the intent is to inject you know unauthorized code on to your device to try and give an adversary access to it. So, then it will give the New Yorker some advice, maybe turn off the phone, maybe reinstall from backup. Again, with this type of alert, we are also not taking a direct action on the device, we are alerting New Yorkers. We are trying to use the app to make New Yorkers more mindful as they navigate their life you know along the internet and to steer away from the threats.

CHAIR PETER KOO: So, how many people downloaded this app already?

JEFF BROWN: We have crossed the threshold of 50,000 downloads which is something my organization is exceptionally proud of. Quite simply, a number of months ago there were 50,000 less devices in New York City that were safe and now there is 50,000 more devices on behalf of New Yorkers that are safer, we are very proud of this.

CHAIR PETER KOO: Any feedbacks from the users?

JEFF BROWN: We have a mechanism through the website Secure.NYC for people to send us questions. We've gotten some, some questions about,

about the device, uhm about the, about the app and we've gotten some very positive feedback too I'm happy to report.

CHAIR PETER KOO: Thank you. So, what are the most common threats from the, that the New York City residents face daily you know in terms of internet, and cyber you know?

JEFF BROWN: So, I think that residents of the City, visitors, businesses, face many, many different threats as they conduct their life online. Research tells us that he most prevalent type of threat is called you know, a phish, uhm that's a very prevalent vector of an advisory trying to control the device, taking control of the device. Uhm there are some great ways of protecting yourself from that type of vector and you know we encourage New Yorkers to avail themselves of those protections.

CHAIR PETER KOO: So, in general how do we protect our systems in their home. We just buy an internet anti-virus software?

JEFF BROWN: So, from a protect systems at your home, I would point.

CHAIR PETER KOO: Uhm, in a small business?

JEFF BROWN: And small businesses. Uhm I would point a small business also towards NYC.Secure. A small business can configure it's Wi-Fi through the DNS solution, quad 9. A small business can put the NYC Secure App on its devices. I would also encourage a small business to research a concept called multifactorial authentication. That is another wonderful way of making sure that your email accounts and the other aspects of your business has additional layers of security. I would highlight of course you know in a land in a landscape where the threats are always evolving. You know, you cannot eliminate every aspect of this risk but there are great ways to help add defensive layers, even in a small business or even at home. We are trying to make sure that we are engaging New Yorkers in that conversation.

CHAIR PETER KOO: Thanks. Uhm Council Member Ulrich you have a question?

ROBERT HOLDEN: Holden yeah.

CHAIR PETER KOO: Holden oh yeah, I'm sorry, yeah.

ROBERT HOLDEN: He's better looking.

ERIC ULRICH: Not quiet.

ROBERT HOLDEN: Alright uhm what, now just uhm do anybody keep try on how many times we are, we are attacked. I mean certainly with the City System but do we have a number on that in your office? First.

JEFF BROWN: The fi…

ROBERT HOLDEN: The Cyberattacks. Yes.

JEFF BROWN: First, good afternoon Council Member Holden, uhm I'm happy to be here today.

ROBERT HOLDEN: Alright.

JEFF BROWN: We do keep track of these types of threats. One of the activities within a New York City Cybercommand is a 24/7 Security Operation Center. That Security Operation Center is part in partial of a capability that we call our Threat Management Function. That Threat Management Function each and every day is monitoring those City Systems has a number of ab… has a number of abilities to understand the amount of attacks, the types of attacks. Uhm the things that are blocked. The things that require further investigation and uhm you know act accordingly. Uhm so that's how we handle the volume. I would say to a certain extent New York

City, City Government Systems is part and partial for a size perspective of you know other very large sort of global companies, it is the size, right. Uhm and so we see accordingly the amount of activity that you would in that type of environment. I would also uhm note to Council that if you think about the internet, the internet itself is continually communicating in many, many ways so sometimes thinking about the sheer number uhm can be daunting but it is really the type of thing that is incredibly important to be mindful of because if we understand the type then we can take that type and make sure our defenses are set accordingly to defend against that type.

ROBERT HOLDEN: Yeah. Almost a day doesn't go by where we don't hear of phishing going on ab… by somebody. It is probably thousands or if not millions of people trying to phish and I do have like uh what is, obviously a lot of it is from oversees. Uhm do we have a country that is leading. I think I know the answer to this but in cyberattacks uhm that we, that we can actually track?

JEFF BROWN: So, in my program we think much less about the who than the how. As I, as I noted a moment ago, the types of attacks that we see

are global and to your point as we look at sort of new cycles in Cybersecurity, we see all kinds of different activity. It could be because of a phish, it could be something is stolen. It could be something is interrupted so what my program tries to do is leave the adversary attribution the who to other practitioners and very much concentrate on the how. Because once we know the how, we can apply that to our defenses to make sure that we are safe.

ROBERT HOLDEN: Right, and, and certainly the losses are, tremendous when people are you know phishing and Cyberattacks. Do we ever catch anybody uhm I mean I know your office, but not your office, do we ever find out as a network of scammers that are out there and you bust them?

JEFF BROWN: Uhm or, so I would point the Council Member to a number of activities that aren't the prevue of the NYC Cybercommand but uhm Department of Justice and other entities are involved very much in the, in the attribution and are working accordingly against that objection.

ROBERT HOLDEN: You know but we don't, let's say my son just got his identity stolen uhm and you know we don't know how it happened it just, you

know but it, it usually goes to the banks. Does that, does that go to law enforcement too? Like who should, if I'm somebody phishing. I'm the victim of phishing. I, you normally the banks get that information, do we have an office where we can call law enforcement?

JEFF BROWN: So, you are correct in the finance service sector, it is incredibly tight relationship with law enforcement and that type of relationship also exists with NYC Cybercommand. We are in close partnership and coordination with NYPD on almost a daily if not weekly basis and a lot of that is because not necessarily uh attribution, most of it is because of information sharing. There are many different channels in the Cybersecurity community to understand as I said the how and we want to make sure that we are connected to every single one of those channels.

ROBERT HOLDEN: Right.

JEFF BROWN: We let, the, the who for them but the how we want to learn from. So, we are very, very careful to get through those channels.

ROBERT HOLDEN: Right I get it, okay thank you.

CHAIR PETER KOO: We are also joined by Council Member Lander.

BRAD LANDER: Good afternoon.

CHAIR PETER KOO: Good afternoon, Council Member you have questions?

BRAD LANDER: Yes, Chair Koo. Thank you very much and I apologize for coming in late, so hopefully I'm not trotting ground. Oh, I'm sorry, if Council Member Yeger was here before me.

KALMAN YEGER: Go ahead.

BRAD LANDER: Okay. Uhm so hopefully I'm not trotting ground you already trod but uhm uhm it's nice to see here you here and thank you for your work. Can you just, first sort of tell me sort of a little bit about the org chart. Where you sit? You know I have been grappling with, you know because we have a Chief Technology Officer, we got a Commissioner of Do It. We have you know the Mayor's Office of Data Analytics which sits at the Mayor's office of operations. And I am having a little bit of a hard time just understanding kind of. I mean we want all of those things and we definitely want Cyber command and I assume you work with a range of obviously a whole much broader range of agencies but

can you just think, I don't know, who do you report to and how do you relate to those other key technology functions?

JEFF BROWN: Happy to. Uhm the Executive Order uhm outlines really the unique place that New York City Cybercommand has and the reason why that uhm it was put into I guess existence that way is for a very concrete reason. The conversation around Cyber Risk now in the City with the creation of New York City Cyber Commands allows us to have that conversation at City Hall as written in the Executive Order. The organization officially reports to the first deputy Mayor, we do work exceptionally closely each and every day with City Hall at the Deputy Mayor level. Uhm but the conversation about Cyber Risk can happen there along with as appear to a conversation around technology strategy and technology risk along with the conversation represented by the agencies around the service that they provide. It is within that context that you can really take a look at all the different ways that Cyber is a multi, sort of disciplinary multi-function, multi-technical conversation that goes beyond just technology. It goes beyond sometimes just business function because

it represents a safety risk. So, to you question, from a hieratical perspective and organization perspective, uhm at we now sit in a place where we can have that conversation as a peer office or to the agencies providing services or technologies across the city landscape. Uh and then beyond that so that's reporting into City Hall, beyond that we break down very much like any enterprise cybersecurity program uhm I would be a little hesitant to go into too much specifics but at a very high level uhm we have a function as I mentioned a little bit earlier, a threat management function, you can think of that as very much the team that does 24/7. They do the detection and response. We have a function called security uhm security sciences and that does the engineer and architecture for our tools and does advisory services as we try and raise the waters of the technology across all of the City landscape. We have a function called urban technology. That is a very interesting function, that is perhaps not something that you would normally see in other enterprises but that is very much a forward looking function to think about, as the, as the City's, as the City landscape proliferates with the devices, we

have to think very mindfully about what types of devices the City operates, so that function, from an urban technology perspective is leading that conversation and then we have business functioning and governance functions, just like you would see in, in any other office here in the City.

BRAD LANDERS: Alright so that's very helpful. And I asked a couple of questions more about uhm you know how some different functions relate, uhm so I know we have had a dialog in the past around the link NYC and how the. And this maybe about protecting New Yorkers Data Privacy and paying attention to you know how they are using it. Obviously, there is a contract and some of that was negotiated there but and there are all kinds of things evolving over time. So, is that a conversation that you are a part of or is that because I don't know whether it was Do It or DCAS that actually negotiated the contract with LINK. Uhm you know was, is that an issue that you guys would deal with or is that in somebody's else's domain?

JEFF BROWN: So, with regard to Link I am first proud to report to the Committee that they are adopting the Quad 9 solution.

BRAD LANDER: And I love link so this not like I'm worried about them it just is a place where these issues exist in, in, in you know in real time.

JEFF BROWN: That's right, so we work, we work very closely with Do It on making sure that the security policy, standards, the principals that we are bringing across all of the umbrella agency systems are applied in like all of their business matters and uhm Link would be inclusive of that. And it would be the same answer to any technology system that an agency is uhm looking to adopt. It goes back to like I outlined, the conversation of Cyber Risk for Technology Risk and Strategy with business function. That's the, that is sort of the table setting of the conversation. We are influential when it comes to Cyber Risk. The threat management function does have you know the, the Executive Order authority to mandate technical controls so that is another umbrella type cyber defense that, that we are the, sort of the central recipient and actor on that.

BRAD LANDER: Uhm and then I guess my last question you know the thing that I think of as paying attention to the data privacy issues for New Yorkers in relationship to government. You know, we

are collecting lots of data, let's say I'm I don't know what it is, I don't know, you know, I deal with parking tickets of whatever. I am an Agency that in one way or another is collecting a lot of New Yorkers uhm data. Uhm in, you it sounds like you are definitely working with me on kind of thinking about the threats that someone might come in and try to get at that, how about the questions about just how we as a City ought to be thinking about that and you know what our algorithms do and where we might expose people to uhm you know. I am actually pretty happy right now that the speed camera and red-light camera data is out there for all to see. I mean it's by license plate, we don't know the name of the individual with the license plate, but every one of those tickets winds up getting aggregating and there is actually a great twitter bot that you can when you see a driver do something horrific or obnoxious you take a picture of their license plate and you tweet it at How's My Driving and you get back this record of all of their violations of our cameras uhm and you know I actually want to use that data to start a more reckless driver accountability program, but for now, there is like some public accountability you know but

I'm sure there are places people would say uhm you know, uhm doing that is a form of doxing or, uhm that certainly is a form of doxing but where is the line. And so uhm if I'm you know I am a CIO in an agency are you guys working with me on that set of data privacy questions or does that sit somewhere else in the City's Technology Firmament?

JEFF BROWN: So, if I may, a number or brief data points on the question. First, of course, there are a number of different stakeholders in that conversation. There is a Chief Privacy Officer. There is an Agency that is building that technology. There is a, you know office for the Data Strategy for the City that is doing it. There is a number of stakeholders in that multi-faceted conversation, uhm another brief point, when it come sot data security, that is a discipline within Cybersecurity so we are working with agencies to make sure that data and systems that hold data are identified. Uhm and that the appropriate controls, encryption and others are applied to those data sets and then third, when it comes to privacy, I would really point the Council Member no further than the NYC Secure Principals. From a Cyber Security perspective, we have said for

New Yorkers that Cyber Security as an essential service, as something that is a public safety issue, needs to protect privacy and respect privacy as well. We have a belief that Cyber Security can uphold privacy and doesn't in no issue should invade a New Yorkers privacy. So that's the principals of my office.

BRAD LANDER: That is great. And so, I, just maybe I should have known we had a Chief Privacy Officer but I that person sits where?

JEFF BROWN: I believe, though I am happy to get back to the Council on this but I believe that is within the Mayor's Office of Operations.

BRAD LANDER: Okay that might be an interesting followup hearing for us to talk with the Chief Privacy Officer about some of the.

CHAIR PETER KOO: So, any more questions members? Seeing none. Mr. Brown thank you very much for that testimony. I'm sorry I didn't turn on the mic. So, I want to thank you for your testimony and thank you for your dedication and your leadership.

JEFF BROWN: Thank you Chair Koo and Council Members for having me today.

CHAIR PETER KOO: Are there any more public participations? Seeing none. This meeting is adjourned. Thank you. (gavel pounding). You always come at the right time.

BRAD LANDER: This was luck today. I was actually trying to get here earlier but I got waylaid on the way in.

C E R T I F I C A T E

World Wide Dictation certifies that the foregoing transcript is a true and accurate record of the proceedings. We further certify that there is no relation to any of the parties to this action by blood or marriage, and that there is interest in the outcome of this matter.

Date JANUARY 14, 2019