

CITY COUNCIL
CITY OF NEW YORK

-----X

TRANSCRIPT OF THE MINUTES

of the

COMMITTEE ON TECHNOLOGY

-----X

January 19, 2012
Start: 10:04 a.m.
Recess: 10:56 a.m.

HELD AT: Council Chambers
City Hall

B E F O R E:
FERNANDO CABRERA
Chairperson

COUNCIL MEMBERS:
Council Member Gale A. Brewer
Council Member G. Oliver Koppell
Council Member Mark S. Weprin

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

Daniel Srebnick
Associate Commissioner for IT Security
Department of Information Technology and
Telecommunications
Chief Information Security Officer for New York City

1
2 CHAIRPERSON CABRERA: Okay, we're
3 ready. All right, let's get this started.
4 Welcome, everyone. Good morning. So happy to be
5 here this morning. This bright, beautiful day.
6 And I'm joined this morning by Council Member Gale
7 Brewer and the introduction, the hearing on Intro
8 664. And I would like to welcome everyone to this
9 hearing on Introduction Number 664, relating to
10 data security plans for City agencies from
11 registering voters to approving permits, to
12 vaccinating children. The City regularly collects
13 important information about its residents in order
14 to effectively provide services. Much of this
15 information, such as medical records and certain
16 political contributions is confidential. Other
17 information, such as addresses, dates of birth,
18 and social security numbers, could be used for
19 identity theft. It is therefore critical that
20 personal information collected by City agencies be
21 kept secure. Experience has shown that this
22 information is not always effectively protected;
23 however, the privacy rights clearinghouse reports
24 that there have been on average nearly 20
25 occurrences of data breaches within New York City

1
2 annually since 2005. One particularly noteworthy
3 example occurred in late 2010, when medical
4 records were stolen from New York City Health and
5 Hospital Corporation. I definitely remember that
6 one. The records were digitally, were digital
7 files being transported in a van, in all 1.7
8 million records were stolen. While most breaches
9 in recent history have been by private
10 organization, some involve New York City
11 government. For example, over 200 case files from
12 the Administration, for children's services,
13 containing sensitive personal data about families
14 and social workers involved in agency cases, were
15 found unshredded in a garbage bag on a street
16 corner in 2006. Other jurisdictions have
17 addressed the risks of data breaches with
18 legislation requiring data security plans;
19 however, New York City agencies are not currently
20 required to create or enforce a plan to secure
21 personal data in their possession. This Committee
22 today will gather testimony on Intro No. 664,
23 which seeks to remedy this problem by requiring
24 agencies to create and enforce, enforce data
25 security plans. Let me now have Council Member

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

Brewer share some words.

COUNCIL MEMBER BREWER: I just want to thank very much the Chair for his interest in this topic, he's had a long time interest in this topic. I want to thank Jeff Baker, I know he's Counsel formerly to the Committee, and been promoted. Crystal Goldpond [phonetic] who's the Policy Analyst, and the new attorney David Seitzer [phonetic], they have all contributed to my knowledge on this topic over the years. I think this is a common sense measure to ensure that every City agency is taking the necessary steps to protect personal information and I think in addition to what the Chair indicated, it also will help set the precedent for some of the nonprofits who are also nervous because they deal with very vulnerable populations and I think that they will have some guidebooks to look to as we go forward with this bill. I think that the issue of encryption is something that we will all be looking toward, that perhaps would have helped with the HHC disaster. And I think we will have a better monitoring process, and I hope that we'll have a more centralized way of looking at the data

1
2 security that we're all so concerned about. It's
3 a brand new world. I think even words, and we'll
4 hear from the very esteemed personnel from DoITT,
5 but even things like passwords may be passé, as
6 time goes on. So the question is how do you come
7 up with a procedure that is also able to be
8 foreseen into the future and keeps up with the
9 technology. And of course all of this is
10 surrounded by paper. I'm the worst, I'm a
11 technology nut and I have too much paper. I'm
12 totally cognizant of that. so the question is, a
13 lot of these agencies have the same issue, and so
14 the question is how do we keep up with the
15 technology, provide security for our data and at
16 the same time deal with this paper. We look
17 forward to your testimony. Thank you, Mr. Chair.

18 CHAIRPERSON CABRERA: Thank you,
19 Council Member Brewer. I want to thank you for
20 being a champion and in protecting personal data
21 and you've been literally in the forefront for
22 many years even before I became a Council Member.
23 So, we, let me just use the word, we honor you
24 today, today for that. Let me now turn it over to
25 Mr. Daniel Srebnick, from DoITT for testimony.

1
2 DANIEL SREBNICK: [off mic] Yeah,
3 thank you--[on mic] Okay. Good morning, Chair
4 Cabrera, and Members of the Council Committee on
5 Technology. My name is Daniel Srebnick, I'm the
6 Associate Commissioner for IT Security at the
7 Department of Information Technology and
8 Telecommunications, or DoITT. And I'm also New
9 York City's Chief Information Security Officer.
10 I'd like to thank you for the opportunity to
11 testify today on Intro 664, in regard to security
12 of personal information. With the maturing of the
13 digital age and the explosion of attendant data,
14 the management of citywide information security is
15 clearly as important as any of DoITT's
16 responsibilities. And accordingly, we've crafted
17 citywide information security policies and
18 standards that are as strong and as dynamic as the
19 City that we serve. Pursuant to the New York City
20 Charter, DoITT is empowered to plan, formulate,
21 coordinate and advance information technology and
22 that includes ensuring the security for data and
23 other information stored in the City's IT
24 infrastructure, for example data centers,
25 networks, web portals that support critical City

1
2 agency functions. In 2006, DoITT assumed primary
3 responsibility for the review of and as necessary
4 the promulgation of new policies and standards to
5 ensure the confidentiality, the integrity and the
6 controlled accessibility of electronic information
7 processed through and by the City of New York.

8 And DoITT also assumed primary responsibility for
9 information security auditing; in other words,
10 through sister agencies and minimizing internal
11 exposures that could compromise sensitive data,
12 disrupt agency operations, cause liability or
13 otherwise diminish public trust. In 2010, the
14 role was further reinforced by Executive Order
15 140, which empowered DoITT to establish and
16 enforce citywide IT policies and for ensuring that
17 those policies are aligned with the City's
18 business needs and investments, as well as the
19 individual business needs of each agency. So,
20 included in this authority is the provision of
21 citywide information security policies and
22 standards, a collection of directives which
23 together provide the basis for the City's IT
24 governance. And pursuant to this authority,
25 DoITT's IT security division ensures the overall

1 security of the City's data and information
2 technology assets. Security services are
3 centrally managed by DoITT for use by City
4 agencies and these include things such as
5 perimeter firewalls, intrusion detection, an
6 industry standard model for three tier public web
7 hosting for internet applications, complete with
8 layered security and citywide malware and spyware
9 protection. And we work constantly to build a
10 consciousness about information security matters
11 by issuing a regular citywide information security
12 awareness newsletter to all City employees. And
13 we've covered topics such as identity theft,
14 protecting portable data, rogue antivirus
15 software, and issues around security and privacy
16 on social networking sites. So these, as well as
17 a comprehensive listing of all of the citywide
18 information security policies and standards, and
19 the appropriate DoITT contacts for IT security
20 matters, are available through City Share, the
21 city's employee internet portal. DoITT's work has
22 led to New York City being viewed as a municipal
23 leader in the information security field. In
24 2009, for example, New York was the first city in
25

1
2 the country to participate in the Department of
3 Homeland Security's biennial "cyberstorm" exercise
4 series, and this simulates large scale cyber
5 events and attacks on government and critical
6 infrastructure, key resources, so that
7 collectively cyber preparedness and response
8 capabilities can be assessed and measured against
9 realistic and credible national level events.

10 More recently, the information security executive
11 program, which holds annual awards to recognize
12 information security directors and teams who've
13 demonstrated outstanding leadership in IT security
14 management, recognized DoITT's IT security team
15 for its work with MacAfee to deploy an integrated
16 network host and cloud security solution, and to
17 leverage threat analytics to support 180,000 users
18 across 52 city agencies. So, as a result of these
19 and other efforts, for more than a decade now,
20 there have been no reported breaches of DoITT
21 managed infrastructure or on any applications
22 where our security accreditation process has been
23 successfully completed. So, as successful as
24 we've been, there's always the opportunity to
25 further improve upon the job we do, and in an area

1
2 as vital as IT security, it's imperative of us
3 first to do so. And because the thrust of Intro
4 664 would help to codify interlocal law much of
5 what our citywide information security policies
6 and standards already require of agencies, we
7 welcome the opportunity to discuss with the
8 Council how the bill can be crafted to ensure it
9 meets those goals, as well as the high standards
10 New Yorkers expect and deserve when entrusting the
11 City with their personal information. So, while
12 we support the spirit of Intro 664, and the
13 emphasis it places on comprehensive citywide
14 information security, the proposal will however
15 require some further examination in areas to
16 ensure feasibility of implementation and
17 standardization across City agencies. So, allow
18 me to outline some of these considerations as
19 follows. The bill as currently drafted would
20 require each individual agency to develop,
21 implement and maintain a comprehensive security
22 program for their systems of records containing
23 personal information. Better we believe to have
24 the City, through DoITT, to continue to review
25 existing and promulgate citywide information

1 security policies and standards, with baseline
2 criteria, which can be applied across all
3 agencies, and this approach, as the current
4 practice does, would still allow agencies that opt
5 for additional security measures to implement them
6 as appropriate while avoiding duplicative effort
7 and unnecessary expense that would accompany an
8 agency by agency mandate or approach. Next, the
9 bill, as currently drafted, places substantial,
10 and appropriate focus on securing files, records,
11 systems, in and on which personal information is
12 stored. But information security can be
13 compromised not only through infrastructure, but
14 through application flaws, and it's important,
15 therefore, to secure the digital and paper based
16 records that applications draw data from and run
17 upon, as it is to secure the applications
18 themselves. So, application security today is
19 addressed by way of DoITT's security accreditation
20 process. And this is a process which we require
21 all applications that are either multiagency or
22 public facing in nature to go through. Pardon me.
23 [pause] So the process is designed to determine
24 whether data contained within a system that's been
25

1 developed, has been appropriately classified;
2 whether the system itself has been constructed
3 with security controls appropriate to that data
4 classification. And, as part of the process, we
5 include automated scans that check the hosting
6 platform and the application for security
7 vulnerabilities that could be leveraged to steal
8 or to otherwise change data. Moreover, as part of
9 the accreditation process, DoITT confirms that all
10 private data is appropriate--appropriately
11 protected by encryption and access controls. So,
12 in 2011, for instance, 25 major applications were
13 accredited through the process, and as examples,
14 the eHire system, the September 11th 10th
15 Anniversary website, and the first accreditation
16 of an externally hosted cloud application, put up
17 by the Department of Transportation, their
18 feedback portal. As part of the process, 1,500
19 vulnerabilities that could've led to the
20 compromise or unwanted disclosure of private data,
21 were uncovered last year, and were remediated
22 before those applications went live. Finally, the
23 bill as currently drafted requires employing some
24 fairly specific user authentication protocols,
25

1
2 which if codified in law could unintentionally
3 prevent the City from implementing the latest
4 tools and security measures. As an example, as
5 technology continues to advance, passwords may no
6 longer be the primary means by which user access
7 is controlled several years from now. So, it
8 would be preferable, therefore, to legislate the
9 establishment of and compliance with an
10 overarching identity management program which
11 would have the flexibility to keep pace with
12 technological advancements and change. So, these
13 are but a few of the topics for further
14 discussion, in a bill otherwise I think rightly
15 aimed at addressing a constant imperative of the
16 digital world: information security. By not
17 confining the City to the parameters of specific
18 technological tools, but rather acknowledging the
19 need within a standard framework of current best
20 practices, to develop policies agile enough for
21 all agencies to adapt to the ever changing and
22 evolving and sophisticated means of technological
23 attack, we can pursue a considered approach to
24 ensuring the continued privacy and security of all
25 New Yorkers. We look forward to working with you

1
2 in that regard, and this concludes my prepared
3 testimony and I'll be happy to address any
4 questions. Thank you.

5 CHAIRPERSON CABRERA: Thank you so
6 much. Can you share with me, you know, last,
7 2010, had a lot of my friends in The Bronx who,
8 Bronx Lebanon and, and there was another hospital,
9 there were digital files that were being
10 transported in a van, and at one point seven
11 million records were stolen. And including staff.
12 And I was really disturbed how easily they were
13 stolen. You know, they were being transported,
14 the laptop was left in the backseat, with the door
15 unlocked. Can you share with us, from--regarding
16 DoITT's policy in transporting any kind of
17 hardware that have any kind of secure information?

18 DANIEL SREBNICK: Yeah, that's a
19 great--

20 CHAIRPERSON CABRERA: Or
21 information that should be secure.

22 DANIEL SREBNICK: --that's a great
23 question, Chairman Cabrera. And these, the
24 matters of both private data and portable data are
25 clearly covered by existing DoITT policies and

1 standards. And to summarize, any private data
2 stored on any medium, whether it's disk, tape, USB
3 drive or so forth, is required to be encrypted.
4 So that's one method of securing it. And then, as
5 well, any portable data of any kind, regardless of
6 classification, is required to be encrypted when
7 being transported.
8

9 CHAIRPERSON CABRERA: My
10 understanding was within New York City Health and
11 Hospitals Corporation data, that it was not
12 encrypted. I know you guys don't, as I
13 understand, you don't have oversight over--do you
14 do have oversight or say regarding the New York
15 City Health and Hospital Corporation?

16 DANIEL SREBNICK: No, no, we, we do
17 not. Normally our oversight extends to those
18 agencies that are either mayoral or by virtue of
19 connection to CityNet, which is the, the
20 institutional network that DoITT manages on behalf
21 of the City.

22 CHAIRPERSON CABRERA: Have you ever
23 had data that was in storage, it was being
24 transported, and stolen?

25 DANIEL SREBNICK: In my

1
2 recollection, the only incident where data was
3 physically stolen, that I'm aware of, occurred
4 several years ago when a laptop containing some
5 private data of New York City pension recipients,
6 that was under control of the financial
7 information services agency, was lost.

8 CHAIRPERSON CABRERA: And was that
9 information encrypted? As you recall?

10 DANIEL SREBNICK: As I recall, it
11 was never clearly understood whether it was
12 encrypted or not. I would feel much better about
13 it if the answer came back that it was encrypted.
14 One of the, one of the services that DoITT now
15 provides to all city agencies that are part of
16 this enterprise agreement with MacAfee, is that we
17 will provide free full disk encryption software to
18 any agency covered under the agreement that would
19 like it. So we, we see no reason why this should
20 ever occur again.

21 CHAIRPERSON CABRERA: Okay. Can
22 you show us, what are your standards of encryption
23 that is being used?

24 DANIEL SREBNICK: Sure. Well,
25 typically, we defer to NIST. So, the federal

1
2 government has invested a lot of money in
3 developing NIST's standards and if NIST says it's
4 good, that's our baseline. So, we're talking
5 about AES 256 bit encryption. And as we stated
6 during the formal testimony, encryption standards
7 change; as technology changes, what was viewed as
8 secure encryption may be broken and technology
9 then will evolve to keep up with that.

10 CHAIRPERSON CABRERA: Now, you're
11 suggesting in your testimony that you would rather
12 see DoITT have complete oversight and setting all
13 the standards and policies for all of the
14 agencies. If that were to be the case, would
15 DoITT have the authority to require agencies to
16 comply to the plan?

17 DANIEL SREBNICK: To a large extent
18 today, DoITT has a lot of leverage in terms of
19 compliance, in that the multiagency network
20 CityNet is managed by DoITT. The internet
21 connection is managed by DoITT. And Executive
22 Order 140 gives DoITT the authority to set those
23 standards.

24 CHAIRPERSON CABRERA: Okay.

25 DANIEL SREBNICK: Additionally,

1
2 there was a memorandum of understanding between
3 our Commissioner and the Commissioner of DOI,
4 delegating that authority that DOI formerly had
5 for such formulation of policies and standards, as
6 well as auditing to DoITT.

7 CHAIRPERSON CABRERA: Let me not
8 hog the pulpit, so let me turn it over now to
9 Council Member Brewer.

10 COUNCIL MEMBER BREWER: Thank you
11 very much, Mr. Chair. And also great testimony.
12 I guess my question is, do you have some sense now
13 of, I don't know, 80, 40, I never remember,
14 Mayoral agencies or whoever's on CityNet, what
15 their policies are, and if they're complying. In
16 other words, how do you monitor whether or not
17 there's compliance.

18 DANIEL SREBNICK: Well, one of the
19 best ways we, we monitor and ensure compliance is
20 through the security accreditation process, as
21 agency's go to deploy public facing applications,
22 because DoITT controls the internet connection
23 ultimately and whether those applications can be
24 deployed. We have, I would say we have a very
25 high level of compliance today, as a result of the

1
2 accreditation process. Furthermore, in terms of
3 policy development, let me explain that we have
4 taken a collaborative approach with City agencies,
5 and for a number of years, and currently under
6 the, the governance of the Technology Governance
7 Board, established through E0140, we hold biweekly
8 meetings with stakeholders in City agencies to
9 discuss the evolution of policies and standards,
10 and we talked to, you know, their security people
11 and get input the issues that they are having. So
12 we're getting input from the human services
13 agencies, from the financial agencies,
14 administrative agencies, and public safety
15 agencies, on this as well.

16 COUNCIL MEMBER BREWER: Okay, and
17 then there was somebody here earlier from Covenant
18 House who had to leave, but how do the social
19 service agencies, which I think would be, along
20 with the police department, perhaps, I'm just
21 making an assumption, the ones where private data
22 might be most at risk, just from a public
23 perspective. So, how do the contracted out
24 agencies, if at all, play any part in this issue.
25 In other words, you've got HRA, and the list goes

1
2 on, do they have to conform to any of these goals,
3 or is this something you're working on, or is it
4 not even relevant?

5 DANIEL SREBNICK: No, HRA, ACS--

6 COUNCIL MEMBER BREWER: The whole
7 list.

8 DANIEL SREBNICK: --and all of the
9 public, the social services agencies, are required
10 to follow the policies and standards. And you
11 mentioned the contracting out that many of these
12 agencies do, and we have recognized that there are
13 issues around information security, in terms of
14 contracts and vendors and as a result, one of the
15 most recently developed policies, which is about
16 to be published, is a policy we're calling the
17 "Information Security Policy for Service
18 Providers." And what this gives is a template
19 guide to agencies of language that should go in
20 contracts where access to City data is involved,
21 to more uniformly require things like security
22 audits, background checks and the types of things
23 that you would want to do.

24 COUNCIL MEMBER BREWER: Are we
25 doing any training for these nonprofits, maybe

1 through the Human Services Council or whatever,
2 about how to conform with these new policies?

3 Because it's my experience that, you know, they're
4 pretty strapped and they don't always have the
5 staff and the expertise that you do in-house.

6 DANIEL SREBNICK: Yeah, we'll have
7 to get back to you see, see what our, what our
8 involvement is on that.

9 COUNCIL MEMBER BREWER: Okay,
10 because they obviously have data issues, took, in
11 addition to the employment and background. So,
12 does this policy include how to conform to data
13 standards when they go back and forth? Because
14 we're all talking about electronic health records,
15 we're all talking about trying to deal with, as
16 you know, figuring out a way that you don't have
17 to put your address down six different times,
18 etc., etc.

19 DANIEL SREBNICK: Yeah, the policy
20 applies to City data, wherever that data is.

21 COUNCIL MEMBER BREWER: Okay. What
22 does an accreditation report look like? That's
23 just my lack of knowledge. Can you describe it?

24 DANIEL SREBNICK: So, so rather
25

1
2 than a report, it's a, it's a process, and the
3 process is supposed to begin when the system is
4 first being designed. The idea is to meet with
5 the stakeholders at the beginning of the, the
6 development, understand what they're trying to
7 design, and to ensure that the ultimate design
8 will, is built to the classification of the data,
9 that the system's going to have, and the
10 appropriate controls are there, whether it's disk
11 encryption, encryption over the wire, multifactor
12 authentication or any of the controls that you
13 would want to have. And it's a, it's an iterative
14 process, and at the end of it we come up with an
15 approved document which shows the data
16 classification, the system architecture, the
17 controls, it will identify any risks. Sometimes
18 there are risks for which an exception can be
19 granted, if a particular control isn't followed,
20 as long as there is another kind compensating
21 control. And at the end, a letter of
22 accreditation is issued to the business owner,
23 that says, "We have reviewed and accredited your
24 application. The controls applied are reasonable,
25 and in keeping with the classification of the

1
2 data, as well as listing any significant risks
3 which are either deemed acceptable or which have
4 deadlines for clearing. And a deadline for
5 clearing might be that a particular database had
6 not, for example, implemented encryption at rest,
7 but while it's being implemented, there are going
8 to be additional audit controls put in place and
9 the stakeholders have agreed, say within six
10 months of going live, that that encryption will be
11 implemented.

12 COUNCIL MEMBER BREWER: Okay. go
13 ahead Mr. Chair.

14 CHAIRPERSON CABRERA: Oh, thank you
15 so much. We've been joined by Council Member
16 Koppell, welcome.

17 COUNCIL MEMBER KOPPELL: [off mic]
18 Thank you.

19 CHAIRPERSON CABRERA: In 2010, the
20 Comptroller issues, he issues some recommendation.
21 Let me go through each one of them.

22 DANIEL SREBNICK: Sure.

23 CHAIRPERSON CABRERA: There were--
24 so in fact there were eight of them. So, I'll try
25 to go through these quickly. The first one was

1
2 "The performance citywide risk assessment of
3 applications that have not participated in
4 security accreditation process." Where are we
5 with that?

6 DANIEL SREBNICK: So, we have
7 completed that, we have given the results to the
8 agencies, and we're currently working with
9 agencies to bring those applications into
10 compliance. The ultimate objective will be to
11 take all of these legacy applications and migrate
12 them to a central secure hosting environment for
13 internet applications at DoITT.

14 CHAIRPERSON CABRERA: Okay, here's
15 number two. "Contact those agencies whose systems
16 posed the most critical risk and request that they
17 submit applications for the security accreditation
18 process."

19 DANIEL SREBNICK: And we have done
20 that, and we are beginning to get some of those.

21 CHAIRPERSON CABRERA: Okay.

22 DANIEL SREBNICK: So we have made
23 some headway there, as well.

24 CHAIRPERSON CABRERA: You're two,
25 you're two for two. Here we go: "Request

1
2 assistance from the Mayor's Office of Operations
3 in directing agencies to participate in security
4 accreditation process."

5 DANIEL SREBNICK: And we are
6 working with the Mayor's Office to direct agencies
7 to comply with all citywide information security
8 policies and standards, including the
9 accreditation process.

10 CHAIRPERSON CABRERA: So, when will
11 you see that--you said this is a, this has been
12 completed or is this just a process, it's an
13 ongoing process?

14 DANIEL SREBNICK: So, so, it's,
15 it's an ongoing process, in that as new
16 applications are developed or old applications are
17 modified, new security issues will come up. So,
18 you know, the work is never done, in that regard.

19 CHAIRPERSON CABRERA: Number four,
20 "Ensure that all the documentation relating to the
21 security accreditation requests for all
22 applications be submitted and maintained."

23 DANIEL SREBNICK: Yeah, so this was
24 a recordkeeping issue from the early days of the
25 accreditation process, when it was really started

1
2 by a staff member on my team as a part time
3 effort. And you know, we realized as the process
4 matured, we needed to formalize things better, and
5 we've gone from keeping the records on a
6 spreadsheet to an internal share point site where
7 all the records are stored. So, we believe we've
8 satisfactorily that.

9 CHAIRPERSON CABRERA: Fantastic.

10 Number five, "Develop a form of security
11 accreditation process that for in-house
12 certifications."

13 DANIEL SREBNICK: Yeah, I think
14 that was a bit of a misunderstanding between the
15 auditors and the team, but essentially what they
16 said is it looked like for a couple of internal
17 DoITT applications, that the process was not
18 followed and we have ensured since that time, that
19 the process is followed, whether DoITT is the
20 business owner of the application, or any other
21 agency.

22 CHAIRPERSON CABRERA: "Assure that
23 security issues found in applications with
24 exceptions, with exceptions, are followed up and
25 corrected by the agency."

1
2 DANIEL SREBNICK: So, I, I
3 mentioned in our accreditation emails now, that we
4 are listing a risk table and giving specific dates
5 by which issues need to be cleared, and if they're
6 not, the application is at risk of either losing
7 its accreditation or there's going to be some
8 follow up or repercussions. So that is, as a
9 direct result of this recommendation.

10 CHAIRPERSON CABRERA: I'm almost
11 done here. "With assistance of the Mayor's Office
12 of Operations, require that agencies participating
13 in the SAP follow all citywide security standards
14 and security policies to ensure the applications
15 are operating in the security environment."

16 DANIEL SREBNICK: And we certainly
17 have done that. And we rigorously enforce the
18 policy to the extent that the application is
19 hosted within a DoITT controlled environment.

20 CHAIRPERSON CABRERA: Let's if you
21 could bat for 100 and be a grand slam DoITT.

22 DANIEL SREBNICK: [laughs]

23 CHAIRPERSON CABRERA: "Enhance the
24 security accreditation process procedures to
25 ensure all agencies deploying applications only

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

after it has been accredited by DoITT."

DANIEL SREBNICK: And, and as mentioned, where we control the pipes and the data center, we certainly do that rigorously.

CHAIRPERSON CABRERA: So you batted for 100. I like that. Let me ask you a question, how do you, how do the agencies respond to breaches? And is there a uniform policy?

DANIEL SREBNICK: There is an incident response policy which at a high level requires agencies to contact us and keep us posted. And generally, where there has been an internal issue, agencies are very quick to reach out for assistance. We have good relationships with law enforcement, we work closely with Lieutenant Lane and the NYPD Computer Crime Squad, so those channels are open and we find there is a high degree of conscientiousness on this issue.

CHAIRPERSON CABRERA: Do, do you find, is this a daily occurrence, where people are trying to breaking into the system? What's the farthest that anybody has been able to achieve?

DANIEL SREBNICK: Yeah, so far, it's a very interesting question. From the

1 internet, it's, you know, happened probably
2 thousands of times while we've just been sitting
3 here. I asked for an update this morning, on some
4 statistics from our internal intrusion detection
5 sensors. And let me, let me put this in
6 perspective for you. I think Commissioner Kelly
7 of the Police Department testified last year in
8 front of Congress that NYPD was probed and
9 attacked externally 70,000 times per day.
10

11 CHAIRPERSON CABRERA: Wow.

12 DANIEL SREBNICK: The daily average
13 for the month of January for the network's DoITT
14 controls is 850,000.

15 CHAIRPERSON CABRERA: Wow.

16 DANIEL SREBNICK: We--

17 CHAIRPERSON CABRERA: How--Yeah, go
18 ahead.

19 COUNCIL MEMBER BREWER: I'll just
20 say one thing which was amazing to me. The public
21 library was hacked, the website, over the weekend.
22 'Cause I tried to get in.

23 CHAIRPERSON CABRERA: Why would
24 they do that?

25 COUNCIL MEMBER BREWER: And Google

1
2 had a big sign on it stating, "You, this site is
3 down." And it was because somebody was trying to
4 steal all of their--like your NYC.gov, that site
5 is hit fabulously all the time, we all use it.
6 And somebody had tried to hack every single one of
7 those members, all of us. And so I'm just saying,
8 it's unbelievable. And they had to close the
9 whole site down.

10 CHAIRPERSON CABRERA: That's crazy.

11 COUNCIL MEMBER BREWER: For a day,
12 just because of--

13 DANIEL SREBNICK: Yeah, I, I had
14 not heard about that, we'll have to look into
15 that.

16 COUNCIL MEMBER BREWER: It was a,
17 but they did it, I mean, it was amazing that that
18 could happen. And just to give an example of how
19 challenging the hackers are, that's all I wanted
20 to say.

21 CHAIRPERSON CABRERA: I--have we
22 been successful in prosecuting those who have
23 breached and system and stolen data?

24 DANIEL SREBNICK: Well, so, since
25 personally we have had no experience with a breach

1
2 into the infrastructure for which my team is
3 directly responsible for, it's difficult to answer
4 that question. There, I know, are issues
5 regularly being investigated by NYPD computer
6 crimes. And I would defer to Lieutenant Lane and
7 the Detective Bureau on a response to that.

8 CHAIRPERSON CABRERA: Thank you so
9 much. Let me turn it over to Council Member
10 Brewer.

11 COUNCIL MEMBER BREWER: Thank you
12 very much. I just want to go back to these, these
13 contracted out agencies, because I do worry that
14 they're not going to be able to successfully
15 implement some of your procedures. So, are you
16 going--I know you talked about getting back to us
17 about the training--but when this implementation,
18 whatever the new information policy for whatever
19 you call it, it's something for I guess the
20 service providers, basically. Once that's
21 recorded and circulated, what will be the follow
22 up that you would likely to see in terms of some
23 of these agencies?

24 DANIEL SREBNICK: Well--

25 COUNCIL MEMBER BREWER: My, my

1
2 experience is that have slow computers, in many
3 cases, I hate to tell you that. They don't have a
4 lot of pipeline, often. And it's, you know, it's
5 a challenge out there. We're not ten years away,
6 we're still not in the 22nd Century for some of
7 them.

8 DANIEL SREBNICK: Yeah, I
9 understand, and I think that strategically, the
10 City and other government entities, as well as
11 business, is wrestling with this whole idea of
12 external data because of the proliferation of
13 mobile devices. And the consensus in the security
14 industry, and it may be a model that the City
15 ought to follow, is that just because an entity
16 needs to access our data, doesn't necessarily mean
17 our data needs to leave the premises. So, through
18 use of technologies such as virtualization and
19 remote access, these problems ought to be
20 solvable, ultimately.

21 COUNCIL MEMBER BREWER: Okay. And
22 this is also my lack of knowledge, but how is the
23 change in the cloud computing able to help you?
24 And how are, how is it, how is it changing? And
25 how are you utilizing it?

1
2 DANIEL SREBNICK: Yeah, well, I
3 mean, the great benefit of the cloud computing is
4 the idea that you can very quickly provision
5 something that may have taken much longer to
6 physically build in-house. I think the great
7 enthusiasm for cloud computing needs to be
8 tempered with the, the knowledge that just because
9 you can spin up a server very quickly, does not
10 mean that you should not follow all of the other
11 processes that you would normally do. For
12 example, the federal government has their fed ramp
13 program. And the fed ramp program is a program
14 which attempts to pre-accredit information hosting
15 providers, but the idea is that any application
16 deployed still has to go through their
17 accreditation process, have data classified, and
18 verify that the controls are adequate.

19 COUNCIL MEMBER BREWER: Okay,
20 that's helpful. How does the Mayor's Office of
21 Operations--you mentioned them a couple of times,
22 as the Chair did--are they like a partner in this?
23 Obviously they have, you know, set policy and so
24 on. How do you work with them and I still worry
25 about my paper in the files. What are we going to

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

do with that?

DANIEL SREBNICK: Oh, well, yeah,
paper, paper in the files.

COUNCIL MEMBER BREWER: It scares
me.

DANIEL SREBNICK: So, the, the best
guidance that I could provide to anyone on that,
is that whether data is on a piece of paper or
stored digitally, that data has a value, that data
has a classification. Know what you have. If
it's on an IT system, encrypt it, employ access
control. If it's on a piece of paper, put it in a
file cabinet, lock the cabinet, lock the door to
the file room. I think the, the controls are
ultimately the same; the manifestation is just a
bit different. And on the question about the
Office of Operations, we regularly work through
our Commissioner to keep them apprised of, of
issues.

COUNCIL MEMBER BREWER: Okay. I
think that your, you know, we're always wondering
in the Council, perhaps inappropriately, you know,
how do you make sure compliance takes place? And
as the Chair indicated, as a sister agency, that

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

might be a challenge. But I think you particularly indicated that through the fact that the agencies have to work with you on CityNet or other kinds of systems, that that's your stick, so to speak. Is that correct?

DANIEL SREBNICK: Mm-hmm.

COUNCIL MEMBER BREWER: In other words are you--

DANIEL SREBNICK: Yes.

COUNCIL MEMBER BREWER: --able to-- that's a very interesting stick, it's a good one. Much--

DANIEL SREBNICK: It's an interesting one. And there's another stick we have not mentioned. And we, we use it sparingly--

COUNCIL MEMBER BREWER: And you should.

DANIEL SREBNICK: --frankly.

COUNCIL MEMBER BREWER: You should.

DANIEL SREBNICK: The Department of Investigation in the Memorandum of Understanding from 2006, delegated to DoITT the authority to go in and audit agencies and how they're doing in terms of securing information. And you know,

1
2 every year we do a fairly in-depth audit of a
3 large number of agencies, and you know,
4 presumably, if we had to, if an agency was not
5 cooperative, which we, we haven't really gotten to
6 that point with anyone, we could go back to the
7 Department of Investigation and they could open
8 the door for us.

9 COUNCIL MEMBER BREWER: And you
10 don't deal with the Department of Education. I'm
11 sure you're pleased that you don't.

12 DANIEL SREBNICK: Well, the
13 Department of Education is a very large, complex
14 environment, and I mean, we work with them
15 regularly, they're our, our partners, they're IT
16 staff sits one floor above me in the building in
17 Brooklyn in which I sit. And we try to lend them,
18 you know, they run their own network, but we try
19 to run, lend them every bit of assistance and
20 support because they, they have a very difficult
21 job, and there are unique security concerns in
22 academia, and unique security concerns whenever
23 you're dealing with smart young people.

24 COUNCIL MEMBER BREWER: Yeah. I
25 [laughs] I would also add that at the end of the

1
2 year, again, the schools themselves are kind of
3 like your nonprofit agencies, and the fact of the
4 matter is that at the end of the year, we often
5 see records on the streets from schools just
6 trying to empty their closets and get ready for
7 September. I guess that's something that they
8 will continue to work on. Is that what your
9 understanding is? I mean, it does happen, there's
10 no question.

11 DANIEL SREBNICK: Yeah, I mean,
12 overall, I think it's a question of awareness--

13 COUNCIL MEMBER BREWER: Why don't
14 they buy a shredder, is what I would say, but that
15 would be my simple, non-tech response.

16 DANIEL SREBNICK: And, and
17 sometimes the answers are that simple. I think
18 it's, you know, the society is going through a, a
19 paradigm shift, and you know, several years ago
20 none of knew what Facebook or Twitter were. And
21 it is, people's lives are now so embedded and
22 dependent upon these new methods of, of
23 communication. And you know, 20 years ago
24 probably no one in this room, or few of us knew
25 what a firewall was, though encryption was

1
2 something the National Security Agency did in
3 dealing with, with our enemies. And you know,
4 attitudes change, technology changes, and the way
5 we view the world changes.

6 CHAIRPERSON CABRERA: Thank you so
7 much, Council Member Brewer. I just have a couple
8 of more questions. You mentioned that, that all
9 personal information ... are secure in cabinets.
10 Are there locations throughout the City where you
11 have certain agencies where they have storage
12 place where there're boxes of files that have
13 personal information, but they are not secure
14 within that building? And let me ask it a
15 different way. And if so, do you consider the
16 fact that the building is a secure place to be the
17 big cabinet, or do you, or what's the policy
18 regarding securing paper?

19 DANIEL SREBNICK: So, I would have
20 to defer on the records management folks from the
21 various agencies, as well as from the DORIS
22 division of DCAS. But overall--

23 COUNCIL MEMBER BREWER: They
24 haven't merged yet. Just so you know, I'm just
25 making that clear.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

DANIEL SREBNICK: Okay.

CHAIRPERSON CABRERA: [laughs]

DANIEL SREBNICK: Thank you for
the--

COUNCIL MEMBER BREWER: Hi, Eric.

DANIEL SREBNICK: Thank you for the
correction. But my, my view, to, to apply the IT
paradigm, a locked data center is not sufficient
to secure the data in the data center, you still
need to secure the data closer to where it lives.

CHAIRPERSON CABRERA: Right. No, I
say this, because I, I remember, I won't mention
the building, but visiting the building, it was,
you know, it was, it's being used for storing
paper information, and there were just boxes all
over the place, they would not being stored in
cabinets, and that was a concern of mine. What
are your views in transferring of data from one
place to another in hardware. How secure should
it be? For example, we mentioned the incident of
Bronx Lebanon. All this data, it was in a laptop
in the back--I mean, shouldn't, shouldn't it be a
cage, shouldn't this have a small cage, these
company's, have some kind of other kind of secure

1
2 mechanism to assure that if somebody tries to
3 steal this hardware, that it would make it, you
4 know, at least twice as hard.

5 DANIEL SREBNICK: Oh, I agree, the
6 security needs to be commensurate with the
7 classification of the data being transported.
8 However, if, for example, I had everyone's social
9 security number, date of birth, name and address
10 on a, on a cartridge or a USB stick, and that
11 device itself was adequately encrypted, it would
12 be of no value to anyone perhaps other than the
13 CIA or the NSA if they got ahold of it.

14 CHAIRPERSON CABRERA: Is there--I'm
15 going to ask you a silly question. Is anybody
16 else, other than the agency that you mentioned,
17 that have the ability to break in, into encrypted
18 data?

19 DANIEL SREBNICK: Well, over time,
20 encryption algorithms have been broken.
21 Typically, any encryption algorithm, no matter how
22 good it is, can probably be broken, given enough
23 time and resources. And the idea is because
24 there's a tradeoff around level of effort and cost
25 to implement technologies. We want to make things

1
2 just, just difficult enough that whoever's going
3 to be going after that data, would go look for
4 something easier than us.

5 CHAIRPERSON CABRERA: But in the
6 minds of the people, I have to tell you, that when
7 you say it's encrypted or not encrypted, it does
8 not matter. They feel that their information, if
9 it's stolen, it was stolen, and somewhere it's out
10 there. Maybe the technology will be out there
11 next year, which could possibly be, somebody, you
12 know, in the world develops some kind of
13 technology that they could easily break into
14 encryptions. I don't know. You know, I'm not an
15 expert on this field. But it's just the
16 perception, and I think that matters sometimes
17 more in the minds of people than even reality.
18 And this is why I'm a firm believer that there
19 should be a locking mechanism, I mean, it doesn't
20 cost a whole lot more to do that. And it's a
21 policy that I would love to see DoITT enforce, you
22 know, throughout these agencies whenever they're
23 transferring, because when those, 1.7 million, my
24 family's been to the hospital. And the first
25 thing came to my mind is, my info is out there.

1
2 And I don't know. I don't know where it's going
3 to end up at, I don't know if somebody could break
4 into it. So, it's something to really strongly
5 consider. I have one more question.

6 DANIEL SREBNICK: And by the way--

7 CHAIRPERSON CABRERA: Yes.

8 DANIEL SREBNICK: --I fundamentally
9 agree with you, and let me add that, for example,
10 when DoITT transports backup tapes of critical
11 City data, to a offsite storage, that you know,
12 this is typically handled by a bonded, secure
13 company that does exercise those types of
14 controls.

15 CHAIRPERSON CABRERA: Well,
16 actually, this comp--the people transporting this
17 information, supposedly they were bonded, they
18 were, you know, a company that normally does this,
19 so that, that's what's scary. [laughs] And
20 that's why I made such a hoopla about it, because,
21 you know, it, I would figure, you know, maybe in
22 my mind I was expecting too much. I figure maybe
23 they have a little cage, you know, inside of the
24 back of the car, you know, the vehicle, they do
25 this for a living. I mean, they're supposed to--

1
2 DANIEL SREBNICK: Yeah, I would say
3 your expectations are reasonable. I would expect
4 the same.

5 CHAIRPERSON CABRERA: Okay, great.
6 Let, here's my last question, unless any other
7 Council Members have any question. Is there a
8 policy on internal breaches, if any employee
9 attempts to access data, they are not allowed, or
10 not authorized to see?

11 DANIEL SREBNICK: Yeah, so, an
12 attempt is not necessarily the same as a breach.
13 Repeated, unwanted attempts are certainly serious
14 and are investigated. That's typically part of
15 the support for applications which would fall
16 under the purview of individual agencies. And I
17 cannot speak to specific cases, but I do know that
18 agencies have been know not take disciplinary
19 action against employees who have misused IT
20 resources, as they would of an employee who might
21 misuse any City resource.

22 CHAIRPERSON CABRERA: Do you have
23 any data as to how often this occurs on a yearly
24 basis?

25 DANIEL SREBNICK: No, I don't, I'll

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

have to check around and we'll get back to you and see if we have anything.

CHAIRPERSON CABRERA: I would love to know. You know, is this a recurring pattern, or is it anomalies that we have out there of a few people who might try to get information for their own benefit or for their own profit?

DANIEL SREBNICK: Well--

CHAIRPERSON CABRERA: If there are no other questions--Yes, go ahead.

COUNCIL MEMBER BREWER: I just want to know if there are any models? I do know, I have, the good news, I think the federal government pays a great deal of attention to making sure that the records of anybody, any family who's HIV positive, does not get circulated. And I've had families in that situation, and I've been pleased with the fact that their information has not been circulated between the social service, Department of Education, etc. So, and so I'm just wondering, are there models like that? I think that's what the Chair is stating, is that we want that kind of secure information, at that level. For whatever

1
2 reason, I guess because of federal law, that
3 particular designation seems to be the kind of
4 secure quality that we're looking for.

5 DANIEL SREBNICK: Agreed, and I
6 would take that and I would extend that to other
7 data elements, such as perhaps the identity of an
8 undercover police officer, the location or address
9 of a victim of domestic violence, or someone who
10 has a restraining order.

11 COUNCIL MEMBER BREWER: Right.

12 DANIEL SREBNICK: So, yeah, I agree
13 with you on all of that.

14 COUNCIL MEMBER BREWER: Okay, so
15 that is the level, though, that we're trying to
16 provide, even for other kinds of data.

17 DANIEL SREBNICK: Yes.

18 COUNCIL MEMBER BREWER: In other
19 words, is that what you're saying?

20 DANIEL SREBNICK: Yes.

21 COUNCIL MEMBER BREWER: Okay.

22 Thank you, Mr. Chair.

23 [pause]

24 CHAIRPERSON CABRERA: Well, I want
25 to thank you for coming. I'm looking forward to

1
2 working with you. And with DoITT. And thank you
3 so much, again, that was very informative. Is
4 there anyone else who has--

5 DANIEL SREBNICK: Okay, thank you
6 very much.

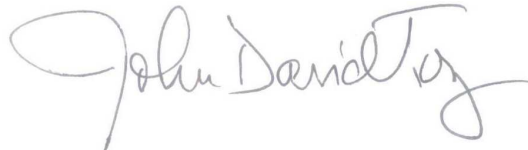
7 CHAIRPERSON CABRERA: Thank you so
8 much. All right, so this meeting comes [gavel] to
9 a happy end.

10 [background noise until end
11

C E R T I F I C A T E

I, JOHN DAVID TONG certify that the foregoing transcript is a true and accurate record of the proceedings. I further certify that I am not related to any of the parties to this action by blood or marriage, and that I am in no way interested in the outcome of this matter.

Signature

A handwritten signature in cursive script that reads "John David Tong". The signature is written in a dark ink and is positioned to the right of the printed word "Signature".

Date February 17, 2012