

1 JOINT HEARING BEFORE THE NEW YORK STATE SENATE
2 STANDING COMMITTEE ON CODES,
3 STANDING COMMITTEE ON CONSUMER PROTECTION, AND
4 STANDING COMMITTEE ON VETERANS, HOMELAND SECURITY,
5 AND MILITARY AFFAIRS
6 -----

7 PUBLIC HEARING:

8 TO ADDRESS NEW YORK STATE'S CYBER SECURITY
9 INFRASTRUCTURE, INCLUDING THE CHALLENGES, RISKS, AND
10 PROTOCOLS USED TO PROTECT STATE INFORMATION,
11 HARDWARE, SOFTWARE, AND SYSTEMS
12 -----

13 Legislative Office Building
14 Hamilton Hearing Room B
15 181 State Street
16 Albany, New York 12247

17 May 20, 2015
18 10:00 a.m. to 4:00 p.m.

19 PRESIDING:

20 Senator Thomas D. Croci
21 Chairman
22 NYS Senate Standing Committee on Veterans,
23 Homeland Security, and Military Affairs

24 Senator Michael F. Nozzolio
25 Chairman
NYS Senate Standing Committee on Codes

Senator Michael Venditto
Chairman
NYS Senate Standing Committee on Consumer Protection

PRESENT:

Senator Joseph P. Addabbo, Jr.
Senator Simcha Felder
Senator Martin J. Golden

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

SPEAKERS:	PAGE	QUESTIONS
Jamie Brown Director of Global Relations CA Technologies	14	23
Donald Freese Director National Cyber Security Advisory Board	49	60
Dr. Peter Bloniarz Executive Director New York State Cyber Security Advisory Board	76	87
Richard Dewey Executive Vice President New York Independent System Operator	112	120

1
2 SENATOR CROCI: My name is Senator Tom Croci.

3 I want to thank you all for joining us today.

4 I'm the Chair of the New York State Senate
5 Standing Committee on Veterans, Homeland Security,
6 and Military Affairs.

7 Welcome to our public hearing on cyber
8 security.

9 This is a joint public hearing today, in
10 cooperation with my colleagues,
11 Senator Mike Nozzolio, Chairman of the Standing
12 Committee on Codes, and, Senator Michael Venditto,
13 the Chairman of the Standing Committee on
14 Consumer Protection.

15 I'm also joined by my distinguished
16 colleagues, Senator Marty Golden;
17 Senator Joe Addabbo, who is the ranking minority
18 member of the Committee on Homeland Security,
19 Veterans, and Military Affairs.

20 Senator Simcha Felder has also joined us
21 today.

22 And I would like to thank all of the staff
23 and members who have come today to highlight the
24 importance of what we're doing.

25 Recently, ISIS put out a video on the web,

1 threatening a cyber attack on the United States.

2 And this just underscores why we're here
3 today, and why it's so important that the government
4 talk about the issues facing our nation and our
5 state.

6 Simply put, we're public servants, and public
7 safety in the protection of our people in the state
8 of New York should be our mission focus. Our
9 critical infrastructure should also be a part of
10 that focus.

11 In our modern world, some of the most
12 devastating weapons in this day and age aren't
13 bullets and armed bombs, but they're electrons.
14 And, certainly, the collective power of all the
15 mobile devices that are in this room right now
16 underscore just how critical those electrons could
17 be if they were turned into a weapon.

18 An indispensable link in our modern world is
19 our computer networks, and they are systems that are
20 interconnected more so every day.

21 Cyber security and cyber threats are a
22 critical challenge for our state's public
23 protection.

24 We're here, all my colleagues and I, to
25 ensure that our state's cyber-security efforts are

1 up to, and are addressing, that challenge.

2 This is one of a series of hearings that
3 we'll -- that has been conducted, and will be
4 conducted, by the Senate on this issue.

5 Today's hearings will focus on what the
6 State of New York should be doing as a governmental
7 entity to address the challenges that we're all
8 facing.

9 We'll hear from four distinguished witnesses
10 today, and I want to thank them all for joining us
11 today. They'll help our Committees continue to
12 build our understanding of this complicated topic.

13 Obviously, my colleagues and I are concerned
14 about it, or we wouldn't be here. We've invited
15 many key leaders in both state departments and
16 agencies. We haven't heard from them as far as
17 their attendance here today. This heightens our
18 concern, but we look forward to hearing from them in
19 the future, and working with us on these important
20 issues.

21 Our cyber-security efforts in the state are
22 of critical importance. We are as large as many
23 countries in this world.

24 Over the past few years there have been
25 questions raised, both at the national level and the

1 state level, about our preparedness in some of these
2 areas, and that those questions also apply to
3 New York State.

4 In -- two years ago in the budget cycle, the
5 Executive removed the cyber-security
6 responsibilities from the control of the State
7 Division of Homeland Security Emergency Services,
8 and placed it under the control of the State Office
9 of Technology Services.

10 These and other questions are things that we
11 should pursue, discuss, and make sure that this
12 state is following the best practices that we have
13 at the national level.

14 This was -- this was a decision done, despite
15 the fact that, certainly, the vision of
16 Homeland Security Emergency Services has an
17 excellent track record, a very highly professional
18 track record, of working in keeping us safe in
19 New York, and is currently very capably led by
20 Commissioner John Melville.

21 Today we seek to clarify precisely what our
22 posture is, and we will continue to do so until we
23 have a coherent posture that we believe well
24 addresses the challenges we face.

25 In addition to the previous public hearings,

1 budget hearings, we also passed in the Senate very
2 important pieces of legislation, four, to improve
3 New York's cyber-security protection, threat
4 prevention, response, and recovery, and to properly
5 assess the status of Executive Branch efforts in
6 this area.

7 I won't read all of the bills, but I will say
8 that the bills include Senate 3405, which would
9 require executive agencies responsible for cyber
10 security to perform a comprehensive review of all
11 cyber-security services every five years.

12 It's always nice to have a benchmark of where
13 you started, and where you are.

14 In addition, Senate 3407 establishes the
15 New York State Cyber-Security Initiative. This bill
16 would establish a New York law, a cyber-security
17 initiative, very similar to that established by the
18 federal government in 2013.

19 Senate 3404 would create new crimes of cyber
20 terrorism in the first and second degrees in the
21 state of New York.

22 And, finally, Senate 3406, which would create
23 a new crime of criminal possession of
24 computer-related materials in the first degree.

25 We have to use any tools that we have at our

1 disposal to address the coming threat.

2 And these important forums are just the
3 beginning. Along with Senator Nozzolio and
4 Senator Venditto, and my other colleagues, our
5 Committees are dedicated to achieving real results,
6 something palpable, that we can have in place before
7 it becomes a situation in our country and in our
8 state that's unmanageable.

9 I know that working with the departments and
10 agencies, and certainly my colleagues, that we're
11 all singularly focused on this vision.

12 We're hopeful that in the days and the weeks
13 ahead that the Executive Branch will share this
14 vision and work with us towards this goal.

15 This issue is too important, and until our
16 state government -- all branches, departments, and
17 agencies -- are acting under a coherent and unified
18 approach, we will always remain at risk.

19 I want to thank you very much, and I'll, at
20 this point, turn it over to Senator Nozzolio.

21 Senator.

22 SENATOR NOZZOLIO: Thank you very much.

23 Thank you very much, Senator Croci.

24 In the few short months that you have served
25 in the State Senate, you have taken a very important

1 leadership role in ensuring our government -- our
2 state government has in place the protocols
3 necessary to protect the citizens of our state.

4 And, as the government is entrusted by those
5 citizens with very important data, as well as very
6 important system information, that affects their
7 lives, your efforts are exemplary in beginning the
8 process of protection.

9 Senator Venditto, also here only for a few
10 months, but has already taken a very important role
11 in ensuring that consumers in our state have the
12 privacy protections necessary, and the reliance --
13 when they do business with the commercial
14 enterprises in this state, a reliance that those
15 commercial enterprises will, in fact, protect their
16 data and the data necessary.

17 As the intersection of both of those
18 objectives, as we look to the criminal-penalty
19 section of our criminal codes, we also, the three of
20 us in particular, are working to ensure that those
21 who are victims of a cyber attack are not further
22 victimized by the process; that we are looking in a
23 lot of different areas to protect government,
24 information, information that's in the custody of
25 government.

1 And thank you the again, Senator Croci, for
2 your leadership in that endeavor.

3 The Attorney General of the State of New York
4 has a measure that we are analyzing, that will take
5 a lot of scrutiny.

6 The scrutiny begins in our meetings that
7 we've had with a lot of different individuals and
8 enterprises over the past few months. But we also
9 will be using these hearings as an opportunity to
10 look at various approaches on data security, in
11 looking at it with a multitude of lenses, to ensure,
12 again, I think the bottom line is that those who are
13 injured aren't further victimized by a process.

14 So, having said that, I welcome those who
15 came, near and far, to testify today.

16 This is the beginning of a very serious
17 deliberation on a very serious issue; and,
18 particularly, New York, which is an international
19 hub of commerce and industry, has certainly -- has
20 the important necessity to take a leadership role in
21 this entire issue.

22 So, thank you to my colleagues for their
23 attention.

24 SENATOR CROCI: Thank you, Senator.

25 Senator Venditto.

1 SENATOR VENDITTO: Senator Croci, thank you
2 so much for the introduction; and, of course, for
3 your efforts in organizing today's event.

4 And thank you, of course, to Senator Nozzolio
5 for his ongoing efforts to keep us moving forward in
6 this very, very important topic.

7 Thank you to my fellow Senators for being
8 here, everyone being present; and, of course, to our
9 presenters, who we're very eager to hear from.

10 You know, we're becoming more and more
11 reliant on the Internet each and every day in our
12 country, and rightfully so, as it provides many
13 advantages to us.

14 We do, however, want those who use the
15 Internet, our consumers, to do so, and we want them
16 to use it without any fear or anxiety of any threats
17 that are out there.

18 And that's the reason why we're assembled
19 here today: to protect our consumers, to protect the
20 residents of our state.

21 I think we're taking a very important step in
22 what is going to be a long journey, but I believe a
23 successful journey, in making these good things
24 happen.

25 So without further ado, I'm hoping to hear

1 from our presenters.

2 And, again, Senator Croci, thanks to you, and
3 I'll kick it back to you now.

4 SENATOR CROCI: Thank you, Senator.

5 And, Senator Golden.

6 SENATOR GOLDEN: I would like to thank
7 Senator Croci as well for holding this hearing, and,
8 of course, all of my colleagues here today.

9 This is the first of two legislative events
10 here in Albany.

11 My office has had several conversations with
12 people in the industry over the last several months,
13 and I've introduced two bills for additional comment
14 and discussion.

15 I'm also sponsoring critically important
16 measures, with Senator Croci, and I look forward to
17 this hearing and comments today.

18 Some of us, obviously, will be in and out
19 because of other hearings going on this morning, but
20 it's important that we have this hearing, and the
21 next hearing as well, so we can take the proper
22 measures to make sure that security measures are in
23 place.

24 The majority of attacks are on three
25 sectors -- public, information, and financial

1 sectors -- but all sectors are vulnerable.

2 According to the Verizon 2015 Data-Breach
3 Investigation Report, and this is one company, there
4 were almost 80,000 security incidents in 2014, with
5 400 million in losses from just over 700 compromised
6 records.

7 And this is a partial report, as not all
8 entities responded this year, and not all entities
9 have given its full data.

10 The key issue is to figure out how to help to
11 protect individual entities, public and private,
12 from the attacks and the breaches.

13 Not every incident is a breach.

14 The issues of data breach, online privacy,
15 and Internet safety are tied to each other.

16 Breaches compromise individual privacy and
17 security, and may lead to directly to loss of data,
18 and directly loss of financial losses.

19 Information in the key area for handling
20 threats. As consumers don't know that a system has
21 been breached, they cannot react.

22 This is important, because the Verizon report
23 also shows that the movement from Victim 1 to
24 Victim 2 takes place in less than 24 hours.

25 Larger companies and entities have resources,

1 but these can be improved.

2 And, clearly, we need a better way of helping
3 consumers and smaller businesses protect themselves.

4 My community alone have seen it spread within
5 2 days to about 16 different store, to the losses of
6 almost \$700,000 in one small community just last
7 year.

8 We should better criminalize certain kinds of
9 behavior -- denial of service, intrusion, cyber
10 theft, and others -- and we should protect the
11 rights of consumers and assure that they have
12 sufficient information to make good choices.

13 I look forward to this hearing, Chairman, and
14 colleagues, and the opportunity to work with you to
15 create the perfect legislation, or the best
16 legislation that we can, to address these issues.

17 Thank you, Mr. Chairman.

18 SENATOR CROCI: Thank you, Senator Golden.

19 Would anyone else like to (inaudible)?

20 With that, we'll move on to our first
21 witness.

22 We're very pleased to have Mr. Jamie Brown,
23 director of global relations for CA Technologies.

24 If you would join us.

25 Of course, CA Technologies is well known, a

1 giant, as far as corporate entities in the state of
2 New York.

3 We're very proud that they are a New York
4 company, and they are a global leader in computer
5 software and technology.

6 They've been around for a long time, and they
7 are resident experts in the field.

8 Mr. Brown, we're very happy to have you
9 here today, and, we look forward to your comments.

10 JAMIE BROWN: Great. Thank you very much.

11 Chairman Croci, Nozzolio, Venditto; Ranking
12 Member Addabbo, and Senators Golden and Felder:

13 CA Technologies appreciates this opportunity
14 to provide testimony at today's hearing to address
15 New York State's cyber-security infrastructure.

16 My name is Jamie Brown, and I serve as
17 director of global government relations for CA,
18 where I manage cyber security, privacy, and
19 cloud-computing policy issues.

20 I'm also a native of the Ithaca area, and
21 very happy to be back in New York State today.

22 CA was founded in 1976 on Long Island, and
23 has grown into a Fortune 1000 enterprise-software
24 company that serves customers around the world.

25 We currently have more than 1500 employees in

1 our Long Island and Manhattan offices.

2 CA's software and solutions help our
3 customers thrive in the new-application economy by
4 delivering the means to deploy, monitor, and secure
5 their IT applications and infrastructure.

6 The threats we face in cyberspace are real
7 and growing.

8 In today's application economy, virtually
9 everything we do happens through digital platforms
10 and these systems are constantly under attack.

11 Cyber attacks that disable
12 critical-infrastructure systems, such as the
13 electric grid, water utilities, financial markets,
14 and even mass-transit systems, could have a
15 potentially catastrophic effect, putting the health
16 and safety of large populations at risk.

17 Given New York's vital position in all
18 sectors of our economy, the state's critical
19 infrastructure is a key potential target for these
20 types of cyber attacks.

21 The key for state, federal, and global
22 policymakers is to develop policies that enable the
23 promise and innovation of new technologies, while
24 also protecting customer privacy and improving
25 security.

1 CA believes there are common principles that
2 lawmakers can apply in cyber-security policies,
3 including stakeholder engagement, flexibility, and
4 global approaches.

5 First, cyber-security policies should be
6 developed in partnership with public and private
7 stakeholders.

8 Stakeholder engagement ensures that different
9 perspectives and experiences are weighed in policy
10 development, and it encourages greater participation
11 and buy-in as policies go into effect.

12 At the federal level, President Obama tasked
13 the National Institute of Standards and Technology,
14 or "NIST," with developing a cyber-security
15 framework to reduce cyber risks to critical
16 infrastructure using an open public-review process.

17 Industry, academic, non-profit, and
18 international and state government officials
19 participated in public workshops on the framework
20 and contributed responses to requests for
21 information.

22 CA was also an active participant in this
23 development process.

24 Ultimately, when NIST released its framework
25 in February of 2014, it did so, having solicited and

1 incorporated significant input from a range of
2 stakeholders that helped to build broad support for
3 the framework.

4 We encourage New York State to leverage the
5 work that has already been completed through the
6 NIST framework process to the greatest extent
7 possible.

8 The State Senate recently considered S-3407,
9 which was sponsored by Chairman Croci, and passed
10 the Senate with a strong bipartisan vote.

11 As the legislative process moves forward, we
12 recommend adding statutory language to S-3407,
13 advising the Division of Homeland Security to
14 actively engage with public and private
15 stakeholders, and, to leverage the NIST framework,
16 to the extent possible, in the development of the
17 New York State cyber-security framework.

18 S-3407 also calls for the establishment of a
19 New York State Cyber Security Advisory Board.

20 CA believes recommendations on board
21 appointments should reflect the diverse array of
22 public and private stakeholders, including
23 representatives from industry, academia, government,
24 standards-development organizations, and other key
25 cyber-security stakeholders.

1 Further, S-3407 calls on state divisions to
2 make recommendations on the feasibility, security
3 benefits, and relative merits of incorporating
4 security standards into acquisition planning and
5 contract administration.

6 This is another area where policymakers can
7 engage with public and private stakeholders who best
8 understand the diverse risk environments of
9 customers and the unique solutions of providers.

10 The second cybersecurity-policy principle is
11 flexibility.

12 Flexibility in policy allows for adaptability
13 in security approaches.

14 While there are some common cross-sector
15 elements to basic information-security programs,
16 there are also significant differences in the threat
17 environments, assets, and business missions amongst
18 critical-infrastructure owners and operators.

19 Flexible, goal-oriented cyber-security
20 policies, rather than specific technology mandates,
21 can best help these organizations optimize their
22 security postures.

23 S-3407 states that the New York State
24 cyber-security framework shall provide a
25 prioritized, flexible, repeatable performance-based

1 and cost-effective approach.

2 We strongly commend the bill's authors for
3 adding this provision.

4 The third principle to apply, is to utilize a
5 global approach in cyber-security policy.

6 Policy to address cyber threats must allow
7 for the use of technologies that align with
8 international market-driven standards.

9 This enables technology companies to focus
10 their resources on enhancing security solutions that
11 can scale for the global market, rather than on
12 making a multitude of adjustments to ensure
13 compliance with a series of static requirements and
14 specifications.

15 S-3407 calls for the New York State
16 cyber-security framework to incorporate voluntary
17 consensus standards and industry best practices to
18 the fullest extent possible.

19 We believe that this is very important for
20 effective cyber security.

21 CA believes that cyber-threat information
22 sharing is an effective tool in helping
23 organizations address the volume, variety, and
24 sophistication of today's cyber attacks.

25 S-3407 tasks the Division of Homeland

1 Security with developing procedures, methods, and
2 directives for a voluntary information-sharing
3 program.

4 CA believes there are a series of policy
5 principles that are necessary components of any
6 successful cyber security information-sharing
7 program.

8 First, the policies should encourage the
9 development and deployment of automated mechanisms
10 to share information in as close to real-time as
11 possible.

12 Once cyber-threat indicators are discovered,
13 this information must also be disseminated rapidly
14 to allow organizations that are the subject of
15 attacks to mitigate against attack effects, and,
16 also, to allow other organizations that haven't been
17 attacked yet to prioritize their defenses.

18 Second, organizations should have targeted
19 liability protection for the data they share or
20 receive. This protection will encourage greater
21 participation in the program, leading to better
22 cyber defense.

23 And, third, legislation should require
24 organizations to take reasonable steps to remove
25 personally-identifiable information of individuals

1 not related to the threat from any cyber-threat
2 information they share through the program. This is
3 vital to protect the privacy of customers and
4 citizens.

5 With respect to protecting the state's own
6 information systems, it's important to find the
7 right balance between effective coordination of
8 cyber-security activities and division flexibility.

9 The New York State Senate recently passed
10 S-3405, which requires the commissioner of
11 Homeland Security to prepare and deliver a
12 comprehensive report on state cyber-security needs,
13 and the ways those needs are being met.

14 This report will help policymakers better
15 understand the risk environments facing state
16 institutions, and will help state divisions
17 benchmark their information-security practices
18 against those of their peers.

19 However, while this coordination is
20 important, state division information-security
21 officers should maintain a level of flexibility on
22 the best means to protect their systems.

23 Policies to safeguard state systems must be
24 risk-based, and enable the use of new technologies
25 and solutions to address evolving risks.

1 Some state governments, including Virginia
2 and Pennsylvania, have committed to adopting the
3 NIST cyber-security framework, or to mapping their
4 own security protocols against the NIST framework.

5 We recommend New York State also consider
6 leveraging the NIST framework to protect its own
7 information systems.

8 Cyber security represents a significant
9 challenge for industry officials and for state,
10 national, and global policymakers.

11 CA applauds the efforts you have taken in
12 tackling the key cyber-security issues of
13 critical-infrastructure protection, cyber-threat
14 information sharing, and protection of state
15 information systems.

16 We stand ready to partner with you in, both,
17 the remaining legislative process, and on effective
18 implementation of New York State's cyber-security
19 policies.

20 Thank you very much for the opportunity to
21 testify, and I look forward to answering any
22 questions you may have.

23 SENATOR CROCI: Thank you, Mr. Brown.
24 I appreciate that testimony.

25 You preempted a lot of my questions in your

1 testimony.

2 But, could you give -- for those who are
3 outside of the business, and the policy-wonks in the
4 room, can you give us a practical application, based
5 on software applications that CA currently works
6 with or provides to the state, what would be a
7 practical application of a vulnerability that would
8 affect a statewide system or users or state
9 employees?

10 JAMIE BROWN: Thanks.

11 Well, very good question.

12 And I think, you know, in today's
13 cyber-security world, you know, we talk about there
14 no longer being a perimeter. You don't really set
15 up walls anymore, you know, that can be breached.

16 Instead, from CA's perspective, identity is
17 the new perimeter, and identity management is going
18 to be extremely important, moving forward, both
19 identity and access management.

20 So what are the effective tools that can help
21 authenticate individuals as they are on systems,
22 and, also, what is the right level of access that
23 they should have to different -- you know, to
24 different data or systems within -- you know, within
25 public systems?

1 So, I mean, CA, you know, for example, does
2 provide identity- and access-management solutions.
3 And one of things we're actually working on, moving
4 forward, is moving away from just user name and
5 password as authentication.

6 I mean, that's been, you know, passwords
7 oftentimes are saved in databases, and those can
8 be -- you know, those can be hacked, and corrupted,
9 and then, therefore, you know, given to bad actors.

10 We're working, actually, you know, on a
11 program that NIST administers, called the "National
12 Strategy for Trusted Identities in Cyberspace,"
13 trying to identify, you know, new means of
14 authentication that can prove that this individual
15 is who he or she says he is, or, as we move into the
16 Internet of thing, that this thing that's
17 communicating is, you know, what it says it is, and
18 then also applies the right amount of access to
19 databases, based on that.

20 SENATOR CROCI: So are there tools right now
21 that state employees would use or state systems are
22 utilizing in that area?

23 JAMIE BROWN: Well, yes.

24 So, I mean, we -- you know, we provide
25 identity- and access-management software that, you

1 know -- that, you know, enables the right amount of
2 access, you know, to state systems. We have a
3 number of state customers that are using these
4 identity-management systems.

5 And, you know, I think, you know, from our
6 perspective, we follow the ISO 27001 standard in
7 identity-access management. And, you know, this is
8 what we apply in our tools, and we think that
9 they've been very effective tools in preserving, you
10 know, the right amount of identity access for
11 New York State systems.

12 SENATOR CROCI: And the -- CA is obviously
13 well-linked with our federal partners, and,
14 certainly, working through the NIST framework.

15 Are you -- are you concerned that there are
16 holes or gaps that the states are not filling in
17 order to meet those standards, and certainly
18 New York?

19 And are there industry leaders, private
20 entities, corporations, who are providing protection
21 to states or monitoring these things for states in
22 another setting in other states?

23 JAMIE BROWN: Well -- so, I think it's -- I'm
24 glad you brought up the NIST framework, because what
25 I think where that helps, in particular, is getting

1 stakeholders, you know, both providers and
2 customers, to use common terminology to get on a
3 common lexicon.

4 Right now, I think what you have is a number
5 of different -- you know, a number of different
6 institutions that are setting up their own security
7 postures, but, what's lacking is, perhaps, the best
8 coordination, and I think, you know, being able to
9 share best practices, you know, being able to
10 leverage, you know, common platforms across
11 different institutions.

12 And I think, you know, what the NIST
13 framework does, is it allows, again, different
14 actors, you know, to at least set a common baseline
15 to use a common set of terminologies across the
16 organization as to, Okay, what are the different
17 practices we can be taking in cyber security?

18 And this works both in states, you know, and
19 at the federal level, and, certainly, for
20 critical-infrastructure owners and operators.

21 And -- you know, so while it puts them -- you
22 know, allows them to use this common terminology, at
23 the same time, it is still gives them the
24 flexibility to identify, you know:

25 What are our most important assets?

1 What is the unique threat environment that we
2 face?

3 Based on that, how do we then prioritize, you
4 know, our limited budget spends so that we're using
5 the most effective manner?

6 So it is a combination, what the NIST
7 framework does, and I think that the states,
8 including New York, can take advantage of, is, you
9 know, get on a common platform using the same
10 terminology, but, maintaining, you know, that
11 specific flexibility, both, at the state level, and,
12 certainly, within different state institutions, you
13 know, to come up with their best risk-management
14 practices.

15 SENATOR CROCI: But the resources are out
16 there and available to the state of New York?

17 JAMIE BROWN: They are -- they are. You
18 know, both CA, and, certainly, many other providers,
19 you know, are at the forefront of a lot of new
20 security technologies that are available.

21 And I think, you know, what is needed is the
22 right level of coordination, leveraging of common
23 platforms. But, then, you know, above that, that
24 flexibility, and sort of mission -- mission-oriented
25 approach to choosing, What are our right

1 cyber-security priorities?

2 SENATOR CROCI: Thank you.

3 And I'll turn it over to my colleague
4 Senator Nozzolio.

5 SENATOR NOZZOLIO: Thank you, Senator Croci.

6 Mr. Brown, thank you very much for your
7 participation and your testimony.

8 And, it's also great to see a fellow Cornell
9 alumnus who's made good, as well as an alumnus from
10 Capitol Hill.

11 So, we appreciate your variety of insights
12 into this process.

13 Your testimony is very helpful. It sets a
14 very good template from which to act.

15 Have you had an opportunity to review a
16 New York State Senate proposal, 4887, that
17 Senator Venditto had introduced on behalf of the
18 Attorney General, for us to be able to analyze the
19 Attorney General's proposals regarding the
20 Data Security Act?

21 Have you had an opportunity to review that at
22 all?

23 JAMIE BROWN: I have not at this point.

24 SENATOR NOZZOLIO: I -- and, certainly, it
25 would be nice if you could have that -- take that

1 opportunity in the next few weeks, and to be able to
2 guide us on any particulars that you see make sense,
3 and don't make sense.

4 One of the things that makes sense from your
5 testimony and your recommendations has been to do
6 all we can to use the NIST framework -- N-I-S-T,
7 framework -- in terms of ability to govern.

8 And that was -- that is something that is a
9 positive about the Attorney General's proposal.
10 And -- but we'd like to have your input as to
11 whether or not you think it goes far enough, or
12 maybe too far.

13 There are some proposals, that I won't
14 belabor today, that really give us great concern,
15 and one of them is contrary to your recommendation,
16 in the sense that you're asking our Legislature to
17 look at an approach that's flexible, in the sense of
18 one size doesn't fit all. I think that's what
19 I gleaned from some of your remarks.

20 And that's a problem we have with the
21 Attorney General's proposal; that it, in fact, is a
22 one-size-fits-all approach. Whether it's a huge
23 user of consumer data, whether it be a big-box
24 store, or an insurer, or whatever, the same laws
25 would govern that person, and enterprise, than the

1 single-proprietor sewing shop that happens to have
2 personal data and information.

3 So it's a -- we have a broad variety of
4 commerce to help establish a framework for.

5 And the flexibility part, something you --
6 that was weaved throughout your testimony, and
7 I think certainly appropriately, we need your
8 thoughts on how we can manage a flexible system of
9 law that it does respond to the commercial
10 differentials that we have in society.

11 Is that, in your knowledge, being worked on
12 by the Congress of the United States?

13 JAMIE BROWN: So, the Congress of the
14 United States, I took the NIST framework, and just
15 last year, you know, past legislation that
16 statutorily puts in place the process, you know,
17 through which the director of NIST should be working
18 with industry stakeholders to come up with a common
19 set of, you know, standards and best practices that
20 would be voluntary.

21 You know, that's, I think, another key point,
22 certainly early on, as, you know, cyber security is
23 such a big topic, and, again, the array of customers
24 are so diverse as well, that -- so that opportunity
25 to, you know, pick certain provisions to weigh your

1 own security practices against that, I think -- and
2 to learn lessons, it's really important, you know,
3 both, you know, the voluntary nature there at the
4 federal level, but then, also, the flexibility is
5 key.

6 And there is a balance between coordination
7 and flexibility, you know, that -- you know, we
8 would recommend to any, you know, state government,
9 including New York, to take.

10 But, you know, ultimately, you know, our
11 feeling at CA is, right, one size does not fit all
12 when it comes to cyber security. And, you know,
13 while there might be a common platform, and perhaps
14 some goals that are set out, the means to address
15 that, and perhaps the specific requirements in that,
16 you know, should enable a -- you know, a limited
17 amount of flexibility.

18 And with respect to Senator Venditto's
19 proposal, yes, we'd be happy to take a look at that
20 and provide follow-up comments if that's helpful.

21 SENATOR NOZZOLIO: And the Attorney General
22 can't introduce legislation by himself. It only can
23 be a member of the Legislature.

24 And Senator Venditto, as an opportunity and
25 service to the rest of the Senate, introduce the

1 measures so that we can analyze it.

2 One of the proposals of the Attorney General
3 is to have the authority to fine up to \$50 million,
4 in terms of penalties, even without a showing of
5 financial loss.

6 So it's, certainly, if there's a data breach,
7 a company, an enterprise, would -- could face a
8 \$50 million fine, without so much as a -- any
9 financial loss either, too.

10 So we have a concern, how do you -- how do --
11 with such a huge amount of penalty, how do you
12 encourage voluntary participation once a breach
13 occurred?

14 JAMIE BROWN: Well, in data breaches, and
15 data-breach reporting requirements, are certainly,
16 you know, a big issue that's being covered both
17 amongst different states and at the federal level.

18 Right now, I think there -- you know, there
19 are 47 different standards set by the states,
20 including 4 more, I think, of U.S. territories, you
21 know, which creates some obstacles and some
22 difficulties for organizations then to have to
23 manage and deal with that.

24 A large organization like CA, we can do that.
25 You know, we have a big legal department. We

1 understand and compliance in different states.

2 As you mentioned, smaller organizations that
3 also do business across state lines, being able to,
4 you know, maintain compliance there is difficult.

5 And on the penalty side, you know, I think
6 one point that we like to stress is that, when a
7 data breach occurs, you know, we like to remind
8 stakeholders that we are also victims of a crime.

9 It is certainly in our interests not to get
10 breached. And, you know, while CA, you know, both,
11 has excellent security measures for our own
12 information systems, and provides them, you know,
13 for other organizations, it can be difficult for
14 smaller organizations to -- you know, to be able to
15 purchase something.

16 So I know that's something that, you know,
17 different organizations are looking at: What are
18 effective security tools for smaller organizations?

19 And, you know, again, when it comes to the
20 size of penalties, you know, something that is very
21 large, maybe \$50 million, for a small or
22 medium-sized business could bankrupt them.

23 And, you know, again, I think keeping in mind
24 that they, too, are -- you know, that they are the
25 victims of a crime, and, you know, do not want to

1 incur breaches, you know, but then to encourage them
2 to sort of tackle goal-oriented approaches to -- you
3 know, to improve their security, and to notify the
4 appropriate authorities, you know, when they are
5 preached, is important.

6 It's something that we'd be happy to work
7 with you on. And I know a number of small-business
8 groups probably would as well.

9 SENATOR NOZZOLIO: Thank you for your input
10 and your responses, and your continued volunteering
11 for analysis over time.

12 And thank you for your participation.

13 SENATOR CROCI: Thank you, Senator.

14 Senator Venditto.

15 SENATOR VENDITTO: Senator Croci, thank you.

16 And thank you again, Mr. Brown, for your
17 testimony and for your presence here today.

18 Just following up on kind of what we were
19 talking about here in the discussion, I mean,
20 obviously, at the end of the day, the -- and, by the
21 way, we are, of course, working with the
22 Attorney General's Office on the legislation.

23 It would be great to sit down as we go
24 forward in the process, to continue to craft it,
25 because we are taking input along the way, and

1 making sure that we come out with a finished product
2 that is reasonable, and that we can all -- you know,
3 all agree upon, going forward.

4 So that would be great to follow up there.

5 Just, in terms of striking that balance,
6 I guess you would call it, you know, we want to
7 protect our users, we also want to protect the
8 companies here. And, you know, the last thing we
9 want to do is deter companies from reporting these
10 breaches. We want to, if anything, create an
11 incentive for them to do so, and that's going to
12 benefit all the parties involved.

13 So just kind of flushing this out a little
14 bit more, is there anything specifically that you
15 can think of now that might create that incentive,
16 rather than a deterrent, in this situation?

17 JAMIE BROWN: It's an excellent question.

18 And, you know, I do think, one of the things
19 I had mentioned in my testimony is the targeted
20 liability protection. I mean, not overly-broad, but
21 instead, you are trying to encourage participation
22 in this program to share information on cyber
23 threats.

24 And, you know, as some organizations start
25 getting attacked, you know, we want to make sure

1 that that information gets to others so that they
2 aren't also attacked, and, you know, so that they
3 can also then rely on appropriate, you know, state
4 and federal and local authorities to help them to
5 mitigate the effects of the -- for those that are
6 attacked, to help them to mitigate those effects.

7 So, you know, I do think, you know,
8 information sharing, cyber-threat
9 information-sharing programs, are important an
10 component to help in that regard.

11 I do think if organizations feel secure, that
12 when they are sharing what they see as anomalous
13 activity that could indicate a threat, you know,
14 that that won't then be turned around, you know, and
15 used against them, you know, for either liability
16 or, you know, a lawsuit, or what have you.

17 And then, you know, on the data-breach side,
18 there are -- there are requirements right now for
19 that notification.

20 I think, you know, ensuring that
21 organizations have the time, first, to investigate
22 the nature of the breach, and to be able to take
23 reasonable steps to mitigate the effects, and to
24 secure their systems, giving them, you know, the
25 right amount of time to do that before then having

1 to notify, that is also important, because you don't
2 want to put out vulnerabilities or threats that have
3 happened if that vulnerability still exists, and if
4 it exists on other -- you know, organizations'
5 systems.

6 So I think taking that reasonable time,
7 though, certainly, quickly, to investigate the
8 nature of a breach, to patch holes, to mitigate
9 effects, share that information across the community
10 so that others can also take advantage of that, and
11 then provide the notification, I think would be
12 helpful.

13 SENATOR VENDITTO: And I appreciate that
14 answer.

15 And that is the goal here, to create that
16 secure environment where we can be, you know,
17 forthright when these breaches do happen.

18 So, thank you for your testimony again, and
19 for all the input that you gave us today.

20 SENATOR CROCI: Thank you, Senator.
21 Senator Golden.

22 SENATOR GOLDEN: Thank you, Mr. Chairman.
23 And thank you for your testimony here today.

24 But, I believe it's so tremendous out there,
25 the costs comes down to us. The people that live in

1 this great city and state, and great nation, they
2 pay the bottom line on these breaches.

3 The Simple credit cards, no chips; right?

4 JAMIE BROWN: Yeah.

5 SENATOR GOLDEN: Now we got a law coming out,
6 we're going to put chips in them.

7 But, they're already getting ahead of that,
8 I understand; right? They have a way of getting
9 around the chip as well.

10 But here's the Simple card.

11 There's a Simple card that was used in my
12 community, and they went into one store, and,
13 supermarket, and they were able to circumvent the
14 hardware and the software, and it cost a tremendous
15 amount of money for that one store.

16 But here's the problem: That store doesn't
17 report it -- that store was the only -- excuse me,
18 that was the only store that reported it.

19 The other stores did not report it. They
20 don't want it out there in the community that their
21 systems have been breached, because they don't want
22 to hurt their businesses. Nobody finds out about
23 it. They let these breaches go on. And then they
24 pay out of their -- the bank cards pay their --
25 those that have been breached, so we never get a

1 police report, we never see a newspaper report. We
2 never see anything.

3 And by the time this has happened in the
4 community, you can hit a community for six,
5 seven hundred thousand dollars overnight, and
6 they're gone.

7 We need to do more in getting the reporting
8 of that breaching.

9 How do we do that?

10 I know, right, we've asked that question
11 probably four different ways here today, and I want
12 to, you know, commend my colleagues, but, we have to
13 do something to get this reported in a way that we
14 noted it's going on, and to the extent that it's
15 going on.

16 JAMIE BROWN: Yeah, and I would -- I mean,
17 I think breach-notification requirements themselves
18 are perfectly appropriate.

19 And I think the key -- you know, and
20 important.

21 And I think the key there is the timing, and
22 then the methods, you know, through which to help
23 others, as you say, you know, so that, you know, if
24 these aren't being reported, to help others protect
25 their systems.

1 And one of those is, you know, in S-3407,
2 I do think the information-sharing provisions will
3 be very helpful.

4 I would also encourage state authorities to
5 look at -- you know, at the federal level, they
6 are -- they're setting up a new information-sharing
7 and analysis organization's, you know, network of
8 information sharing, allowing, you know, both on the
9 state level, and then, certainly, you know, state
10 entities or private entities within the state to
11 consider participating in that.

12 And then, you know, it is appropriate,
13 obviously, on data breaches, not just to notify
14 customers, but to notify the appropriate authorities
15 as well who have some of the tools to help -- to
16 help make these patches.

17 And, again, I would go back to say, Okay,
18 I would not make public notice until you have taken,
19 you know, reasonable steps, you know, in an
20 expeditious fashion to patch those breaches, you
21 know, and to begin to secure your systems again, so
22 that you're not putting out there, Hey, you know,
23 here's a vulnerability that we had that we haven't
24 patched yet. Keep coming -- keep coming at us, to
25 the bad guys.

1 But, you know, a combination of effective
2 information sharing, you know, there have to be
3 those requirements to certain state authorities so
4 they can take steps to help.

5 And then, also, you know, the protections so
6 that companies feel secure in sharing
7 organizations -- or, excuse me, sharing information
8 across other -- you know, other peer organizations
9 so that they can, you know, take advantage of that
10 new threat knowledge, I think would be very helpful.

11 SENATOR GOLDEN: I'm talking about large
12 retailers as well.

13 JAMIE BROWN: Yeah, sure.

14 SENATOR GOLDEN: I'm talking about stores
15 with the hardware, and software should have been
16 updated, and wasn't updated. They just let it go,
17 and let the system exist, and not go for the extra
18 money that's required to update that hardware and
19 software.

20 JAMIE BROWN: Well, and in those cases,
21 right, obviously, there was a -- a very significant
22 breach that happened, you know, last year to a large
23 retailer.

24 And I think, in many ways, that was a
25 game-changer, from a market perspective.

1 I mean, the motivation -- the cost to
2 their -- to the business of the large retailer that
3 suffered that breach in the wake of that, especially
4 by their reputation, was extremely significant.

5 I think the CEO was let go. There was some
6 turnover on the board as a result.

7 There's a strong motivation there, saying,
8 Okay, we better take steps to ensure, both, that our
9 own systems are secure, and also working with our
10 suppliers.

11 Because, you know, for instance, you know, in
12 the case of Target, I think, ultimately, the breach
13 that occurred happened through an HVAC supplier that
14 they had, you know, that was exploited.

15 The cost to the business is making other
16 retailers sit up and take notice, without question.
17 And I think they are -- they see now, as part of
18 their overall business's risk-management approach,
19 that cyber security has to play an extremely
20 important role. It has to be, you know, part and
21 parcel of the overall risk-management system because
22 that does, ultimately, affect both the top line and
23 the bottom line of their business.

24 So, I do think you're seeing changing
25 behavior just through that market dynamic right now.

1 But, at the same time, you know, again,
2 certain data-reporting requirements under law, you
3 know, are necessary to protect citizens as well.

4 I mean, I think finding the right balance
5 there is important.

6 SENATOR GOLDEN: And the fines, you know, the
7 \$50 million fines, sounds like you'd get people to
8 pay attention. But, unfortunately, that gets passed
9 down through other costs to the retailer, and to us
10 as the -- as the purchaser of those goods.

11 So, at some point, you can fine everybody in
12 the world, but the end result is, we're the ones
13 that are going to be paying for it.

14 JAMIE BROWN: Right.

15 SENATOR GOLDEN: Correct?

16 JAMIE BROWN: No, that is correct. I mean,
17 it ultimately does flow down, you know, to the
18 customers and, you know, citizens, and what extra
19 costs that they will ultimately incur.

20 It's a shame that it requires large events to
21 sort of serve as teaching examples, but --

22 SENATOR GOLDEN: We have to do it,
23 unfortunately.

24 JAMIE BROWN: -- it has, and it will.

25 I mean, you know, even if everyone had, let's

1 say, the state-of-the-art system in place right now,
2 you know, I think we try to make the point that
3 every data system at some point or another -- you
4 know, we say there are two types of organizations:
5 Those that have been breached. Those that don't
6 know that they've been breached yet.

7 And, you know, cyber threat -- the
8 cyber-threat environment is continuing to evolve.
9 You know, there's no perfect security system, but
10 I think that the key is continually circling back,
11 looking at, you know, your risk priorities, looking
12 at what the state-of-the-art is available for
13 security technology, and then trying to line those
14 up as much as possible on a continuous basis over
15 time.

16 It isn't a one-time, you know, we're done.
17 We put in a security system, we're now safe forever.

18 It's got to be a continuous movement.

19 SENATOR GOLDEN: Two more quick questions.

20 JAMIE BROWN: Sure.

21 SENATOR GOLDEN: Facebook. Somebody took a
22 picture and puts the person's picture on the
23 Facebook and creates a face -- a fake Facebook, and
24 then creates a database, and then goes in and rips
25 off a number of seniors by creating this new face

1 and this new image. And people fall for these
2 scams.

3 And by the time you figure it out, you
4 haven't figured out that people are using your
5 picture on Facebook to set up these phony images and
6 phony, you know, personas, so they can go in there
7 and do these scams.

8 Are you encountering a lot of that?

9 JAMIE BROWN: Yeah.

10 Well, I think, on an increasing basis, you're
11 seeing, you know, more that these types of scams
12 leveraging, you know, what can be real images to set
13 up fake identities.

14 And here's an area, this is an excellent
15 area, that only governments can play; and that is,
16 you know, What is the coercive power to impose
17 strict penalties on cyber crime, you know, whether
18 it be identity fraud, or others?

19 And -- I mean, I think -- I can't remember
20 the name of the organization that conducted the
21 study. It might have been the Center for Strategic
22 and International Studies. But, they calculated
23 that, last year, cyber crime alone costs the
24 economy -- the world economy about \$450 billion, you
25 know, with a "b."

1 I mean, that's a massive number, and you
2 think, what could that have been better spent on,
3 you know, to help improve the economy, and other
4 areas?

5 So I think having those -- those penalties in
6 place that are appropriate and commensurate with
7 that size of theft, with that type of identity
8 fraud, is extremely important.

9 SENATOR GOLDEN: The last question: The --
10 to differentiate between public security attacks and
11 private ones, are they basically the same, or,
12 essentially, different, in manner and scope?

13 MTA, water supply, electrical grids.

14 We've been talking about, basically consumer,
15 we've been talking about going after retailer, we've
16 been going after different types of cyber crimes.

17 But, what's the difference in the larger
18 crime, and the effect, obviously, of these larger
19 crimes?

20 And how are they different, or are they
21 basically the same?

22 JAMIE BROWN: I -- when you see attacks on
23 both, like you say, those that are against
24 customer-facing organizations, and others, and
25 I don't have the specifics on, you know,

1 dollar-figure effects of each attack. But I do
2 have, in my written testimony I cite a study that
3 was conducted, I think, by the Ponemon Institute
4 last year, where it talked about, 70 percent -- more
5 than -- excuse me, more than 70 percent of
6 critical-infrastructure owners and operators
7 reported at least one security breach in the
8 previous year that led to the loss of either
9 customer personal information, or, that disrupted
10 operations in that year leading up to the study.

11 So you think about disrupting operations,
12 I mean, if you have someone cleaning the water
13 supply, if you have someone providing power, you
14 know, the effects of those attacks, if successful,
15 and if -- you know, if the attacker decides to sort
16 of go all the way through and try to, you know,
17 execute the maximum amount of damage, I mean, that
18 could -- that could cause significant -- significant
19 damage.

20 So, it is extremely large on both the big
21 organizational level; the critical infrastructure,
22 where customers may not be directly affected. They
23 are certainly indirectly affected.

24 But, you know, I don't have the specifics on
25 the figures; but, no, it is a growing vector for

1 attacks, that, you know, bad actors in the cyber
2 world are looking to exploit more attacks against
3 critical infrastructure.

4 SENATOR GOLDEN: Thank you, Peter.

5 SENATOR CROCI: Thank you, Senator.

6 And, Mr. Brown, I want to thank you for
7 your testimony here.

8 I was struck by one of the comments you just
9 made, that, unfortunately, sometimes it takes a
10 large-scale event to get us to move in the direction
11 that we need to.

12 This is something that a great former
13 governor and member of the Legislature,
14 Theodore Roosevelt, said, that, "Unfortunately,
15 Americans don't learn by experience. We learn by
16 catastrophe."

17 And, today, the purpose of these hearings is
18 to try to avoid that catastrophe, and we appreciate
19 you being part of that effort.

20 JAMIE BROWN: Thank you.

21 SENATOR NOZZOLIO: Thank you very much.

22 SENATOR CROCI: Our next witness to join us
23 today, and we're very pleased to have him here, is
24 Special Agent Donald Freese.

25 Special Agent Freese is the director of the

1 National Cyber Investigative Joint Task Force for
2 the Federal Bureau of Investigation.

3 Certainly, the bureau and the DOJ have been
4 pioneers in this field, as have the Department of
5 Defense, and some of the legacy agencies of DHS.
6 They've really composed the community of excellence
7 in the cyber-security field.

8 And, so, we're especially honored to have you
9 here today, Director Freese.

10 DONALD W. FREESE: (Microphone turned off.)
11 Thank you, Senator. Appreciate it very much,
12 sir.

13 SENATOR CROCI: And we'll take any opening
14 statements or testimony that you would like to read
15 at this time.

16 DONALD W. FREESE: Good morning, Senator.

17 I do have some opening statements --

18 SENATOR CROCI: Please.

19 DONALD W. FREESE: -- or, prepared remarks.
20 I'd just like to lead off with those to give you a
21 little bit of an overview of the cyber landscape
22 (inaudible) the postures that we look at and handle
23 every day.

24 (Inaudible.)

25 SENATOR NOZZOLIO: His mic's not on.

1 SENATOR CROCI: There might be a button.

2 SENATOR NOZZOLIO: Just pull it a little
3 closer to you.

4 DONALD W. FREESE: (Microphone turned on.)
5 Good morning.

6 How's that work?

7 SENATOR CROCI: You got it.

8 DONALD W. FREESE: All right. There we go.
9 Thank you.

10 All right. Good morning, and thank you for
11 inviting me to provide these remarks to the
12 New York State Senate at its public hearing on cyber
13 security.

14 The Federal Bureau of Investigation has a
15 long history of working with all levels of law
16 enforcement, the intelligence community, and private
17 industry in carrying out the FBI's mission. Through
18 this collaboration we focus on building partnerships
19 to help combat the cyber threat to our nation.

20 We value the relationships we have with our
21 New York State partners in helping to protect the
22 residents of New York, as well as other partnerships
23 across the nation, to help protect the United States
24 from malicious cyber incidents and other attacks.

25 I understand the challenges you face, and

1 would like to talk about how we at the FBI view
2 cyber threat, and how we can continue to work
3 together to combat this threat.

4 I also want to impress upon you the
5 importance that the FBI puts on this issue.

6 Although counterterrorism remains the FBI's
7 top priority, we anticipate the cyber security may
8 well become our highest priority in years to come.

9 We at the FBI understand that securing our
10 national infrastructure and networks from these
11 attacks is vital, and that New York State needs to
12 do all that it can to be on the forefront of cyber
13 security.

14 To this end, I'd like to begin today by
15 speaking to you about cyber threat facing both
16 New York and the nation.

17 Between December 2000 and June 2014, the
18 estimated number of Internet users grew from almost
19 361 million to 7.2 billion, an increase of more than
20 741 percent.

21 The use of the Internet increases our
22 capacity for communication, learning, and commerce,
23 and, thus, benefits the world tremendously.

24 The Internet, however, also provides
25 malicious actors with a new avenue for conducting

1 crimes.

2 The White House "Strategy to Combat
3 Transnational Organized Crimes" states that, "Cyber
4 crime costs consumers billions of dollars annually,
5 threatens sensitive corporate and government
6 computer systems, and undermines worldwide
7 confidence in the international financial systems."

8 FBI Director Comey recently stated that, "The
9 Internet is now a vector for criminal activity that
10 completely changes the traditional notions and
11 frameworks of how to deal with criminal activity."

12 Although I'm here today addressing the
13 New York State Senate, one major take-away I hope
14 I've impressed on you already is the fact that the
15 advent and use of the Internet by criminals has
16 redefined the traditional and territorial boundaries
17 of criminal behavior.

18 And although the FBI has had success bringing
19 some of these cyber criminals to justice, due to the
20 difficulties inherent in conducting broad-based
21 international investigations, criminals feel
22 invincible today, and victims feel like they won't
23 ever get justice.

24 The main point is that, what affects
25 New York State can easily affect other states across

1 the country, and vice versa, and fighting today's
2 cyber-crime threat requires a holistic and joint
3 approach.

4 That being said, today's cyber threat to the
5 nation and the state of New York can be separated
6 into several categories.

7 I'd like to just go over those at this time
8 to ensure that you see, from the federal
9 perspective, how we address this threat.

10 First being cyber terrorists.

11 We all know that terrorism has affected
12 day-to-day life across our nation at all levels.

13 Although similar to traditional terrorist
14 activities, the current methodology of cyber
15 terrorists focus on disrupting day-to-day
16 operations.

17 Typically, the sophistication involves low-
18 to medium-level attacks, but make no mistake, these
19 malicious actors have the intention of evolving
20 their capabilities, and they have demonstrated a
21 history of steadily learning and adaptation. They
22 are increasingly cyber-savvy, and much like other
23 multi-national organizations, they are using the
24 Internet to recruit prospective members, grow their
25 business, and carry out small- to large-scale

1 operations.

2 For example, hackers broke into eBay and
3 stole a database full of user information between
4 late February and early March of 2014, and according
5 to open sources, the attackers managed to obtain a
6 small number of eBay employees' log-in credentials,
7 which they used to exploit the company's corporate
8 network. EBay did not disclose how many of its
9 148 million active accounts were affected; however,
10 a spokeswoman said the hack impacted a large number
11 of accounts.

12 From terrorists, we move to the nation-state
13 threat.

14 Terrorist use of the Internet is not our only
15 national-security concern. Foreign state-sponsored
16 computer hacking poses a significant security
17 challenge, and foreign state-sponsored hackers are
18 patient and calculating. They have the time, the
19 money, and the resources to burrow in, and to wait.

20 They may come and go, conducting
21 reconnaissance and exfiltrating bits of seemingly
22 innocuous information. Information that in the
23 aggregate may be of high value.

24 Increasingly in the news, there have been
25 reports of cyber intrusions and attacks on the

1 United States that have been purported to originate
2 from other nation states. We know that, depending
3 on which country is in question, they are reported
4 to conduct a wide range of operations, including
5 persistent computer-network exploitations, also
6 known as "CNE," and computer-network attacks, or
7 "CNA," with the potential targeting of
8 critical-infrastructure data and hardware
9 destruction.

10 For example, in July of 2013, the FBI
11 witnessed malicious cyber actors committing
12 distributed denial-of-services, or "DDoS," attacks
13 against a high-profile U.S. business.

14 Upon investigating the actors further, FBI
15 investigators learned that the hackers intended to
16 expand their DDoS attacks to target the
17 U.S. financial infrastructure.

18 Through investigation, analysis, and
19 coordination with public and private-sector
20 partners, the FBI produced notices to the financial
21 sector of the actors' techniques -- tactics,
22 techniques, and procedures, or "TTPs," empowering
23 financial institutions to secure their networks
24 against the threat.

25 Moving down a list of priorities, we move to

1 financial actors and those motivated by financial
2 gain.

3 And aside from these national-security-level
4 components with both terrorism that we talked about
5 before and nation-state actors, we find that the
6 core motivation -- financial gains -- still
7 represents a major motivation for hackers. Many of
8 the vectors for these cyber crimes are done through
9 social-engineering sites and network exploitations
10 for the purposes of accessing and stealing from
11 business and personal financial accounts.

12 The sophistication of these attacks runs the
13 gambit, and the cyber-crime underworld is a working
14 economy with professionals filling a wide range of
15 job roles at all skill levels, from apprentice, to
16 journeyman, into master class.

17 In other words, this has led to the
18 commoditization of malware, hacking, and
19 services-for-hire by the criminal elite.

20 We move that on into the world where we start
21 to bleed into what we call "hacktivism," or
22 "hactivsts." It's a term that refers to cyber
23 attacks in the name of political and social
24 activism.

25 The segment of cyber-threat spectrum covers

1 everything, from individual hackers seeking thrills
2 and bragging rights, to organized hacking groups
3 conducting distributed denial-of-service attacks and
4 web defacements against government and corporate
5 entities.

6 Moving further towards the core of what we're
7 examining today, the insider threat is something
8 that's always been in existence, from both spies and
9 corporate insiders. It has been -- the risk has
10 been increased through the automation process.

11 And the last group that we'll talk about is
12 cyber attackers. It involves one that can perhaps
13 pose the most serious threat to all levels of
14 industry and government; and that's the insider
15 threat, or the threat from people who are part of
16 the actual institutions which are being targeted.

17 Often their attacks include CNA, CNE,
18 physical exfiltration or actual destruction of
19 information, or sensitive or classified data.

20 Potential insider-threat actors include
21 non-technical employees with access to sensitive
22 data, third-party contractors and partners,
23 including IT administrators and any employee with a
24 grudge or perceived wrong. Insider-threat activity
25 can be witting malicious theft attack, espionage, or

1 unwitting accidental data leaks or destruction.

2 I'll leave you with one final example.

3 A research scientist recently admitted to
4 stealing trade secrets from a chemical company and a
5 diversified manufacturer worth between 7 and
6 20 million.

7 A software engineer stole proprietary
8 technology trade secrets that handset manufacturers
9 had spent hundreds of millions of dollars to
10 develop.

11 The government agency paid \$20 million to
12 settle a class-action lawsuit, after a laptop
13 containing millions of dollars in personal PI was
14 stolen from the employee's home.

15 In summary: Government and private-industry
16 IT professionals indicate insider threats currently
17 account for 25 to 50 percent of all cyber-security
18 incidents. The threat is so serious that
19 Executive Order 13587 addressed insider threats, and
20 stood up the Insider-Threat Task Force to advise on
21 detering information-security risks posed by
22 insiders.

23 At this point, I would submit the rest of my
24 prepared comments to the record, and for your
25 questions.

1 I would submit myself for your response.

2 SENATOR CROCI: We very much appreciate that,
3 Director Freese.

4 And, I have one question from
5 Senator Addabbo.

6 SENATOR ADDABO: Thank you.

7 Thank you, Mr. Chair.

8 Thank you Mr. Chair.

9 I want to thank yourself, the veteran
10 Committee Chair;

11 Senators Nozzolio and Senator Venditto,
12 thank you very much;

13 And your staff, for the efforts today on a
14 critical important issue for our state.

15 All the more reason that the Legislature must
16 have a cooperative working effort with our
17 administration, for the sake of our people, and the
18 safety of the people throughout the state, on this
19 issue of cyber terrorism.

20 Mr. Freese, thank you very much for your
21 time today and for your efforts at the FBI.

22 We discussed so far about cyber terrorism,
23 cyber threats, regarding infrastructure, utilities,
24 and so forth.

25 I want to expand a little bit to airports and

1 aircraft.

2 Recently, earlier in the week, we had an
3 individual -- not a terrorist individual -- we had
4 an individual who claims that he has hacked into --
5 20 times over the course of a number of years,
6 2011 to 2014, hacked into different aircraft,
7 adjusting their plane flight, mobility,
8 entertainment system.

9 It's a major concern, certainly, as we have
10 airports throughout the state. This plane was bound
11 for Syracuse, I understand.

12 I have a district that is adjacent to JFK.
13 I'm in a borough that has JFK and Laguardia.

14 We know the weapons -- when planes are used
15 as weapons, the devastation that can occur.

16 I would like you to weigh in on that issue.

17 Cyber terrorism as it relates to our aircraft
18 and airports, how real is it? And what possible,
19 you know, measures can be taken?

20 DONALD W. FREESE: Okay.

21 You referred, Senator, to a specific incident
22 that's in the paper just recently, I believe?

23 SENATOR ADDABO: It's not so much that
24 particular incident, but the issue in general,
25 because you know it's a threat.

1 DONALD W. FREESE: Right, absolutely.

2 Yeah, I'll talk about the issue in general,
3 and the automation of both aircraft, aircraft
4 systems, and aircraft-control systems.

5 Certainly, the risks to those systems have
6 grown more broadly as the information technology has
7 rapidly infiltrated almost every element of the
8 aircraft industry.

9 If we just focus on that for a few minutes,
10 I will describe that risk as both broad; however, it
11 is extremely regulated, and, in my opinion, well
12 mitigated. All right?

13 My opinion is supported by all of the
14 professionals in the industry that we have looked
15 at, both, from the FAA, from the federal government
16 regulatory side, as well as our partners in private
17 industry who deploy the different control mechanisms
18 and modules.

19 Quite simply, there are broad claims of
20 penetration vulnerabilities on the systems from
21 different individuals throughout the world in
22 different things that are not true vulnerabilities.

23 Now, that being said, nothing is completely
24 foolproof. And we all know that to be the case,
25 particularly in a digital environment, there are

1 vulnerabilities.

2 I can tell you, however, that, the act, the
3 industry takes seriously, both, from the private
4 side; that is, the aircraft controllers, from the
5 manufacturing and the supply-chain risks, right down
6 to who develops the engineering and the core-chip
7 processing of each one of those components, whether
8 it's fly-by-wire components, whether it's
9 entertainment systems, or whether it's
10 airline-control components.

11 Each one of those things is very closely
12 controlled from both the manufacturing supply chain,
13 all the way through the implementation, execution,
14 as well as testing, and "penetration testing," a
15 term we use in the industry to determine whether or
16 not those systems are, to use a layman's term,
17 "hackable."

18 And, quite simply, those systems are some of
19 the best-defended in the world.

20 So to answer your broader question, that is
21 not a threat that we focus on highly as a tier one
22 high-risk area, because the industry is so
23 financially motivated to protect both the brand and
24 both the protection of their industry.

25 Any type of intrusion by some type of actor

1 to control an aircraft would, obviously, have
2 devastating consequences if that could occur.

3 We feel that the industry has postured as
4 well, through the FAA, and other regulatory,
5 including the state regulatory agencies, who look at
6 these things, multiple layers of security, multiple
7 redundancies, to fully mitigate that threat.

8 SENATOR ADDABO: It must be an extremely
9 daunting task because now we're talking about, at
10 this point, global airports throughout the world,
11 carriers starting from here, going to Europe, and so
12 forth.

13 Can you weigh in -- we mentioned it a little
14 earlier, can you weigh in on that particular
15 incident that happened earlier in the week?

16 Is that an ongoing investigation?

17 Did that spur another, you know, look at this
18 issue of airport cyber terrorism?

19 DONALD W. FREESE: Yeah, I won't speak
20 specifically to that issue because of the ongoing
21 investigative nature of it.

22 However, I will speak to that type of event,
23 and I believe I heard a two-part question, both
24 nationally or internationally, what the aspects of
25 the airline industry are. And although I'm not an

1 expert in that field, certainly have worked in and
2 around the IT infrastructure in that field.

3 That the claims of certain individuals, not
4 just the one that we're referring to, are often
5 built on theoretical and not actually applied
6 measures.

7 So, theories are great; and, in theory,
8 certain things could happen. However, all of the
9 layers of defense and the penetration testing, as
10 well as the encryption of the particular systems,
11 are extremely robust.

12 And the concept that any individual, nation
13 state or all the way through, could somehow
14 interfere with those in an effective way, to also
15 remove -- and this is very important point -- remove
16 the human in the loop; or, in other words, usurp a
17 pilot's command of an aircraft, simply does not make
18 sense.

19 And so we have to remember the human in the
20 loop can often be a weakness in information
21 technology and security risks.

22 And that's a little bit of a different
23 question, but I wanted to underscore, no matter who
24 has manufactured the aircraft at this time, and,
25 unlike a train or something else, that co-pilot

1 system is there in place. There's always two people
2 in control, cognitive control, of any aircraft,
3 under U.S. regulations, now focusing just on U.S.,
4 and they are able to understand and monitor those
5 systems in an effective way and to fly the aircraft.

6 And, in fact, they're trained to fly those
7 aircraft no matter what happens to any
8 instrumentation or fly-by-wire controls.

9 And so that type of human monitoring,
10 real-time, of what the situation awareness is with
11 that aircraft is what we rely on, ultimately, as the
12 security elements.

13 Just like you do in any building or other
14 thing, you always have those humans who are involved
15 in the security process.

16 So, I want to allay the fears that, somehow,
17 something would occur so rapidly, or, with such
18 devastating consequences, that, you know, active
19 control of an aircraft would be lost in that
20 situation.

21 SENATOR ADDABO: Mr. Freese, again, I want to
22 thank you very much for weighing in on that
23 particular issue; but that particular issue aside,
24 I want to thank you very much for the FBI's efforts,
25 and your reassurance that this issue about cyber

1 terrorism, as it relates to our airports, is, you
2 know, being taken care of, or at least being
3 acknowledged, very seriously.

4 Chairman Croci, thank you very much.

5 SENATOR CROCI: Thank you, Senator.

6 DONALD W. FREESE: Thank you, Senator.

7 SENATOR CROCI: Senator Nozzolio.

8 SENATOR NOZZOLIO: Thank you very much.

9 I add my gratitude for your excellent
10 testimony.

11 And I -- on pages 4 -- the written testimony
12 you gave us, 4 through 8, you had listed a number of
13 items that you would like to see, and I think it's a
14 great template as we look to legislation, to see
15 which steps are being taken.

16 DONALD W. FREESE: Sure.

17 SENATOR NOZZOLIO: One bit of additional
18 guidance I would like to give -- get from someone
19 with such great experience as you, in terms of the
20 encouragement for the private sector to share with
21 the public about a data breach.

22 What would you suggest, as one who has been
23 called in to investigate criminal activity, what
24 would we best do to encourage a process that doesn't
25 further victimize the person that says, I've been

1 injured as an organization?

2 Your thoughts?

3 Yet, and at the same time, help you do your
4 job, and the bureau's job, in terms of protecting
5 Americans?

6 DONALD W. FREESE: Sure.

7 The question is, as I understand it, Senator,
8 what would we encourage with private industry to
9 work with government, broad whole-of-government
10 approach here, whether at the state, federal, or
11 local level, in order to be more transparent when
12 breaches occur?

13 Do I have that question correct, sir?

14 SENATOR NOZZOLIO: Yes.

15 DONALD W. FREESE: Okay.

16 Specifically, one strong recommendation that
17 the FBI makes, is to ensure that, constitutionally
18 protected, or personal information is always
19 protected, in any sharing process that occurs.

20 We see people's -- or, the tension, shall we
21 say, between personal privacy, and a security, is
22 something that always needs to remain in balance.

23 So all my comments are balanced on that
24 principle right there.

25 So, we also see that, the rule of law, and we

1 expect that the rule of law in the United States, is
2 one of the sterling examples that keep our country
3 free, and keep us from becoming what would sometimes
4 be described as a "police state," and other
5 examples.

6 So, specifically to your question, balanced
7 on those two points, we would always encourage that
8 any legislation requires reporting, when an
9 intrusion occurs that is significant, to the proper
10 law-enforcement authorities, and that should be
11 scaled on the level of the event and the level of
12 the company.

13 For example, if this is a very small business
14 that is merely run at a local or municipal level,
15 and, they have an intrusion problem with their
16 computer system, that should be so reported at that
17 level.

18 And if there is something that is
19 interconnected with the systems of that business, as
20 we start to grow in scale and scope of the
21 enterprise, we believe that the reporting to law
22 enforcement should occur at a broader level.

23 We focus on law enforcement here, as opposed
24 to intelligence agencies, because we believe that
25 law enforcement is the proper action arm inside the

1 domestic space of the United States in order to
2 prevent, to respond, and investigate any of these
3 intrusions that would occur.

4 Now, we treat -- for example, when we deal
5 with one of those reportings, we treat that company,
6 first of all, as a victim, and we treat the victims
7 as victims. There's a dual-victimization process
8 there.

9 So any legislation that encourages, both,
10 that law-enforcement reporting, and then the
11 secondary portion, depending on the sector that
12 we're talking, about regulatory reporting.

13 For example, two of the most vulnerable
14 industries, certainly, with New York State
15 infrastructure and with our nation, when we talk
16 about sectors, would be the financial sector and the
17 energy sector, just to talk about those, and
18 vulnerabilities and cyber attacks in both those
19 sectors are extremely high.

20 Both sectors are also heavily regulated, and
21 so regulators at all those agency levels should be
22 part of that reporting stream so that they can help
23 understand, as well as federal law enforcement, and
24 to help to engage, share openly the information
25 about whatever attack occurred or whatever intrusion

1 occurred so that we can help mitigate that threat.

2 And that would always be the encouragement to
3 any legislation, based on constitutional protections
4 and the rule of law, where people can feel that this
5 type of commerce is protected.

6 SENATOR NOZZOLIO: Thank you. That's very
7 helpful.

8 I think the other area where we wish to have
9 your guidance, you suggested a holistic approach in
10 your testimony, and that a multi-city approach,
11 multi-jurisdictional approach.

12 New York is unique in a number of ways. The
13 Stock Exchange is here. The financial-services
14 industry is centered here.

15 We've always been an international hub of
16 commerce.

17 What unique aspects in the hosting of that
18 role that we play should we provide additional tools
19 for law enforcement within our own state laws, to --
20 that may be unique to New York, in solving some of
21 the issues that an international hub of commerce
22 would normally have at its nexus?

23 DONALD W. FREESE: If I understand your
24 question, Senator, it was, what tools at the state
25 level would we encourage?

1 Is that correct?

2 SENATOR NOZZOLIO: For law enforcement,
3 within this broad national and international dynamic
4 that occurs in New York State.

5 DONALD W. FREESE: I would highlight --
6 I would highlight two areas for you, Senator, that
7 I think should fully be supported at the state
8 level, and also reinforced through your local
9 enforcement agencies; and that is participation with
10 the federal government.

11 And I'll give you two specific examples, with
12 the FBI cyber and FBI terrorism investigations,
13 because there is an overlap between the two, and
14 that's how I started my briefing.

15 We need to keep a high level of situational
16 awareness with target and threat vectors in both
17 areas.

18 So, the cyber -- FBI Cyber Division, which
19 I represent here today as the director of the
20 NCIJTF, I also represent 22 other federal agencies,
21 we have a fellowship program wherein we actively
22 recruit and work with state and local
23 law-enforcement officers. In fact, I have several
24 on my team right now. We bring them in for
25 six months of full-time training, and we train them

1 at the national level. We clear them at the
2 top-secret level, with certain other clearances, to
3 have full access to all national-security scope and
4 spectrum.

5 And what we're doing there is what we've done
6 for over 100 years in the FBI, in including state
7 and local partners in the national fight against
8 threats that are natural -- national and holistic.

9 So I would heartedly recommend support of
10 programs like that.

11 It is -- it does require your state and local
12 officers to be away from their departments, but that
13 is time well-spent.

14 Not only do we have them doing on-the-job
15 training, but we also give them formal. Over
16 \$80,000 in federal funds are spent to train those
17 officers in cyber-intrusion and cyber-investigative
18 techniques. And that's designed with developing
19 young leadership in those departments at both the
20 state and local level, to learn how to not only
21 understand the cyber threat, but to scale against
22 and to lead their teams against it.

23 We have very successful models, and I'll
24 transition here to the terrorism task force.

25 You have several joint terrorism task forces,

1 very successful, here in New York State.

2 That's a repeatable model that we handle
3 throughout the United States. We model our cyber
4 task force: you have a cyber task force right here
5 in Albany, certainly a very robust one. And, in
6 New York City, multiple teams in New York City, for
7 example.

8 I would fully support -- or, I would
9 encourage any legislation at the state and local
10 level to support and encourage those officers to
11 become trained at the national level, because all of
12 these threats, the ones that are truly high-impact,
13 the highest-level risks that we talk about in the
14 cyber community, need to be mitigated and
15 understood, first of all, from a nation state and
16 international terrorism threat.

17 Those officers come back, they work in the
18 cyber task forces and the joint terrorism task
19 forces here locally; they bring that knowledge.

20 More importantly, they bring the developing
21 leadership, and they recruit other officers to
22 continue to scale into that.

23 And we spend millions of dollars at the
24 federal-government level to train those officers
25 then on to the -- the -- really, the nuts and bolts

1 of cyber defense, cyber-security.

2 And so I would recommend those programs to
3 you strongly.

4 I believe that you -- well, I know for a fact
5 you have several officers that you could bring in to
6 testify and talk to you about their experiences in
7 New York State. You've been tremendous partners in
8 that, in all ways.

9 And I would encourage you to proceed forward
10 in those partnerships.

11 SENATOR NOZZOLIO: That's a great suggestion.
12 Thank you very much.

13 DONALD W. FREESE: Yes, sir.

14 SENATOR NOZZOLIO: Appreciate it.

15 SENATOR CROCI: Thank you, Senator.

16 Any further questions for this witness?

17 Director Freese, I just want to thank you.

18 You preempted all of my questions.

19 Very thorough testimony, and your advice and
20 your guidance and expertise in this area is very
21 much appreciated.

22 I want to compliment you on your role with
23 the bureau now. And, also, thank you for your
24 military service, and your long and distinguished
25 career with the bureau.

1 And, we look forward to being partners with
2 our federal partners, from the state level, to
3 ensure that we're doing everything we can not to be
4 the weak link, and to be a strong link and partner
5 with the government -- the federal government.

6 So, thank you very much for your appearance
7 here today.

8 DONALD W. FREESE: Thank you, Mr. Chairman.

9 And on behalf of Director Comey and his
10 staff, we thank you for your support, and, we're
11 always here to serve the state and local at every
12 level, and we're committed to doing that in our
13 roles, and we intend to do that, moving forward.

14 Please let us know how we can be of
15 assistance in the future.

16 Thank you, Mr. Chairman.

17 SENATOR CROCI: Thank you, sir.

18 SENATOR NOZZOLIO: Thank you, Director.

19 DONALD W. FREESE: Thank you.

20 SENATOR CROCI: Thank you, sir.

21 Our next witness is going to be
22 Dr. Peter Bloniarz, executive director of the
23 Governor's Cyber Security Advisory Board.

24 Good morning, Doctor.

25 How are you?

1 DR. PETER BLONIARZ: (Microphone turned off.)
2 (Inaudible.)

3 SENATOR CROCI: If you would like to make any
4 opening statements at this time, please feel free to
5 do so.

6 DR. PETER BLONIARZ: I would like to thank
7 the Senators, especially Senator Croci and
8 Senator Nozzolio and --

9 SENATOR CROCI: Push the button.

10 DR. PETER BLONIARZ: (Microphone turned on.)
11 I would like to thank the Senators,
12 especially Senator Croci, Senator Nozzolio, and
13 Senator Venditto, for the invitation to speak this
14 morning.

15 My name is Peter Bloniarz. For the past year
16 and half I have been the executive director and
17 senior policy advisor to the New York State Cyber
18 Security Advisory Board.

19 Recently I also became acting chief
20 information-security officer in the Office of
21 Information Technology Services in the state.

22 These two roles are complementary, in that
23 I now have the ability to translate recommendations
24 of the board into practice, and work more closely
25 with state Chief Information Officer Maggie Miller

1 and her team to protect New York government
2 infrastructure.

3 In my career I spent more than 35 years as a
4 faculty member and academic researcher at the
5 University at Albany, State University of New York,
6 where I was the founding dean of the College of
7 Computing and Information.

8 I have a Ph.D. in computer science and
9 electrical engineering from the Massachusetts
10 Institute of Technology.

11 In May 2013, recognizing the challenges to
12 the state, Governor Cuomo convened a Cyber Security
13 Advisory Board to advise his administration on
14 policies, programs, and developments in cyber
15 security.

16 The advisory board is co-chaired by
17 Terry O'Leary, the Governor's deputy secretary for
18 public safety; Ben Lawskey, the state superintendent
19 of financial services; and Will Pelgrin, president
20 and CEO of the Center for Internet Security, a
21 New York-based not-for-profit that plays a key role
22 in cyber security at the state and local level.

23 The other four board members are key former
24 architects of cyber-security programs in the federal
25 government, each having served respective roles in

1 the White House, the Department of Homeland
2 Security, and the FBI.

3 In my role on the advisory board, I advise on
4 how to protect not just state government's assets,
5 but also the development of best cyber-security
6 practices for the state as a whole.

7 Our first task on the board was one that,
8 Senator Croci, you mentioned in your opening
9 remarks: What's the State's role in cyber security?

10 There's a lot of activity at the federal
11 level that we've just heard about, at the
12 private-sector level.

13 How does the State add to what's going on at
14 the federal and private levels, local government,
15 without being duplicative in adding to the solution?

16 We see four roles that the state government
17 plays.

18 First, to protect New York State government's
19 information assets.

20 Second, to help New York State's citizens and
21 institutions, particularly our critical
22 infrastructures and those that are economically
23 important to us, to protect themselves.

24 Third, is to enforce cyber-security laws, and
25 to provide targeted intelligence wherever it's

1 needed in law enforcement and homeland security.

2 And, fourth, to support the growth of
3 New York's cyber-security workforce and
4 cyber-security industry.

5 Director Freese talked about the importance
6 of that training and education, that workforce
7 development, that's especially important.

8 The State's efforts in cyber security
9 emphasize several themes that you've heard earlier
10 today: Collaboration, cooperation, prioritizing our
11 efforts, being flexible and adaptable,
12 standardizing, and simplifying, and then, finally,
13 making sure that we're prepared should a security
14 incident occur and we have to deal with that.

15 We are using best practices that have been
16 adopted by successful organizations across the
17 globe.

18 In carrying out those four functions, those
19 four roles, several executive-branch offices are
20 responsible for carrying out that role.

21 The first role, protecting the state
22 government's information assets, is part of every
23 state employee's job.

24 Every state agency has sensitive and
25 essential information that needs to be protected, so

1 cyber security falls under the purview of every
2 state employee, every state agency.

3 Their efforts are coordinated by the
4 Office of Information Technology Services in the
5 state.

6 IT Services uses best practices and standards
7 from around the country to carry out its
8 responsibilities, including the cyber-security
9 framework promulgated by the National Institute of
10 Standards and Technology, that "NIST" framework that
11 you heard in the first testimony.

12 This is an emerging and useful standard for
13 organizing our cyber-security protection for the
14 nation's critical infrastructures.

15 For the second role, helping New York State
16 citizens and institutions protect themselves,
17 several state agencies share responsibility.

18 The New York State Division of Homeland
19 Security and Emergency Services plays a key
20 coordinating role in this process as part of their
21 all-hazards approach to protecting the state.

22 As one example, in their 2014 Homeland
23 Security Strategy, one of the 10 goals for the
24 division is enhancing New York State's
25 cyber-security capacities, and they coordinate

1 activities of several agencies, including
2 IT Services, in working to achieve that goal.

3 We rely on DHSES's expertise and preparedness
4 planning through their Office of Emergency
5 Management and their Office of Counterterrorism to
6 provide hazard mitigation in any threat that faces
7 our state.

8 They play a key role in our cyber-security
9 resiliency, in addition to the traditional roles
10 they've have always played in incident response.

11 We look forward, as one example, to using
12 their expertise as we're planning cyber exercise
13 that will enhance our resiliency at the highest
14 level of executive leadership.

15 In addition to Homeland Security and
16 Emergency Services, other agencies, including
17 regulatory agencies, like the financial -- the
18 Department of Financial Services and the
19 Public Service Commission, play an important role,
20 both, on their own, and in coordination with
21 Homeland Security and Emergency Services' efforts.

22 These agencies utilize intimate knowledge of
23 their regulated industries to tailor state efforts
24 to help secure critical sectors of New York's
25 economy and industrial base.

1 For third role, law enforcement, the
2 New York State Police leads New York's efforts, in
3 concert with local and federal law enforcement,
4 including the FBI and Secret Service.

5 An important asset for both the state police
6 and Homeland Security and Emergency Services is the
7 New York State Intelligence Center, the state's
8 fusion center, where federal, state, and local law
9 enforcement and Homeland Security personnel work
10 together on a number of fronts, including cyber
11 security.

12 The intelligence center is in East Greenbush,
13 co-located in the same building as the Center for
14 Internet Security, the not-for-profit cyber-security
15 organization I mentioned earlier.

16 The Center for Internet Security, or "CIS,"
17 as it's called, plays an important role in the
18 state's activities in cyber security.

19 The federal Department of Homeland Security
20 has a designated CIS, through its Multi-State
21 Information Sharing and Analysis Center, or
22 "MSISAC," is the key resource in cyber security for
23 state, local, tribal, and territorial governments in
24 the United States.

25 CIS operates a 24-by-7 security operation

1 center and serves as the central resource for
2 information sharing and incident response for
3 New York, and the rest of the country.

4 CIS is a key asset for the state on all four
5 of our responsibilities.

6 In addition to participating in the MSISAC,
7 the Office of IT Services maintains an independent
8 contract with CIS to monitor the networks of
9 New York State and certain local governments in the
10 state, proactively looking for activity that might
11 indicate a compromise or a data breach.

12 Finally, the workforce and
13 economic-development roles are carried out by
14 several agencies and partners.

15 IT Services plays a lead role here. They
16 hold programs, ranging from those designed for
17 elementary school students, to an academic
18 conference, in conjunction with the annual state
19 cyber-security conference that will be held later
20 this summer in -- June 1st and 2nd and 3rd here in
21 Albany.

22 Empire State Development, the Department of
23 Labor, and the advisory board will be holding a
24 series of cyber-security roundtables later this year
25 to engage the private sector in critical areas, such

1 as the cyber-security industry itself, health care,
2 financial, energy, to dialogue about best practices.

3 In pursuing these four roles in coordinated
4 and collaborative fashion, New York has created a
5 strong foundation for securing the state.

6 The four agencies that bear primary
7 responsibility, Division of Homeland Security,
8 IT Services, and the state police, along with the
9 not-for-profit Center for Internet Security, work
10 hand-in-hand on a regular basis to protect our
11 infrastructure, identify incidents when they occur,
12 and recover quickly.

13 The move to a consolidated data center is
14 accelerating our efforts to protect state assets.

15 This will allow us to simplify and
16 standardize our approaches to cyber security.

17 It will enable us to apply uniform criteria
18 and methodologies for accessing our information
19 systems, the kind of identity and access management
20 that was talked about earlier.

21 It will let us simplify the monitoring of
22 external Internet connections. It will let us track
23 and, potentially, intercept intrusions as they are
24 happening.

25 Recognizing the significant step that

1 New York is taking in cyber security, when the
2 National Governors Association held a summit on
3 state cyber security earlier this year, they invited
4 us to present New York's approach in the panel on
5 cyber governance.

6 This past Monday, the assistant secretaries
7 for cyber security and intergovernmental affairs at
8 the federal Department of Homeland Security came to
9 NYSIC to learn firsthand how New York has organized
10 firsthand, and how we can work better to share
11 information and intelligence.

12 Our unified and collaborative approach is one
13 that can serve as a model for other states.

14 All that said, our work to protect
15 New York State is an ongoing mission.

16 We face continued threats for those who seek
17 to infiltrate our systems at home and abroad, and we
18 will continually improve our efforts.

19 We will continue to automate, to simplify,
20 and improve our defenses.

21 We'll continue to work with partners in the
22 federal government and the private sector to carry
23 out a multi-layered defense against our cyber
24 adversaries.

25 And, finally, we will continue to remind

1 people, both our employees and all our citizens,
2 about the need for constant education on the issue
3 of cyber security, because an aware and proactive
4 public is a critical component in protecting our
5 information and our infrastructures.

6 Finally, we will prepare for events that
7 hopefully will never happen, but for which we must
8 continue to remain vigilant.

9 I thank you, Senators, for your attention.

10 I look forward to your questions and our
11 conversation.

12 SENATOR CROCI: Thank you, Doctor.

13 I appreciate your testimony here today.

14 Just a couple of questions.

15 First off, you serve as the chair of the
16 advisory board.

17 You -- thank you for clarifying who makes up
18 the advisory board.

19 Do you think that that advisory board has
20 been important into what you've described as an
21 integrated approach to our cyber-security posture?

22 DR. PETER BLONIAZ: I very much think so.

23 I think one of the -- one of the things that
24 sets New York apart from other states is that we
25 have coordination directly from the top, through the

1 advisory board, to all the units that pay -- that
2 are responsible for carrying out our mission.

3 Just one correction: I'm not the chair of
4 the board. I'm the executive director.

5 The co-chairs are Terry O'Leary, Ben Lawskey.
6 These are folks in the state who, you know, bear
7 major responsibilities for some of our protective
8 roles.

9 We work very closely with the other deputy
10 secretaries on the second floor.

11 We work very closely with agency heads that
12 are important to serving our mission.

13 We have advice from the best of the folks who
14 are on the board, as I said, helps shape federal
15 policy, helps shape federal programs.

16 These are people like, Richard Clark, the
17 White House first cyber advisor. Howard Schmidt,
18 the second cyber advisor. Sean Henry, who's with
19 the -- he's helped set up the FBI's cyber programs
20 that you just heard about today. Phil Reitingger,
21 who was both in the White House and DHS.

22 And so I think that the -- the advice that
23 we've been given, and the support from, both, on the
24 executive chambers, as well as agency heads, has
25 been extraordinary.

1 SENATOR CROCI: Given the importance, it
2 would seem logical that we codified in statute to
3 make sure that is there for generations to come, if
4 it's been, certainly, influential and important at
5 the inception of what is a new field in this
6 country.

7 It sounds as though, I don't know if you
8 would agree, should it be codified and made
9 permanent?

10 DR. PETER BLONIARZ: Yeah, those are
11 questions that really are above my pay grade.

12 Sorry about that.

13 But, you know, my job is to do what I can to
14 help protect the state. I give advice.

15 I think that input from everybody is
16 extremely important --

17 SENATOR CROCI: And to that point -- I'm
18 sorry to interrupt.

19 To that point, would it be prudent then to
20 have additional representation, additional input,
21 from industry, on that board?

22 DR. PETER BLONIARZ: In terms of industry, we
23 have gotten that -- such input.

24 The folks that are on the board are now all
25 in private industry, so that they're -- you know,

1 the four members that I mentioned that came from the
2 federal government, they are now all working in
3 industry.

4 But we've had --

5 SENATOR CROCI: In what sectors, for
6 instance?

7 DR. PETER BLONJARZ: The -- Dick Clark is
8 cyber-security industry.

9 Phil Reitingger was the former director at
10 Sony -- the cyber-security director at Sony.

11 The people that we've -- yeah, the people on
12 the board are primarily from the cyber-security
13 field because they wanted to get expertise.

14 But our interaction with folks is not just
15 limited to, you know, the members of the board.

16 I mentioned earlier, the roundtables that
17 we'll be doing around the state.

18 The first one is scheduled for June 1st here
19 in Albany, with representatives from the
20 cyber-security industry.

21 The other roundtables are targeting -- wish
22 to get input directly from key sectors of the
23 state's economy.

24 So as I mentioned, we've been working with
25 the Department of Health to schedule one for the

1 health sector. We may run two of those.

2 Health is -- you know, with the Anthem
3 breach, even though that's not the health industry,
4 it's more the insurance industry, but the -- you
5 know, that sector is an increasingly important
6 target for attacks.

7 So, these roundtables are designed to get
8 exactly the kind of input and conversation that
9 you're describing from industry sectors who are
10 trying to protect their networks, and, where are
11 their challenges, the objective of these.

12 We held -- just as an example, we held one
13 with the energy sector back on April 2nd. Public
14 Service Commissioner, the Chair, Audrey Zibelman,
15 Homeland Security Commissioner Melville, and myself,
16 held a cyber-security summit with folks from the
17 industry -- the electrical sector, and guest
18 sectors, mostly private sector. One or two of the
19 utilities are publicly-owned, but most of them are
20 private sector.

21 And the question was, What should the State
22 be doing to help you protect your systems, to help
23 you do your job better, because we're all in this
24 together?

25 It's --

1 SENATOR CROCI: But you don't believe it's
2 necessary to have those key sectors represented at
3 the advisory board level?

4 DR. PETER BLONIAK: As members of the board?
5 I think we're getting the input that we need
6 from the private sector at this point.

7 Part of my job as executive director is to
8 make sure that, you know, we do get the input from
9 the folks that we need.

10 So, you know, the membership is the
11 Governor's choice, so....

12 SENATOR CROCI: Understood.

13 The other question I had is, in
14 Director Freese's testimony, he mentioned the -- the
15 hardware vulnerabilities.

16 So, we know about the software
17 vulnerabilities, and the application
18 vulnerabilities, but, he mentioned the hardware
19 vulnerabilities; our servers, for instance.

20 Are we convinced at the state level that
21 we're doing everything we can, from a
22 continuity-of-government perspective, to ensure that
23 not only those servers are protected in the most
24 secure facilities possible, but also that -- our
25 critical information systems and our intelligence

1 apparatus are being protected from a
2 continuity-of-government perspective?

3 DR. PETER BLONIARZ: Yes, I think that's
4 someplace that, again, where -- where New York is --
5 has been very -- I think we have a huge advantage,
6 in that we're moving to consolidate data centers
7 across the state. You know, moving from
8 65 agencies, all of which had their own facility, to
9 one facility that -- where we can apply uniform
10 hardware implementations, where we can apply uniform
11 policies.

12 I think that's one of the strongest steps
13 that we've taken towards security, even though it
14 happened before my time in the Governor's Office.

15 I think that, you know, in terms of some of
16 the issues that were talked about, the coordination
17 of -- or -- and control of monitoring of who gets
18 access to the networks, how do -- what kind of
19 traffic is going across the network?

20 What kind of traffic is going out of the
21 network?

22 Is -- are there unusual patterns that we
23 should investigate?

24 I think that we're in exceptional shape to do
25 that because we're bringing all of that together.

1 So I think -- with regards to the hardware,
2 I think that we have the strategy and plan to really
3 provide the kinds of security that New York
4 deserves, yes.

5 SENATOR CROCI: And as far as any -- what
6 regulatory actions, or, in what way have the
7 departments and agencies within the state brought to
8 bear regulatory powers in order to better posture
9 us?

10 DR. PETER BLONIARZ: That was something that,
11 again, the board encouraged us to -- encouraged the
12 State to use all of its powers to make us more safe.

13 I'm sure you're familiar with the work that
14 the Department of Financial Services has done in the
15 financial field, doing -- you know, examining what
16 the status is in the banks that we regulate, and the
17 insurance companies.

18 How are they paying attention to their risks?

19 What are they doing for identity management?

20 How are they dealing with the fact that, you
21 know, oftentimes, stolen credentials are the way
22 that people wreak havoc and get information in the
23 systems.

24 Looking at, you know, what does your supply
25 chain look like?

1 How are -- are the companies that you depend
2 on, are they having the same security practices as
3 you have, because that's an important aspect of your
4 business?

5 SENATOR CROCI: Has that regulatory been
6 brought to bear? Have we brought to bear that
7 regulatory action?

8 DR. PETER BLONIARZ: I'm not -- I know
9 regulations have been proposed. I'm not sure today,
10 as we speak, what status that is.

11 I know that Financial Services, again, like,
12 you know, any regulatory organization, proposed
13 regulation, get input from the community about them,
14 and then finalize those regulations.

15 Where we are today, I'm not -- you know,
16 where it is in the -- in the -- I'm not perfectly
17 familiar, but I would be happy to get you that
18 information, if you'd like.

19 SENATOR CROCI: Yes, please.

20 DR. PETER BLONIARZ: But what I do know is
21 that, you know, from the superintendent on down,
22 they take cyber security very seriously.

23 They see that their role is to help protect
24 New York State's economic institutions, to help
25 protect its citizens, and they take that role very

1 seriously.

2 So -- but I'll get you that information of
3 where that -- the regulations stand right now. I'd
4 be happy to do that.

5 SENATOR CROCI: I would very much appreciate
6 it.

7 And my final question: You are recently the
8 director at ITS; correct?

9 DR. PETER BLONIARZ: I'm recently appointed
10 as acting chief information-security officer.

11 SENATOR CROCI: And when did that occur?

12 DR. PETER BLONIARZ: It was about 2 1/2 weeks
13 ago.

14 SENATOR CROCI: Okay. Are you -- and maybe
15 this will require more time, but, are you convinced
16 that the separation of the cyber role from the DHSCS
17 structure is appropriate?

18 DR. PETER BLONIARZ: How you structure things
19 is, I think, a small part of how -- of our
20 effectiveness.

21 I think that what's most important is how
22 teams work together to mitigate our risks, to
23 strengthen up our weak areas.

24 I talked earlier about the -- you know, the
25 State has four different roles, and I think they're

1 distinct roles.

2 IT Services has a responsibility -- a direct
3 responsibility, Megan Miller and her team, have
4 responsibility for making sure that the whole state,
5 and I emphasize that it's not just her job and her
6 technology people to protect the state, but state
7 agencies play an important role.

8 You heard earlier testimony about how you
9 have to identify your most critical assets.

10 That's an agency job. Every agency has to do
11 that.

12 You have to apply the appropriate controls
13 because we can't afford to protect everything, and
14 we shouldn't try to protect everything.

15 We have to -- to the same degree, we have to
16 protect appropriately.

17 So I think that IT Services has a major
18 responsibility in coordinating all those efforts at
19 the state level.

20 I think the Division of Homeland Security and
21 Emergency Services has an equally important role in
22 protecting the state as a whole, and help -- and,
23 again, most of the state is private-sector entities.

24 There are a lot of local governments.

25 There's more than 3,000 local governments that need

1 assistance.

2 But there's 2 million or so institutions in
3 the state of New York, almost 20 million people.

4 That squarely is the Department of Homeland
5 Security and Emergency Services' role that they
6 still carry on.

7 So that -- and, you know, in working with
8 them they recognize that role. They have the
9 targets in the homeland-security plan. And, they
10 don't do all of the activities in there. Some of
11 them are being done by other agencies, other
12 activities, but -- but they coordinate all that
13 activity and make sure that it gets done.

14 And I'm very confident that that sort of dual
15 responsibility is working.

16 SENATOR CROCI: Senator Nozzolio.

17 SENATOR NOZZOLIO: Thank you, Mr. Chairman.

18 Thank you, Doctor.

19 DR. PETER BLONIARZ: Thank you.

20 SENATOR NOZZOLIO: Thank you, Doctor, for
21 your information and help.

22 Someone with as a distinguished a career as
23 you have had, I certainly, any governor, or head of
24 Homeland Security, or head of the Division of Public
25 Protection, anyone in state-government role, would

1 benefit from your expertise, and your technical
2 background.

3 I share, though, Senator Croci's concern that
4 we have a structure to advise, but not necessarily a
5 structure to execute, particularly in terms of an
6 emergency response that's necessary.

7 And, this is not to criticize the individuals
8 who are part of this network, or to criticize the
9 Governor who put together individuals that are
10 important to the process.

11 We just heard from the FBI chief in this
12 area, how important it is for coordination of all
13 law-enforcement function; and that's not a job for
14 you. It's not a job for our technical IT folks.
15 It's not even a job for agency heads that are
16 supposed to be entrusted with protecting data.

17 I know this is not -- as you say, it is a
18 question above your pay grade, but, listening to you
19 and having the benefit of your testimony, it's
20 apparent that this advisory board is playing a very
21 important role, and could play an important role in
22 the future.

23 However, I believe Senator Croci's approach
24 on structuring this team with important lines of
25 communication and reporting, that with important

1 budgetary aspects, I listened to every second of the
2 10-hour Public-Protection Budget Subcommittee this
3 year, and I was head of the Public-Protection Budget
4 Subcommittee process for the Senate, and this issue
5 was barely addressed.

6 And it's a question, I think, that cries out
7 for accountability.

8 And, again, not that -- you're here; you're
9 helping us in terms of framing this question.

10 But as we're trying to focus on the
11 appropriate role, it -- from a management
12 perspective, this issue cries out for a structured,
13 reportable budgetary-process perspective.

14 So just by outlining what you've established,
15 help us, I think, better frame the necessity for
16 this.

17 Again, I -- if for nothing else, to execute
18 some of the great suggestions that are here, and to
19 ensure that those department heads put them forward.

20 There's a centralized, I don't want to call
21 it a database, but a Centralized Intelligence Center
22 that's located in East Greenbush.

23 Are there other centralized intelligent
24 processes throughout the state, or is that the
25 central, or the only, the singular, point for the

1 state of New York?

2 DR. PETER BLONIARZ: So is your question, are
3 there other intelligence centers in the state of
4 New York?

5 SENATOR NOZZOLIO: Yes, in terms of the role.
6 Is the -- this in East Greenbush -- is that
7 NYSIC in East Greenbush, is there any similar
8 replication of that, or is this the sole for the
9 state?

10 DR. PETER BLONIARZ: That -- that is the
11 state's designated fusion center, so that is
12 where -- and that has a cyber responsibility.
13 They're in the process of adding a team of five
14 cyber analysts into the intelligence center.
15 I mentioned it's co-located with the Center for
16 Internet Security, which is the, you know, national
17 resource for state and local government. They
18 maintain a -- you know, a significant team of
19 analysts there as well, and are getting information
20 directly from Department of Homeland Security and
21 other federal agencies along the way.

22 So, I think that -- so, are there other
23 formal intelligence-sharing mechanisms in the state
24 of New York?

25 There are -- again, we -- you know, we are a

1 piece of the solution.

2 A lot of the federal information flows to the
3 private sector through what are called "Information
4 Sharing and Analysis Centers," like the Multi-State
5 ISAC over in East Greenbush.

6 There's one the energy every sector. There's
7 one for the education sector. There's one for
8 transportation sector.

9 Every sector has such information-sharing
10 units, so that, for example, financial services,
11 last year, as part of their reviews, what their
12 study found was that a lot of the large companies, a
13 lot of the large banks, a lot of the large insurance
14 companies, are getting the information that they
15 need to protect themselves.

16 But that the smaller banks, and the smaller
17 institutions, sometimes are, you know, not getting
18 the same level of information.

19 And part of that is because they're not
20 participating in the networks that the feds and the
21 State have set up to share that information.

22 And so they encouraged -- in a formal letter
23 from the superintendent, encouraged every financial
24 institution to join the financial-sector information
25 sharing and analysis center, so that -- and, again,

1 that's a private-sector organization. That's not
2 one that the State participates directly in, but
3 they get their information from the same place we
4 do, which is, you know, the federal Department of
5 Homeland Security.

6 So, this whole issue of intelligence sharing
7 and information sharing is a delicate one because,
8 you know, a lot of times -- I mean, this was part of
9 the discussion on -- in the Hill on the federal
10 level, is we want more information, we want more
11 sharing of information, but we also want to protect
12 individuals and, you know, company secrets in the
13 process; so, figuring out what that right balance
14 is.

15 So to answer your question, there are other
16 mechanisms, but the -- NYSIC the primary state
17 government official one through which those --
18 information is communicated.

19 SENATOR NOZZOLIO: Thank you, Doctor.

20 When you participated in the Governors
21 Association forum, did -- was there any discussion
22 of what other states are doing that sort of
23 impressed you to want to implement in New York?

24 DR. PETER BLONIAZ: I think that, you know,
25 we're taking some of those steps already. You know,

1 the board -- the advisory board has been around the
2 block. Some of them are on other state commissions
3 like ours.

4 Some of the things that we are doing are ones
5 that we admire.

6 I think this expansion of the intelligence
7 center's role is one that, frankly,
8 Northern California, their fusion center is a very
9 big cyber presence and contributes significantly.

10 So, that's one model that we had already
11 started before we -- you know, before I personally
12 saw what was going on out there, but that's
13 something that we model.

14 Some of the things that we're looking at now,
15 and this gets to your question earlier,
16 Senator Croci, about, sort of, whose responsibility
17 is things, I think the Division of Homeland Security
18 recognizes they have a significant responsibility to
19 local governments, and how do we provide resources
20 to them?

21 And, again, some of the states are taking
22 similar -- some of those states are taking similar
23 initiatives.

24 Oftentimes -- you know, Senator, you
25 mentioned the ISIS threat in your opening remarks.

1 When that threat came out we got calls from
2 local government about, What is this? Should we
3 shut down our networks? Is this something we need
4 to take care of?

5 We worked with the Center for Internet
6 Security, we worked with the folks at the
7 New York State Intelligence Center; got information
8 about, Is this real? What should we be doing? And
9 then communicated that to local governments.

10 I think that that's the kind of role that
11 I see state government especially playing, is making
12 sure that those who need the information get the
13 information.

14 We don't want to give it twice to somebody
15 large that already gets the information directly
16 from the federal government, but we want to make
17 sure that everybody has the information that they
18 need to protect their information.

19 And we see that as an important role in what
20 we're doing.

21 SENATOR NOZZOLIO: Thank you very much,
22 Doctor.

23 Thank you, Mr. Chairman.

24 SENATOR CROCI: Thank you, Senator.

25 Doctor, just one final question.

1 DR. PETER BLONJARZ: Sure.

2 SENATOR CROCI: So much of the technical
3 expertise to deal with some of these challenges
4 doesn't reside within government. We just can't do
5 it all, and I think we recognize that. Certainly,
6 at the federal level they do.

7 How do we determine what goods, services,
8 skills, hardware, are required at the state level?

9 How is that determined? How is that vetted?

10 DR. PETER BLONJARZ: Sure. The first thing
11 is to start with your -- you know, how do you
12 approach what you're doing? And that's to do a
13 risk-based decision-making.

14 I mean, we could buy lots of stuff that will
15 help with problems, but if they're not problems that
16 we have or we see a lot of, there's no point in
17 solving that problem.

18 So you have to start with understanding
19 where --

20 SENATOR CROCI: Where physically does that
21 start? What department? branch? agency? office?

22 How does that begin?

23 DR. PETER BLONJARZ: Well --

24 SENATOR CROCI: I know how it's done in the
25 military. You find something that you need to

1 combat a threat, you bring your technical experts
2 together.

3 Who are those experts? How does the process
4 begin and end?

5 DR. PETER BLONIARZ: Right, again, two
6 aspects.

7 If we're talking about protecting
8 state-government-information aspects, that's in the
9 Office of IT Services.

10 SENATOR CROCI: Okay.

11 DR. PETER BLONIARZ: If we're talking about
12 protecting the state as a whole, then that's the
13 Division of Homeland Security and Emergency
14 Services.

15 SENATOR CROCI: Okay.

16 DR. PETER BLONIARZ: So -- so, you know,
17 two interrelated but separate tasks, because they
18 have separate missions.

19 So -- yeah, so in deciding --

20 SENATOR CROCI: So the need starts there.

21 DR. PETER BLONIARZ: -- in deciding --

22 SENATOR CROCI: And then how do we go out and
23 obtain those goods and services, or technical
24 expertise?

25 DR. PETER BLONIARZ: So let me talk about the

1 two of them separately.

2 With regards to state-government
3 infrastructure, where are we challenged?

4 You know, analyze the data-breach reports
5 that we that get. Analyze the incidents that we've
6 got. Analyze -- what what's going on elsewhere.

7 Some of the important things that we need to
8 pay attention to are perimeter defense; making sure
9 that we monitor our networks to see what's going on
10 there.

11 You heard earlier how, you know, this --
12 we're moving to a world where there's no perimeter.
13 Everything is in the cloud.

14 We need to protect our information in the
15 cloud, and we need to monitor what's going on,
16 because -- for anomalous patterns, to make sure
17 that, you know, information is not getting moved
18 from here to there where it shouldn't be getting
19 moved from here to there.

20 So -- and that responsibility is in --
21 clearly, in IT Services, as they're designing the
22 new network and designing the new server system, all
23 that that's going on there.

24 So they have responsibility for initiating,
25 deciding, and then executing and implementing that

1 plan.

2 SENATOR CROCI: So, initiating and -- so
3 what's the process number two?

4 I understand where the need originates, and
5 requirements.

6 Now, how do you meet the requirements in the
7 procedural and contractual in the sense for goods
8 and services and people?

9 DR. PETER BLONIARZ: It's a combination of
10 technical requirements, and then translating that
11 into the contractual requirements that the CIO's
12 office implements.

13 I mentioned that --

14 SENATOR CROCI: I'm sorry, which office?

15 DR. PETER BLONIARZ: The CIO (the Office of
16 IT Services).

17 SENATOR CROCI: Okay.

18 DR. PETER BLONIARZ: Megan Miller's office.

19 So she has a technical team that's, you know,
20 architecting the new data center that's taking all
21 the existing data centers and putting them into one
22 place, and then migrating to the new system that's
23 there.

24 As they're procuring components of that, the
25 technical components for that, security is built in

1 on the ground floor.

2 We have a team that focuses on the secure --
3 I forget the name of it, but the secure-architecture
4 group that works with the technical people to make
5 sure that those requirements are built in from the
6 beginning, so that we're building an infrastructure
7 that's capable of doing what we need.

8 SENATOR CROCI: But they're doing this
9 without the guidance and expertise of the advisory
10 board?

11 DR. PETER BLONIARZ: Well, the advisory board
12 is -- operates at a, sort of, 40,000-foot level.

13 We're recommending where the State should put
14 its emphases, one of which is to make sure that the
15 task that you're describing is being done by the
16 implementation teams.

17 You know, we don't use the advisory board as
18 a sort of unpaid consultant to come in and audit
19 what we're doing at the purchasing level; but,
20 instead, use them to set direction and emphases of
21 where that should be, and then it's up to the
22 Office of IT services to execute that. And Maggie
23 has a good team to do that.

24 SENATOR CROCI: So there's collaboration --

25 DR. PETER BLONIARZ: That's right.

1 Absolutely.

2 SENATOR CROCI: -- sort of recognizing the
3 expertise on the board?

4 DR. PETER BLONIARZ: Yeah.

5 SENATOR CROCI: Very good.

6 DR. PETER BLONIARZ: And I have -- you know,
7 as advisory board member, even before taking this
8 position, there was an ongoing, you know,
9 conversation about, What are we doing in the new
10 data center? How are we building this in?

11 My job is to, you know, be the middle person
12 between the advisory board and the people who are
13 actually executing in this state.

14 SENATOR CROCI: Doctor, thank you so much for
15 your testimony today.

16 We definitely appreciate your expertise, and
17 we look forward to working together as we go
18 forward, to ensure that we're in the best position
19 we can be in, and, certainly, the proof is in the
20 pudding.

21 DR. PETER BLONIARZ: Right.

22 SENATOR CROCI: So we'll see.

23 Thank you so much.

24 SENATOR NOZZOLIO: Thank you.

25 DR. PETER BLONIARZ: Senator, I appreciate

1 your interest, both of you, and this is an important
2 topic that we all have to work together on.

3 So, I thank you for your interest.

4 Look forward to working with you in the
5 future.

6 SENATOR CROCI: Thank you.

7 Our final witness today will be
8 Mr. Rich Dewey, the executive vice president of the
9 New York Independent System Operator (the New York
10 ISO).

11 We'd love to have you come down and take the
12 chair.

13 Mr. Dewey, thank you so much for joining us
14 today, and, I'd ask if you'd like to make any
15 opening comments.

16 We do have your testimony, so if you want to
17 highlight certain sections in deference to time,
18 that would be fine.

19 The floor is yours, sir.

20 RICHARD DEWEY: Sure.

21 Thank you.

22 You have my testimony.

23 I'm just going to hit some highlights along
24 the way, and then we can submit to questions.

25 Senator Croci, Senator Nozzolio, thank you

1 for having me here today.

2 I'm happy to present some thoughts, and
3 answer any questions that you may have.

4 For everyone else in the room, my name is
5 Rich Dewey. I'm the executive vice president of the
6 New York Independent System Operator.

7 The New York ISO is a non-profit independent
8 corporation that performs three key functions to
9 electricity consumers within New York State.

10 We manage the reliability of the electric
11 grid. We do so under -- and in compliance with a
12 myriad of standards at the local and national at the
13 level.

14 We administer the wholesale energy markets,
15 and strive to come up with the most efficient
16 dispatch of generation to serve the load and the
17 consumers of New York State.

18 And we also are responsible for planning the
19 state's energy future for reliability and for
20 demand. And as part of that role, we are non-voting
21 members of the New York State Energy Planning Board.

22 As an independent entity and resource, we
23 provide, and strive to provide, authoritative
24 information-resource analysis for market
25 participants, regulators, and policymakers like

1 yourself.

2 We take pride in our independent role, and we
3 strive to be the honest brokers of information of
4 all matters related to the power grid and to the
5 energy industry.

6 As the executive vice president, I've got
7 responsibility for those three functions within the
8 New York ISO, overseeing the operations, the markets
9 group, the planning organization, as well as
10 information technology.

11 I've been with the New York ISO since 2000.
12 I just celebrated 15-years anniversary.

13 I got a bachelor of science in electrical
14 and computer engineering from Clarkson University,
15 and a master of science in engineering from
16 Syracuse University.

17 The New York State electricity consumers have
18 enjoyed benefits of 15 years of competitive markets.

19 We have the most stringent set of reliability
20 standards that we operate the grid to in the
21 country.

22 We feel that we operate the most efficiency
23 energy markets for the benefits of consumers.

24 And some of the efficiency improvements that
25 we've introduced through 15 years of competition

1 into the system have yielded significant benefits
2 and savings and prices and in energy costs to
3 consumers, as well as significant reductions in
4 emissions and environmental improvements to the air
5 quality within New York State.

6 As part of those reliability functions, we
7 take very, very seriously the role, and pay
8 attention to the risk of cyber-security threats to
9 our industry.

10 The entire electric industry has been working
11 very, very closely and diligently for quite some
12 time; since 2006, really. And as such, we feel that
13 we've got a pretty mature set of standards and
14 reliability roles that we comply with relative to
15 other critical infrastructure in the country.

16 Operating through the North American Electric
17 Reliability Corporation, which is the enforcement
18 arm of the federal Energy Regulatory Commission, we
19 have developed and enforced sets of
20 critical-infrastructure protections standards, or
21 "CIP standards," way back since 2006.

22 We operate and continue to evolve these
23 standards. We subscribe to the notion of continuous
24 improvement.

25 We are getting set as an industry to

1 implement Version 5 of those standards since the
2 inception of the process.

3 And we submit regularly to audits, where all
4 responsible entities need to demonstrate compliance
5 with those standards. And those are some fairly
6 rigorous audits that take place on a regular basis.

7 The CIP standards employ a lot of the
8 industry-leading practices that you've heard
9 mentioned today -- looking at access control, asset
10 identification, continuous monitoring -- really,
11 defense in depth, where we look for layers of
12 protection to protect the system so we're not
13 reliant on any one technology or any one defense
14 mechanism to protect the industry as a whole.

15 The New York ISO is regularly recognized as
16 an industry leader.

17 We participated in the development of those
18 standards at the national level through NERC, and
19 we've got a very strong track record of compliance
20 and success against the audits against which we're
21 measured.

22 Beyond these mandatory standards, the
23 electric industry has also established a strong
24 system of information sharing, both formally and
25 informally.

1 Some of the other -- some of the other
2 speakers have talked about these mechanisms for
3 sharing information, and the importance of it within
4 the industry itself.

5 You look at cyber threats, and the reality
6 is, they're continuously evolving. On a daily basis
7 we've got new threats.

8 And the best security schemes employ active
9 information sharing so entities can respond to this
10 changing threat landscape as quickly as possible.

11 It's not only the frequency of information
12 that's important, but it's the quality of that
13 information as well, so that entities can be made
14 aware of the evolving threat landscape and then
15 change their defenses to react and respond to that.

16 On the formal basis, the New York ISO
17 participates actively with the Department of
18 Homeland Security, the FBI, the Department of
19 Energy, and the North American Electric Reliability
20 Corporation, or "NERC," to share information about
21 these events.

22 We also have established, and we've been
23 leaders in the industry to establish, more effective
24 informal information sharing between like entities.

25 For example, the ISO RTO Council, which is

1 made up of the nine entities in North America that
2 run competitive markets within the industry, has
3 established a security working group that meets at
4 least monthly, and frequently -- more frequently
5 during phone conversations, to share the most
6 current information about threats.

7 The New York ISO has recently worked
8 collaboratively within New York State, for example,
9 to establish a similar informal information
10 sharing between the electric utilities within
11 New York State.

12 And you heard from Dr. Bloniarz. We actually
13 have involved him in some of our conversations as
14 well, to make sure that state government and state
15 agencies have access to that very same information
16 sharing.

17 We feel that these informal mechanisms for
18 sharing information are an outstanding precursor to
19 some of the more formal processes that evolve, and
20 allow us to really, not only share information about
21 threats, but information about best practices, and
22 help each other, just as an industry, establish
23 better defenses.

24 In addition to having good information
25 sharing, it's also vital and important to establish

1 the right kind of recovery plans and resiliency
2 plans for when there is an event.

3 And you heard a lot about some of the
4 high-profile public events that some companies have
5 encountered.

6 Every organization and entity needs to go
7 into the process with the assumption that, one day,
8 they're going to have a problem, they're going to
9 have a breach of some sort. And then it's a matter
10 of having the right kind of recovery plans and
11 resiliency strategy to recover as quickly as
12 possible, and to mitigate that damage and restore
13 service to your customers.

14 The New York ISO has been active at the
15 formal national level with developing these plans.

16 In October of last year we actually took a
17 leadership role to conduct a New York State cyber
18 exercise, where we invited all of the electric
19 utilities within New York State, also the Department
20 of Energy, the federal Department of Homeland
21 Security, New York State Department of Homeland
22 Security, and we actually conducted a two-day drill
23 at our offices over in East Greenbush, New York,
24 where we simulated an event, a combination physical
25 and cyber-security event, to test each of the

1 entities on the completeness and accuracy of their
2 recovery plans, and also to test those inter-agency,
3 inter-organization, communication paths that would
4 be so important and vital during a critical event.

5 The results of that exercise were
6 encouraging, in terms of the readiness of the
7 electric industry to respond to these types of
8 events, as well as the spirit of collaboration that
9 takes place between agencies, both public and
10 private organizations, in sharing that information.

11 And we were very happy to share that
12 information with New York State agencies as well.

13 In support of our mission to provide the most
14 reliable service, New York ISO looks forward to
15 supporting the Committees' efforts to strengthen
16 cyber-security posture of the state and of the
17 industry as a whole.

18 I want to thank you for the opportunity to
19 present these initial comments, and I'd be pleased
20 to answer any questions you may have about the
21 statements or testimony that I submitted.

22 SENATOR CROCI: Thank you Mr. Dewey.

23 Senator Nozzolio.

24 SENATOR NOZZOLIO: Thank you, Mr. Chairman.

25 Vice President Dewey, thank you for your

1 input.

2 How did that drill go?

3 It was -- it sounds like it was quite a fire
4 drill, if you will.

5 RICHARD DEWEY: It was.

6 SENATOR NOZZOLIO: What -- how many did you
7 have -- how many participants?

8 And, was there anything you discovered that
9 needs work?

10 RICHARD DEWEY: Yeah, that's a great
11 question.

12 We had 120 participants: 15 electric and gas
13 utilities across New York State, almost every
14 New York State agency, that has a stake or a role or
15 is involved in the protection of cyber-security
16 assets.

17 The way the drill was conducted is, we
18 provided a simulation, a timeline of imaginary or
19 simulated events, of increasing catastrophic impact.

20 It involved, both, cyber-security attacks, it
21 involved a simulated or a pretend supply-chain
22 problem, and then we followed that up with a series
23 of staged and simulated physical attacks.

24 Each of the entities that was involved in the
25 drill was asked to describe what processes they

1 would follow within their own operation.

2 What was their plan for recovery?

3 How would they notify their customers?

4 Who would they contact?

5 At what various points would they establish
6 communication with the various government agencies,
7 law enforcement, et cetera?

8 And then we stepped the entire process
9 through for a one-day period, to explore if there
10 was any problems, if there was any issues, or, was
11 there somebody that didn't know what to do?

12 The following day we recreated the same
13 exercise with the CEOs of each of those
14 organizations.

15 So, at the top level of management, we wanted
16 to make sure that everybody understood what the
17 strength and weaknesses of each of their plans was,
18 and to demonstrate that we knew how to work together
19 as an industry to be able to address a catastrophic
20 attack like we had simulated.

21 We were very encouraged that every entity had
22 very, very robust plans within their organizations.

23 Every one of the executives that took part in
24 the exercise had deep knowledge and very specific
25 informed information about what each of their

1 organizations would need to do in the event of a
2 crisis of that nature.

3 And it really gave us a lot of encouragement
4 that the industry was well-positioned and
5 well-postured to be able to deal with an exercise.

6 SENATOR NOZZOLIO: Was this the first time
7 you ever engaged in that type of exercise at that
8 level, that scale?

9 RICHARD DEWEY: The North American Electric
10 Reliability Corporation, or "NERC," holds a national
11 exercise of similar design every two years.

12 This is the first time that we really focused
13 it on just the entities within New York State, and
14 to try to focus on those relationships and those
15 communication paths within the state itself.

16 It was a very good event to reinforce that
17 the plans we had in place were solid.

18 Some of the areas that we looked to improve,
19 or recognized is the need to maybe have SOME
20 improvements, IS in the area of communication
21 command and control during the crisis itself; that
22 clear realization over who is in charge at what
23 points in time.

24 So when you go through an event like this,
25 you start out, you think it's very localized. Then

1 you suddenly realize, "It's not just me. It's
2 everybody in the state." And there's an escalation
3 point where you involve various levels of law
4 enforcement.

5 And, ultimately, when you realize that it's a
6 large-scale event, somebody much higher in state
7 government, probably from the Governor's Office,
8 then needs to get involved, and, then, which
9 agencies are in charge of which aspect of that.

10 And there was different timing
11 considerations.

12 And, it helped us fine-tune some of our own
13 procedures, quite honestly.

14 SENATOR NOZZOLIO: Did you establish a series
15 of protocols as a result that are ingrained, or is
16 it still a work in progress?

17 RICHARD DEWEY: We did establish an
18 after-action report that summarizes the findings and
19 some of the next steps.

20 Dr. Bloniarz talked about the April session
21 that was held at the New York State Department of
22 Public Service. We used our report from the exercise
23 in October to start the conversation at that.

24 So, even from the time we did the drill in
25 October, until the Public Service Commission had

1 their event in April, we could see progress made,
2 procedures that were tightened up.

3 And I think that there's a pretty good path
4 going forward now if we ever --

5 SENATOR NOZZOLIO: Do you plan to continue
6 these types of exercises on an annual, semiannual,
7 basis?

8 RICHARD DEWEY: We do, we do.

9 It's vitally important not only to continue
10 to test and validate your plans as new people come
11 into the organizations, but as new threats become
12 available and visible on the landscape, you need to
13 be able to have those kind of tests on your
14 processes and procedures.

15 At this point, our plan is that we're going
16 to all participate in the NERC national event which
17 will take place in November of this year, and then
18 we'll immediately start planning for another
19 New York State event on the subsequent year in 2016.

20 SENATOR NOZZOLIO: Mr. Dewey, is there any
21 integration between your report or an assessment
22 with the Governor's task force that -- on cyber
23 security that we just heard from?

24 RICHARD DEWEY: There was very good alignment
25 between the information that we learned from our

1 drill and the Governor's plan.

2 SENATOR NOZZOLIO: How about Homeland
3 Security per se, were they part of --

4 RICHARD DEWEY: Homeland Security, both at
5 the New York State level and at the national level,
6 were -- participated in the drill and were involved
7 in the plan, yes.

8 SENATOR NOZZOLIO: At the state level, as
9 well as the national level?

10 RICHARD DEWEY: Yes, sir.

11 SENATOR NOZZOLIO: How about local law
12 enforcement or -- by "local" I mean, all law
13 enforcement -- let me strike that.

14 All law enforcement, from the local PDs, to
15 the state police, to the FBI, and beyond, is a --
16 were they integrated into this process?

17 RICHARD DEWEY: The New York State Police did
18 participate in the drill as observers.

19 And, the local Albany FBI office also
20 participated in the drill, and we shared some of the
21 results of that exercise with them.

22 So, they were very involved.

23 SENATOR NOZZOLIO: I'm not asking for
24 specifics of what you found, but it would be very
25 interesting to see, at some point, were there any

1 impact of law that needed to be changed to be
2 able -- for you to engage in fully doing your job
3 should there be a cyber attack?

4 That, I think, we'll keep for another day,
5 the discussion.

6 But, just moving into that area for a second,
7 if I may, Mr. Chairman, I think that it would be
8 very helpful to know how you assess the risk.

9 We've had testimony today, saying that
10 companies believe that 70 percent of them either
11 have been attacked, or even more anticipate attack.

12 What is the general belief among the --
13 your -- you and your peers across the country on
14 this issue?

15 RICHARD DEWEY: I think that the strategy has
16 evolved from one of defense to one of resiliency.

17 The aspects of defense and to build those
18 tight walls so the bad guys can't get in is a part
19 of every good security plan, good defense mechanism,
20 but it's not sufficient.

21 You have to assume that, at some point, that
22 those defenses are going to be -- that those
23 defenses are going to be breached, and you need to
24 approach it from a standpoint of resiliency, where
25 you look at the design of your systems itself, and

1 try to define and design your networks and your
2 software systems such that any one component of it
3 is not so integral to the entire system, that you
4 could lose a piece of it and still provide service.

5 There's also the aspect of planning for very
6 quick resolution.

7 So when a system is -- is breached or somehow
8 compromised, you've got to have recovery plans that
9 can very rapidly isolate that system, and then
10 replace it with some capability so that the
11 enterprise or the corporation can go on with
12 business, and do so as quickly as possible.

13 That approach, coupled with a defense
14 in-depth strategy, where there's -- you know, you
15 don't just have one firewall that blocks your whole
16 network. You have layers of defenses, where
17 different levels of access and different levels of
18 tests and validation need to be challenged at every
19 step of the way, and then, that way, if you've got
20 one vulnerability, it's not sufficient to get all
21 the way through to, say, take out the entire
22 capability of your organization.

23 So that new approach to design of systems,
24 and to plan for that resiliency and recovery, really
25 helps mitigate the risk of what many people believe

1 is an inevitability: that every organization, at
2 some point in time, is going to be impacted in some
3 way.

4 You just try to minimize it so that it
5 doesn't disrupt the service to your customers or to
6 your stakeholders.

7 SENATOR NOZZOLIO: I know this is a daunting
8 task, and I know you are not responsible for,
9 certainly, every generator of electricity in this
10 state.

11 I know most generators have their own
12 private -- not all -- generators have their private
13 security forces. Rely on local law enforcement as
14 well.

15 In terms of protocols, besides the -- what
16 sounds like an excellent drill that you engaged in
17 and managed, what about the protocols established in
18 terms of danger from within?

19 There was testimony, I think, by the FBI
20 about that being a concern; not to indict any
21 employees, but some terrorist group or some
22 individual who wanted to do damage that was part of
23 the network, that was part of the inside, if you
24 will, or had inside -- had significant inside
25 information.

1 What's the confidence level that that's being
2 monitored and policed?

3 RICHARD DEWEY: Insider threat is one of the
4 most challenging -- challenging threat factors to
5 protect from, because you do all the up-front work
6 that's prudent and necessary to assure that the
7 individual that you're bringing into the
8 organization can pass all the tests.

9 So, we do background checks, seven or eight
10 different types of background checks, on every
11 person's history, plus references, plus
12 law-enforcement checks, before they come into the
13 organization.

14 And even then, you never know if their
15 philosophical, their socioeconomical, situation
16 might change.

17 They could -- you know, they could be the
18 model citizen when they come into your organization.
19 And then something could happen in their life such
20 that they get influenced in some way, that you've
21 got to be concerned about what their -- you know,
22 what their intent is.

23 We approach it at the New York ISO by
24 establishing the access to the systems, that you
25 only are given access to what you need to do, what

1 you need to perform the job that you're hired to do.

2 So, you don't have cart blanche on every
3 system. You've only got that access to be able to
4 interface with the systems that are necessary for
5 your job.

6 And for those critical systems, there's a lot
7 of checks and balances, where, to perform certain
8 critical functions, no one person with their access
9 can do it.

10 It's very similar and analogous, we heard the
11 airline description today, there's two co- --
12 there's two pilots in the cockpit at every time.

13 A lot of the functions necessary to actually
14 operate, and the command and control necessary to
15 maintain reliability, of the power grid require
16 multiple individuals to act in concert to be able to
17 carry out the key functions.

18 So a lot of the key functions are designed
19 with that in mind, and then, that way, you've got
20 the checks and balances so no one person with a
21 specific malicious intent can cause that much
22 catastrophic damage.

23 It's very similar to, we heard the
24 conversation about the human in the loop.

25 It's very analogous to what goes on in the

1 management of the power grid.

2 We've got highly automated, highly
3 computerized algorithms, that maintain the
4 reliability and the balance of power delivery on the
5 power grid.

6 But, still, 24/7, 365, we've got
7 6 control-room operators sitting in our control room
8 that are looking at those advisory outputs,
9 monitoring what the computers are doing, following
10 their own checks and balances, and human controls,
11 and ready to intercede whenever something looks like
12 it's not operating like it should.

13 So, in that way, you've got the humans
14 watching the computers, if you will. And that human
15 in the loop is so important to combat a lot of the
16 risk, or to mitigate a lot of the risk, of what is
17 increasingly becoming a highly-automated society.

18 SENATOR NOZZOLIO: Are these national
19 standards that we've established since
20 September 11th, pretty much?

21 RICHARD DEWEY: There are national standards
22 for electric-system reliability that have been in
23 place for years.

24 A lot of the security standards have evolved
25 over the years as certain events, such as

1 September 11th; such as, for example, the
2 power-system event that happened on the east coast
3 in 2003, where a reliability situation in the
4 midwest cascaded through Ontario and New York and
5 created widespread outages.

6 That resulted in much more stringent and
7 mandatory reliability standards that were put in
8 place.

9 Also put in place at that time were much more
10 significant and broad power-system monitoring and
11 management tools, so that we can monitor what's
12 going on the power grid well outside of our borders,
13 so we can get advanced notice of reliability events
14 that can take place way out in the midwest or down
15 in the south.

16 So as these events happen, we're continuously
17 looking to improve our standards, continuously
18 looking to improve our processes and controls, to be
19 able to mitigate the effect of similar events, and,
20 hopefully, prevent similar events.

21 And, as Senator Croci commented, you know,
22 hopefully, try to prevent hypothetical events, and
23 continuously think of those disastrous-type things
24 that we hope never happens; but if they did, what
25 would we do in preparation for it?

1 SENATOR NOZZOLIO: Thank you very much.

2 SENATOR CROCI: Thank you, Senator.

3 Mr. Dewey, the -- when we think of critical
4 infrastructure, I can't think of a more critical
5 sector of our infrastructure than energy.

6 Nothing highlights that better than the
7 events of September 11th, and how power affected
8 communications.

9 Nothing illustrates that better than the
10 events of "Superstorm Sandy," and how power affected
11 communications, and our ability to power our homes,
12 and our ability to power our backup generators and
13 get fuel supplies to the generators.

14 That is the most critical of critical
15 infrastructure. Our national defenses, our state
16 defenses, everything relies on power.

17 I've been pleased, and at ease, in working
18 with the ISO, because I know that you're doing
19 everything in your power, pun intended, to ensure
20 that when disaster strikes -- well, first of all,
21 you're in a better position to prevent disaster,
22 but, when disaster strikes, that we have the power
23 to deal with whatever that incidence is.

24 I'm very appreciative of your testimony and
25 some of your comments.

1 I heard "informal processes" with the state.

2 I hope that those are in the process, and
3 maybe you can speak to, will those processes be
4 codified?

5 And I would also like to have you -- well,
6 let's start with that one.

7 Your contact with the state, and the informal
8 setting, and how we can codify that? Or --

9 RICHARD DEWEY: Sure.

10 I'll talk generally about what I see to be
11 some of the challenges and barriers to effective
12 information sharing, and then how that gets
13 established in terms of law or policy.

14 I think it will be just be important to
15 recognize it with what the strength and weaknesses
16 are.

17 One of the barriers to information sharing
18 is, is entities and organizations are sometimes
19 unwilling to disclose certain information if they
20 think it's going to lead to public-relations
21 problems for them or embarrassment at the public
22 level.

23 So if you're an organization, whether it's a
24 department store or some entity who has just
25 experienced a security breach, it would be most

1 effective for society and for the industry if they
2 would broadcast and publish the details of that
3 breach such that any other organization that employs
4 similar systems or tactics could maybe examine their
5 defenses to make sure that they won't be the next
6 target.

7 But if that organization is concerned about
8 the publicity that -- the negative publicity that
9 they're going to get from disclosing that
10 information, then they're subjected to weighing the
11 risks of, What's the PR hit that I'm going to take?
12 as compared to, How I can benefit society or my
13 competitor down the street by sharing the
14 information.

15 So I think that information sharing needs to
16 be encouraged, and the entities need to be assured
17 that they can do it in a way that protects their
18 reputation to the greatest extent possible.

19 We want the information to get out, because
20 the most effective information is hearing from your
21 friends and neighbors about the types of experiences
22 that they've had, so you can fix your own defenses,
23 but you don't want people to be disincented from
24 sharing that.

25 It's -- you can do that through mandatory

1 requirements.

2 You can -- you know, there are, certainly
3 within our industry, because it's just so vital to
4 national defense and society that we share
5 information, there are standards and requirements
6 that we're obligated to comply with as a mandatory
7 matter of practice and law.

8 But, at the lower level, and across more
9 private organizations, you still want to get that
10 information shared, but you want the organizations
11 to feel comfortable in doing so.

12 I also heard earlier about a question, you
13 know, How do we incentivize entities to want to do
14 that?

15 The easiest way that I can think of is, give
16 them something back. Right?

17 So, a lot of times we're in this situation
18 where we have the mandatory and obligatory
19 reporting, so we ship it off -- we ship the
20 information off to the federal organization that
21 we're responsible for reporting it to.

22 But, how frequently do we get actionable and
23 useful information back about other threats, that
24 then I can use to protect myself and to harden my
25 defenses?

1 So I think that, you know, that's an
2 important piece of it as well: Not just to harp on
3 the obligation to report, but think about, What are
4 the benefits to the organization in terms of
5 complying with that? And how can we make it so that
6 they are incentivized in a meaningful way so that
7 they want to participate?

8 SENATOR CROCI: Your organization is a
9 not-for-profit corporation?

10 RICHARD DEWEY: That's correct.

11 SENATOR CROCI: Are you in any way involved
12 in an advisory role with our state government,
13 either on the Governor's Advisory Board, or in other
14 capacity, other than in your exercises?

15 RICHARD DEWEY: No.

16 I have participated and spoken at a couple of
17 the advisory board meetings, as invited by the
18 board, Dr. Bloniarz.

19 We do participate very collaboratively,
20 through your stakeholders process, and through some
21 of our planning sessions with New York State
22 government, at the Public Service Commission level,
23 with Department of Homeland Securities, with -- we
24 participate very frequently with the Federal Bureau
25 of Investigation in terms of regular briefings and

1 industry updates that we have with them.

2 As far as a formalized, structural, codified
3 way? No.

4 We -- we're an independent entity, we're a
5 501(c)3. We operate under an independent board that
6 has no connection to any of the stakeholder groups
7 that we serve.

8 That independence is important, to make sure
9 that we've got the most bipartisan influences, if
10 you will, in terms of coming up with -- you know,
11 being that honest information broker about future
12 plans, and how the markets are running, and how
13 reliability is maintained.

14 SENATOR CROCI: And you mentioned previously
15 that, during the course of an event, sometimes the
16 scope can change.

17 And as a state organization, a state
18 structure, it's not clear always who might be in
19 charge in the response and recovery phases
20 post-disaster.

21 Are we any clearer, or are you clearer, that
22 if something happened tomorrow, you would know, as
23 the event escalated, where to go, that single point
24 of contact within our state infrastructure?

25 Similar to the national-response framework,

1 do we have that clarified, from your perspective as
2 a state entity?

3 RICHARD DEWEY: I think we do. I think it's
4 a lot more clear.

5 It -- absolutely, we learned a lot from the
6 exercise.

7 We learned as an industry, and not just
8 myself, but the other entities, such as the
9 utilities, public and gas, that participated in it.

10 We learned a lot about what the roles and
11 responsibilities are for a number of the agencies
12 that, prior to that event, was just alphabet soup
13 for some entities.

14 I think that we came out of that with a much
15 clearer understanding of what the role of DHS Energy
16 Services is, of what the role of ITS is, of what the
17 role -- when to call the FBI, and under what
18 circumstances.

19 I worry that it's more a function of
20 everybody knowing who's the right person in their
21 rolodex, as opposed to, exactly, does everybody know
22 what to do --

23 SENATOR CROCI: Which highlights our concern
24 about codifying some of these relationships,
25 because, very often in government, people come and

1 go, and industry as well.

2 And if these structures are in place, which
3 was the point of the national-response framework,
4 and some of our emergency-management protocols, that
5 we have a better chance of ensuring that there is a
6 blueprint, regardless of the situation and
7 regardless of the personalities.

8 Would you agree with that?

9 RICHARD DEWEY: Absolutely. I think it would
10 certainly improve the structure.

11 Also, continuous drills, like the exercise
12 that we sponsored in October.

13 As people change, as organization structure
14 changes, just to test and validate that the
15 structure is well known, and test and validate that
16 the plans are updated such that the people that need
17 to make decisions at those critical junctures know
18 which decisions to make and who to contact.

19 SENATOR CROCI: And that was my last
20 question.

21 At the federal level there's a national-level
22 exercise in various areas yearly. It's put on by
23 the Executive Branch.

24 Certainly, all the departments and agencies,
25 it's an inter-agency drill, very helpful.

1 So much of what have we've learned about how
2 to deal with whether it's -- in the all-hazards
3 sphere; where it's a natural disaster or a terrorist
4 act, comes from the lessons we've learned at those
5 national-level exercises (unintelligible).

6 We have employed that at the county and the
7 town levels in recent years, to try to have that
8 same level of preparedness.

9 Do you recommend -- obviously, you had a very
10 successful drill that you sponsored.

11 Would you recommend the State take on the
12 responsibility of having that kind of a -- not an
13 NLE, but an SLE?

14 RICHARD DEWEY: I can tell you that, in my
15 experience, you can never practice your
16 crisis-management skills too frequently.

17 When you're faced with an actual crisis, and
18 there's that confusion of "Who's in charge, and what
19 do I do?" having had benefit and experience of going
20 through and having drilled that, just prepares, you
21 know, whatever those first responders or individuals
22 who need to take action or make decisions, it
23 absolutely helps.

24 SENATOR CROCI: We say, "Train like you
25 fight; fight like you train."

1 RICHARD DEWEY: Yep. And we're in a fight.

2 SENATOR CROCI: Right.

3 Thank you very much.

4 If you have no other questions, Senator?

5 SENATOR NOZZOLIO: No.

6 Very helpful. Thank you.

7 RICHARD DEWEY: Okay. Thank you.

8 SENATOR CROCI: Thank you so much.

9 And just to close, I want to thank our -- all
10 of our witnesses today; certainly,

11 Special Agent Freese from the FBI; Dr. Bloniarz,
12 executive director at Cyber Security Advisory Board;

13 Mr. Richard Dewey, thank you again;

14 And, Mr. Brown from CA Technologies.

15 Our purpose today was stated in the
16 beginning, but, we just want to make sure that our
17 government, the people who work in government, have
18 the appropriate level of unease and anxiety that the
19 general population has about the threats that we
20 face in the cyber world.

21 And I think that my colleagues and
22 I certainly do, and we will help spread that unease
23 until we're completely confident that we have done
24 everything we can, because the worst thing that we
25 can do is wake up the day after a cyber attack and

1 say, You know, we could have done X, Y, or Z.

2 So this body is certainly committed to that.

3 And, I want to thank you all for your
4 participation.

5 (Whereupon, at approximately 2:10 p.m.,
6 the joint public hearing held before the three
7 New York State Senate Standing Committees
8 concluded, and adjourned.)
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25