JOINT HEARING BEFORE THE NEW YORK STATE SENATE
STANDING COMMITTEE ON CODES,
STANDING COMMITTEE ON CONSUMER PROTECTION, AND
STANDING COMMITTEE ON VETERANS, HOMELAND SECURITY,
AND MILITARY AFFAIRS

PUBLIC HEARING:

TO ADDRESS NEW YORK STATE'S CYBER SECURITY
INFRASTRUCTURE, INCLUDING THE CHALLENGES, RISKS, AND
PROTOCOLS USED TO PROTECT STATE INFORMATION,
HARDWARE, SOFTWARE, AND SYSTEMS

Legislative Office Building
Hamilton Hearing Room B
181 State Street
Albany, New York 12247

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

PRESIDING:

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

Senator Michael F. Nozzolio
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

SENATOR CROCI: My name is Senator Tom Croci.

I want to thank you all for joining us today.

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

Welcome to our public hearing on cyber security.

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

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

Senator Simcha Felder has also joined us today.

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

Recently, ISIS put out a video on the web,

threatening a cyber attack on the United States.

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

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

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

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

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

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

up to, and are addressing, that challenge.

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

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

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

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

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

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

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

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

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

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

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

In addition to the previous public hearings,

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

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

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

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

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

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

We have to use any tools that we have at our

disposal to address the coming threat.

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

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

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

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

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

Senator.

SENATOR NOZZOLIO: Thank you very much.

Thank you very much, Senator Croci.

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

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

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

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

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

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

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

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

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

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

So, thank you to my colleagues for their attention.

SENATOR CROCI: Thank you, Senator.

Senator Venditto.

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

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

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

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

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

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

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

So without further ado, I'm hoping to hear

from our presenters.

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

SENATOR CROCI: Thank you, Senator.

And, Senator Golden.

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

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

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

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

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

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

sectors -- but all sectors are vulnerable.

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

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

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

Not every incident is a breach.

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

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

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

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

Larger companies and entities have resources,

but these can be improved.

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

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

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

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

Thank you, Mr. Chairman.

SENATOR CROCI: Thank you, Senator Golden.

Would anyone else like to (inaudible)?

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

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

If you would join us.

Of course, CA Technologies is well known, a

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

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

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

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

JAMIE BROWN: Great. Thank you very much.

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

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

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

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

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

We currently have more than 1500 employees in

our Long Island and Manhattan offices.

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

The threats we face in cyberspace are real and growing.

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

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

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

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

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

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

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

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

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

CA was also an active participant in this development process.

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

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

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

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

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

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

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

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

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

The second cybersecurity-policy principle is flexibility.

Flexibility in policy allows for adaptability in security approaches.

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

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

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

and cost-effective approach.

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

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

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

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

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

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

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

S-3407 tasks the Division of Homeland

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

You preempted a lot of my questions in your

testimony.

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

JAMIE BROWN: Thanks.

Well, very good question.

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

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

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

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

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

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

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

JAMIE BROWN: Well, yes.

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

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

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

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

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

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

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

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

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

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

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

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

What are our most important assets?

What is the unique threat environment that we face?

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

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

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

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

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

cyber-security priorities?

SENATOR CROCI: Thank you.

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

SENATOR NOZZOLIO: Thank you, Senator Croci.

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

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

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

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

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

Have you had an opportunity to review that at all?

JAMIE BROWN: I have not at this point.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

measures so that we can analyze it.

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

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

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

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

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

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

understand and compliance in different states.

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

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

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

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

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

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

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

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

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

And thank you for your participation.

SENATOR CROCI: Thank you, Senator.

Senator Venditto.

SENATOR VENDITTO: Senator Croci, thank you.

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

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

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

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

So that would be great to follow up there.

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

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

JAMIE BROWN: It's an excellent question.

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

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

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

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

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

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

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

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

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

SENATOR VENDITTO: And I appreciate that answer.

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

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

SENATOR CROCI: Thank you, Senator.

Senator Golden.

SENATOR GOLDEN: Thank you, Mr. Chairman.

And thank you for your testimony here today.

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

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

The Simple credit cards, no chips; right?

JAMIE BROWN: Yeah.

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

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

But here's the Simple card.

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

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

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

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

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

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

How do we do that?

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

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

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

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

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

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

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

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

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

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

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

JAMIE BROWN: Yeah, sure.

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

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

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

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

I this the CEO was let go. There was some turnover on the board as a result.

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

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

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

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

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

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

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

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

JAMIE BROWN: Right.

SENATOR GOLDEN: Correct?

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

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

SENATOR GOLDEN: We have to do it, unfortunately.

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

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

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

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

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

It's got to be a continuous movement.

SENATOR GOLDEN: Two more quick questions.

JAMIE BROWN: Sure.

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

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

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

Are you encountering a lot of that?

JAMIE BROWN: Yeah.

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

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

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

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

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

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

MTA, water supply, electrical grids.

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

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

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

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

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

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

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

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

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

SENATOR GOLDEN: Thank you, Peter.

SENATOR CROCI: Thank you, Senator.

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

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

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

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

JAMIE BROWN: Thank you.

SENATOR NOZZOLIO: Thank you very much.

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

Special Agent Freese is the director of the

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

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

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

DONALD W. FREESE: (Microphone turned off.)

Thank you, Senator. Appreciate it very much, sir.

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

DONALD W. FREESE: Good morning, Senator.

I do have some opening statements --

SENATOR CROCI: Please.

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

(Inaudible.)

SENATOR NOZZOLIO: His mic's not on.

SENATOR CROCI: There might be a button.

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

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

How's that work?

SENATOR CROCI: You got it.

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

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

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

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

I understand the challenges you face, and

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

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

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

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

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

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

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

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

crimes.

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

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

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

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

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

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

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

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

First being cyber terrorists.

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

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

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

operations.

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

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

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

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

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

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

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

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

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

Moving down a list of priorities, we move to

financial actors and those motivated by financial gain.

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

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

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

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

The segment of cyber-threat spectrum covers

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

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

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

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

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

unwitting accidental data leaks or destruction.

I'll leave you with one final example.

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

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

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

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

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

I would submit myself for your response.

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

And, I have one question from Senator Addabbo.

SENATOR ADDABO: Thank you.

Thank you, Mr. Chair.

Thank you Mr. Chair.

I want to thank yourself, the veteran Committee Chair;

Senators Nozzolio and Senator Venditto, thank you very much;

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

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

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

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

I want to expand a little bit to airports and

aircraft.

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

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

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

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

I would like you to weigh in on that issue.

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

DONALD W. FREESE: Okay.

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

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

DONALD W. FREESE: Right, absolutely.

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

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

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

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

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

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

vulnerabilities.

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

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

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

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

Any type of intrusion by some type of actor

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

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

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

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

Is that an ongoing investigation?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Chairman Croci, thank you very much.

SENATOR CROCI: Thank you, Senator.

DONALD W. FREESE: Thank you, Senator.

SENATOR CROCI: Senator Nozzolio.

SENATOR NOZZOLIO: Thank you very much.

I add my gratitude for your excellent testimony.

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

DONALD W. FREESE: Sure.

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

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

injured as an organization?

Your thoughts?

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

DONALD W. FREESE: Sure.

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

Do I have that question correct, sir?

SENATOR NOZZOLIO: Yes.

DONALD W. FREESE: Okay.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

occurred so that we can help mitigate that threat.

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

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

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

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

We've always been an international hub of commerce.

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

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

Is that correct?

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

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

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

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

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

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

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

So I would heartedly recommend support of programs like that.

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

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

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

You have several joint terrorism task forces,

very successful, here in New York State.

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

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

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

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

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

of cyber defense, cyber-security.

And so I would recommend those programs to you strongly.

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

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

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

DONALD W. FREESE: Yes, sir.

SENATOR NOZZOLIO: Appreciate it.

SENATOR CROCI: Thank you, Senator.

Any further questions for this witness?

Director Freese, I just want to thank you.

You preempted all of my questions.

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

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

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

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

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

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

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

Thank you, Mr. Chairman.

SENATOR CROCI: Thank you, sir.

SENATOR NOZZOLIO: Thank you, Director.

DONALD W. FREESE: Thank you.

SENATOR CROCI: Thank you, sir.

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

Good morning, Doctor.

How are you?

DR. PETER BLONIARZ: (Microphone turned off.)

(Inaudible.)

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

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

SENATOR CROCI: Push the button.

DR. PETER BLONIARZ: (Microphone turned on.)

I would like to thank the Senators, especially Senator Croci, Senator Nozzolio, and Senator Venditto, for the invitation to speak this morning.

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

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

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

and her team to protect New York government infrastructure.

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

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

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

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

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

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

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

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

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

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

We see four roles that the state government plays.

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

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

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

needed in law enforcement and homeland security.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CIS operates a 24-by-7 security operation

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

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

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

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

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

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

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

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

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

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

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

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

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

Recognizing the significant step that

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

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

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

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

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

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

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

And, finally, we will continue to remind

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

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

I thank you, Senators, for your attention.

I look forward to your questions and our conversation.

SENATOR CROCI: Thank you, Doctor. I appreciate your testimony here today.

Just a couple of questions.

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

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

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

DR. PETER BLONIARZ: I very much think so.

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

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

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

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

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

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

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

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

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

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

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

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

Sorry about that.

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

I think that input from everybody is extremely important --

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

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

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

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

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

But we've had --

SENATOR CROCI: In what sectors, for instance?

DR. PETER BLONIARZ: The -- Dick Clark is cyber-security industry.

Phil Reitinger was the former director at Sony -- the cyber-security director at Sony.

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

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

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

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

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

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

health sector. We may run two of those.

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

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

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

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

It's --

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

DR. PETER BLONIARZ: As members of the board?

I think we're getting the input that we need from the private sector at this point.

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

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

SENATOR CROCI: Understood.

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

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

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

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

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

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

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

What kind of traffic is going out of the network?

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

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

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

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

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

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

How are they paying attention to their risks?

What are they doing for identity management?

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

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

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

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

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

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

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

SENATOR CROCI: Yes, please.

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

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

seriously.

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

SENATOR CROCI: I would very much appreciate it.

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

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

SENATOR CROCI: And when did that occur?

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

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

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

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

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

distinct roles.

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

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

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

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

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

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

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

There are a lot of local governments. There's more than 3,000 local governments that need

assistance.

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

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

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

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

SENATOR CROCI: Senator Nozzolio.

SENATOR NOZZOLIO: Thank you, Mr. Chairman.

Thank you, Doctor.

DR. PETER BLONIARZ: Thank you.

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

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

benefit from your expertise, and your technical background.

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

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

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

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

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

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

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

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

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

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

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

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

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

state of New York?

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

SENATOR NOZZOLIO: Yes, in terms of the role.

Is the -- this in East Greenbush -- is that NYSIC in East Greenbush, is there any similar replication of that, or is this the sole for the state?

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

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

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

piece of the solution.

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

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

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

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

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

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

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

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

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

SENATOR NOZZOLIO: Thank you, Doctor.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SENATOR NOZZOLIO: Thank you very much, Doctor.

Thank you, Mr. Chairman.

SENATOR CROCI: Thank you, Senator.

Doctor, just one final question.

DR. PETER BLONIARZ: Sure.

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

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

How is that determined? How is that vetted?

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

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

So you have to start with understanding where --

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

How does that begin?

DR. PETER BLONIARZ: Well --

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

combat a threat, you bring your technical experts together.

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

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

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

SENATOR CROCI: Okay.

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

SENATOR CROCI: Okay.

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

So -- yeah, so in deciding --

SENATOR CROCI: So the need starts there.

DR. PETER BLONIARZ: -- in deciding --

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

DR. PETER BLONIARZ: So let me talk about the

two of them separately.

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

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

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

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

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

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

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

plan.

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

I understand where the need originates, and requirements.

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

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

I mentioned that --

SENATOR CROCI: I'm sorry, which office?

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

SENATOR CROCI: Okay.

DR. PETER BLONIARZ: Megan Miller's office.

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

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

on the ground floor.

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

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

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

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

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

SENATOR CROCI: So there's collaboration --

DR. PETER BLONIARZ: That's right.

Absolutely.

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

DR. PETER BLONIARZ: Yeah.

SENATOR CROCI: Very good.

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

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

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

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

DR. PETER BLONIARZ: Right.

SENATOR CROCI: So we'll see.

Thank you so much.

SENATOR NOZZOLIO: Thank you.

DR. PETER BLONIARZ: Senator, I appreciate

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

So, I thank you for your interest.

Look forward to working with you in the future.

SENATOR CROCI: Thank you.

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

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

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

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

The floor is yours, sir.

RICHARD DEWEY: Sure.

Thank you.

You have my testimony.

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

Senator Croci, Senator Nozzolio, thank you

for having me here today.

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

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

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

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

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

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

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

yourself.

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

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

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

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

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

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

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

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

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

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

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

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

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

We are getting set as an industry to

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

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

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

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

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

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

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

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

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

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

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

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

For example, the ISO RTO Council, which is

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SENATOR CROCI: Thank you Mr. Dewey.

Senator Nozzolio.

SENATOR NOZZOLIO: Thank you, Mr. Chairman.

Vice President Dewey, thank you for your

input.

How did that drill go?

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

RICHARD DEWEY: It was.

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

And, was there anything you discovered that needs work?

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

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

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

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

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

would follow within their own operation.

What was their plan for recovery?

How would they notify their customers?

Who would they contact?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

And there was different timing considerations.

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

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

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

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

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

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

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

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

RICHARD DEWEY: We do, we do.

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

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

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

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

drill and the Governor's plan.

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

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

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

RICHARD DEWEY: Yes, sir.

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

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

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

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

So, they were very involved.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

You just try to minimize it so that it doesn't disrupt the service to your customers or to your stakeholders.

SENATOR NOZZOLIO: I know this is a daunting task, and I know you are not responsible for, certainly, every generator of electricity in this state.

I know most generators have their own private -- not all -- generators have their private security forces. Rely on local law enforcement as well.

In terms of protocols, besides the -- what sounds like an excellent drill that you engaged in and managed, what about the protocols established in terms of danger from within?

There was testimony, I think, by the FBI about that being a concern; not to indict any employees, but some terrorist group or some individual who wanted to do damage that was part of the network, that was part of the inside, if you will, or had inside -- had significant inside information.

What's the confidence level that that's being monitored and policed?

RICHARD DEWEY: Insider threat is one of the most challenging -- challenging threat factors to protect from, because you do all the up-front work that's prudent and necessary to assure that the individual that you're bringing into the organization can pass all the tests.

So, we do background checks, seven or eight different types of background checks, on every person's history, plus references, plus law-enforcement checks, before they come into the organization.

And even then, you never know if their philosophical, their socioeconomical, situation might change.

They could -- you know, they could be the model citizen when they come into your organization. And then something could happen in their life such that they get influenced in some way, that you've got to be concerned about what their -- you know, what their intent is.

We approach it at the New York ISO by establishing the access to the systems, that you only are given access to what you need to do, what

you need to perform the job that you're hired to do.

So, you don't have cart blanche on every system. You've only got that access to be able to interface with the systems that are necessary for your job.

And for those critical systems, there's a lot of checks and balances, where, to perform certain critical functions, no one person with their access can do it.

It's very similar and analogous, we heard the airline description today, there's two co- -- there's two pilots in the cockpit at every time.

A lot of the functions necessary to actually operate, and the command and control necessary to maintain reliability, of the power grid require multiple individuals to act in concert to be able to carry out the key functions.

So a lot of the key functions are designed with that in mind, and then, that way, you've got the checks and balances so no one person with a specific malicious intent can cause that much catastrophic damage.

It's very similar to, we heard the conversation about the human in the loop.

It's very analogous to what goes on in the

management of the power grid.

We've got highly automated, highly computerized algorithms, that maintain the reliability and the balance of power delivery on the power grid.

But, still, 24/7, 365, we've got 6 control-room operators sitting in our control room that are looking at those advisory outputs, monitoring what the computers are doing, following their own checks and balances, and human controls, and ready to intercede whenever something looks like it's not operating like it should.

So, in that way, you've got the humans watching the computers, if you will. And that human in the loop is so important to combat a lot of the risk, or to mitigate a lot of the risk, of what is increasingly becoming a highly-automated society.

SENATOR NOZZOLIO: Are these national standards that we've established since September 11th, pretty much?

RICHARD DEWEY: There are national standards for electric-system reliability that have been in place for years.

A lot of the security standards have evolved over the years as certain events, such as

September 11th; such as, for example, the power-system event that happened on the east coast in 2003, where a reliability situation in the midwest cascaded through Ontario and New York and created widespread outages.

That resulted in much more stringent and mandatory reliability standards that were put in place.

Also put in place at that time were much more significant and broad power-system monitoring and management tools, so that we can monitor what's going on the power grid well outside of our borders, so we can get advanced notice of reliability events that can take place way out in the midwest or down in the south.

So as these events happen, we're continuously looking to improve our standards, continuously looking to improve our processes and controls, to be able to mitigate the effect of similar events, and, hopefully, prevent similar events.

And, as Senator Croci commented, you know, hopefully, try to prevent hypothetical events, and continuously think of those disastrous-type things that we hope never happens; but if they did, what would we do in preparation for it?

SENATOR NOZZOLIO: Thank you very much.

SENATOR CROCI: Thank you, Senator.

Mr. Dewey, the -- when we think of critical infrastructure, I can't think of a more critical sector of our infrastructure than energy.

Nothing highlights that better than the events of September 11th, and how power affected communications.

Nothing illustrates that better than the events of "Superstorm Sandy," and how power affected communications, and our ability to power our homes, and our ability to power our backup generators and get fuel supplies to the generators.

That is the most critical of critical infrastructure. Our national defenses, our state defenses, everything relies on power.

I've been pleased, and at ease, in working with the ISO, because I know that you're doing everything in your power, pun intended, to ensure that when disaster strikes -- well, first of all, you're in a better position to prevent disaster, but, when disaster strikes, that we have the power to deal with whatever that incidence is.

I'm very appreciative of your testimony and some of your comments.

I heard "informal processes" with the state.

I hope that those are in the process, and maybe you can speak to, will those processes be codified?

And I would also like to have you -- well, let's start with that one.

Your contact with the state, and the informal setting, and how we can codify that? Or --

RICHARD DEWEY: Sure.

I'll talk generally about what I see to be some of the challenges and barriers to effective information sharing, and then how that gets established in terms of law or policy.

I think it will be just be important to recognize it with what the strength and weaknesses are.

One of the barriers to information sharing is, is entities and organizations are sometimes unwilling to disclose certain information if they think it's going to lead to public-relations problems for them or embarrassment at the public level.

So if you're an organization, whether it's a department store or some entity who has just experienced a security breach, it would be most

effective for society and for the industry if they would broadcast and publish the details of that breach such that any other organization that employs similar systems or tactics could maybe examine their defenses to make sure that they won't be the next target.

But if that organization is concerned about the publicity that -- the negative publicity that they're going to get from disclosing that information, then they're subjected to weighing the risks of, What's the PR hit that I'm going to take? as compared to, How I can benefit society or my competitor down the street by sharing the information.

So I think that information sharing needs to be encouraged, and the entities need to be assured that they can do it in a way that protects their reputation to the greatest extent possible.

We want the information to get out, because the most effective information is hearing from your friends and neighbors about the types of experiences that they've had, so you can fix your own defenses, but you don't want people to be disincented from sharing that.

It's -- you can do that through mandatory

requirements.

You can -- you know, there are, certainly within our industry, because it's just so vital to national defense and society that we share information, there are standards and requirements that we're obligated to comply with as a mandatory matter of practice and law.

But, at the lower level, and across more private organizations, you still want to get that information shared, but you want the organizations to feel comfortable in doing so.

I also heard earlier about a question, you know, How do we incentivize entities to want to do that?

The easiest way that I can think of is, give them something back. Right?

So, a lot of times we're in this situation where we have the mandatory and obligatory reporting, so we ship it off -- we ship the information off to the federal organization that we're responsible for reporting it to.

But, how frequently do we get actionable and useful information back about other threats, that then I can use to protect myself and to harden my defenses?

So I think that, you know, that's an important piece of it as well: Not just to harp on the obligation to report, but think about, What are the benefits to the organization in terms of complying with that? And how can we make it so that they are incentivized in a meaningful way so that they want to participate?

SENATOR CROCI: Your organization is a not-for-profit corporation?

RICHARD DEWEY: That's correct.

SENATOR CROCI: Are you in any way involved in an advisory role with our state government, either on the Governor's Advisory Board, or in other capacity, other than in your exercises?

RICHARD DEWEY: No.

I have participated and spoken at a couple of the advisory board meetings, as invited by the board, Dr. Bloniarz.

We do participate very collaboratively, through your stakeholders process, and through some of our planning sessions with New York State government, at the Public Service Commission level, with Department of Homeland Securities, with -- we participate very frequently with the Federal Bureau of Investigation in terms of regular briefings and

industry updates that we have with them.

As far as a formalized, structural, codified way? No.

We -- we're an independent entity, we're a 501(c)3. We operate under an independent board that has no connection to any of the stakeholder groups that we serve.

That independence is important, to make sure that we've got the most bipartisan influences, if you will, in terms of coming up with -- you know, being that honest information broker about future plans, and how the markets are running, and how reliability is maintained.

SENATOR CROCI: And you mentioned previously that, during the course of an event, sometimes the scope can change.

And as a state organization, a state structure, it's not clear always who might be in charge in the response and recovery phases post-disaster.

Are we any clearer, or are you clearer, that if something happened tomorrow, you would know, as the event escalated, where to go, that single point of contact within our state infrastructure?

Similar to the national-response framework,

do we have that clarified, from your perspective as a state entity?

RICHARD DEWEY: I think we do. I think it's a lot more clear.

It -- absolutely, we learned a lot from the exercise.

We learned as an industry, and not just myself, but the other entities, such as the utilities, public and gas, that participated in it.

We learned a lot about what the roles and responsibilities are for a number of the agencies that, prior to that event, was just alphabet soup for some entities.

I think that we came out of that with a much clearer understanding of what the role of DHS Energy Services is, of what the role of ITS is, of what the role -- when to call the FBI, and under what circumstances.

I worry that it's more a function of everybody knowing who's the right person in their rolodex, as opposed to, exactly, does everybody know what to do --

SENATOR CROCI: Which highlights our concern about codifying some of these relationships, because, very often in government, people come and

go, and industry as well.

And if these structures are in place, which was the point of the national-response framework, and some of our emergency-management protocols, that we have a better chance of ensuring that there is a blueprint, regardless of the situation and regardless of the personalities.

Would you agree with that?

RICHARD DEWEY: Absolutely. I think it would certainly improve the structure.

Also, continuous drills, like the exercise that we sponsored in October.

As people change, as organization structure changes, just to test and validate that the structure is well known, and test and validate that the plans are updated such that the people that need to make decisions at those critical junctures know which decisions to make and who to contact.

SENATOR CROCI: And that was my last question.

At the federal level there's a national-level exercise in various areas yearly. It's put on by the Executive Branch.

Certainly, all the departments and agencies, it's an inter-agency drill, very helpful.

So much of what have we've learned about how to deal with whether it's -- in the all-hazards sphere; where it's a natural disaster or a terrorist act, comes from the lessons we've learned at those national-level exercises (unintelligible).

We have employed that at the county and the town levels in recent years, to try to have that same level of preparedness.

Do you recommend -- obviously, you had a very successful drill that you sponsored.

Would you recommend the State take on the responsibility of having that kind of a -- not an NLE, but an SLE?

RICHARD DEWEY: I can tell you that, in my experience, you can never practice your crisis-management skills too frequently.

When you're faced with an actual crisis, and there's that confusion of "Who's in charge, and what do I do?" having had benefit and experience of going through and having drilled that, just prepares, you know, whatever those first responders or individuals who need to take action or make decisions, it absolutely helps.

SENATOR CROCI: We say, "Train like you fight; fight like you train."

RICHARD DEWEY: Yep. And we're in a fight.

SENATOR CROCI: Right.

Thank you very much.

If you have no other questions, Senator?

SENATOR NOZZOLIO: No.

Very helpful. Thank you.

RICHARD DEWEY: Okay. Thank you.

SENATOR CROCI: Thank you so much.

And just to close, I want to thank our -- all of our witnesses today; certainly, Special Agent Freese from the FBI; Dr. Bloniarz, executive director at Cyber Security Advisory Board;

Mr. Richard Dewey, thank you again;

And, Mr. Brown from CA Technologies.

Our purpose today was stated in the beginning, but, we just want to make sure that our government, the people who work in government, have the appropriate level of unease and anxiety that the general population has about the threats that we face in the cyber world.

And I think that my colleagues and I certainly do, and we will help spread that unease until we're completely confident that we have done everything we can, because the worst thing that we can do is wake up the day after a cyber attack and

say, You know, we could have done X, Y, or Z.

So this body is certainly committed to that.

And, I want to thank you all for your participation.

(Whereupon, at approximately 2:10 p.m., the joint public hearing held before the three New York State Senate Standing Committees concluded, and adjourned.)