Committee Meeting

of

SENATE LAW AND PUBLIC SAFETY COMMITTEE

"The Committee will hear testimony from invited guests on cybersecurity issues affecting New Jersey, including current and future efforts to address those issues"

LOCATION: Committee Room 10
State House Annex
Trenton, New Jersey

DATE: March 21, 2022
10:00 a.m.

MEMBERS OF COMMITTEE PRESENT:

Senator Linda R. Greenstein, Chair
Senator Nicholas J. Sacco, Vice Chair
Senator Nia H. Gill
Senator Declan J. O'Scanlon, Jr.
Senator Jean Stanfield

ALSO PRESENT

Amanda D. Holland
Thomas M. Kelly
Office of Legislative Services
Committee Aides

Matthew Peterson
Senate Majority Office
Committee Aide

Sarah Fletcher
Senate Republican Office
Committee Aide

Meeting Recorded and Transcribed by
The Office of Legislative Services, Public Information Office,
Hearing Unit, State House Annex, PO 068, Trenton, New Jersey

Thomas Ke
Amanda D. Holla
Office of Legislative Servi
Committee Au
609-847-3
Fax 609-777-2

NEW JERSEY STATE LEGISLATURE

SENATE LAW AND PUBLIC SAFETY COMMITTEE

STATE HOUSE ANNEX • P.O. BOX 068 • TRENTON, NJ 08625-0068
www.njleg.state.nj.us

REVISED

COMMITTEE NOTICE

TO: MEMBERS OF THE SENATE LAW AND PUBLIC SAFETY COMMITTEE

FROM: SENATOR LINDA R. GREENSTEIN, CHAIRWOMAN

SUBJECT: **COMMITTEE MEETING - MARCH 21, 2022**

The public may address comments and questions to Amanda D. Holland or Thomas M. Kelly, Committee Aides, or make bill status and scheduling inquiries to Michelle L. McArthur, Secretary, at (609)847-3870, fax (609)777-2715, or e-mail: OLSAideSLP@njleg.org. Written and electronic comments, questions and testimony submitted to the committee by the public, as well as recordings and transcripts, if any, of oral testimony, are government records and will be available to the public upon request.

The Senate Law and Public Safety Committee will meet on Monday, March 21, 2022 at 10:00 AM in Committee Room 10, 3rd Floor, State House Annex, Trenton, New Jersey.

The committee will hear testimony from invited guests on cybersecurity issues affecting New Jersey, including current and future efforts to address those issues.

The State House Annex has reopened to the general public. The Committee will meet in-person and there will not be an option to participate by telephone or video.

Visitors are required to wear a mask to access the State House Annex, in hallways, and in certain other facilities. Masks may be required in Senate Committee Rooms. Please visit https://www.njleg.state.nj.us/Publications/PDF/JMC%20Rules.pdf for more information.

The following bill(s) will be considered:

S297 Greenstein/Madden	Requires public agencies report cybersecurity incidents to New Jersey Office of Homeland Security and Preparedness.
S347 Singleton	Eliminates presumption of non-imprisonment for theft of a firearm.

(OVER)

S355 Gopal/Greenstein	Makes permanent temporary enactment allowing certain alcoholic beverage retailers to sell and deliver alcoholic beverages and mixed drinks; establishes certain sale and delivery privileges for alcoholic beverage manufacturers.
S703 Beach/Greenstein	Provides employment protections for paid first responders diagnosed with post-traumatic stress disorder under certain conditions.
S1367 Scutari/Holzapfel	Allows police chief and fire department chief members of PFRS to serve until age 67.
S1505 Gopal/Greenstein	Permits operation of pedicabs and alcoholic beverage consumption by passengers of pedicabs in certain circumstances.
S2081 Greenstein	Expands authority of Missing Persons and Human Trafficking Unit; creates rebuttable presumption of criminal activity in high risk missing persons cases.
S2356 Stack/Gopal/Greenstein	Extends prohibition on certain utility discontinuances for certain customers.

*FOR DISCUSSION ONLY:

S513 Cryan/Turner	Establishes rebuttable presumption of pretrial detention for defendants who commit certain firearm offenses under Graves Act.

Issued 3/16/22
*Revised 3/17/22 S513 changed to discussion only.

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

Page

SENATOR LINDA R. GREENSTEIN (Chair): Good morning, everybody, and welcome to this meeting of the Senate Law and Public Safety Committee.

We have a very good crowd here today, and a couple of speakers. So I look forward to sharing with all of you.

Will you please take attendance?

MS. HOLLAND (Committee Aide): Senator Stanfield.

SENATOR STANFIELD: Present.

MS. HOLLAND: Senator O'Scanlon:

SENATOR O'SCANLON: Here.

MS. HOLLAND: Senator Sacco.

SENATOR NICHOLAS J. SACCO (Vice Chair): Here.

MS. HOLLAND: And Senator Greenstein.

SENATOR GREENSTEIN: Here.

MS. HOLLAND: We have a quorum.

SENATOR GREENSTEIN: Okay, thank you very much.

We're going to start with the hearing on cybersecurity. We have two speakers; and it doesn't sound like a lot, but they're two really good speakers in the field who know a lot about it. So I'm hoping you'll have some questions.

And the first speaker, who we'll begin with, is Mike Geraghty. Please come up to the microphone and tell us who you are, what your title is.

And when you press that microphone, make sure it shows red. Red is "go" in Trenton.

M I C H A E L G E R A G H T Y: Good morning, Senators, and thank you for having me.

So my name is Mike Geraghty; I'm the State's Chief Information Security Officer and the Director of the New Jersey Cybersecurity and Communications Integration Cell -- the *NJCCIC*, as we call it. We're organized under the New Jersey Office of Homeland Security and Preparedness, and we act as part of the State cybersecurity function. Not only is it OHSP, but we also have representatives from the New Jersey State Police as part of the NJCCIC, as well as the New Jersey Office of Information Technology. That allows us to act in both a cyberfusion center and security operations center capacity, serving New Jersey residents and State government with cybersecurity services in all sorts of functions.

We were created back in 2015 under Executive Order 178, that was signed by Governor Christie. It created the NJCCIC to be this one-stop shop for cybersecurity information sharing, threat intelligence, best practices, incident reporting, and incident response functions. So in that regard, we serve, obviously, the citizens in the State of New Jersey, but also public and private sector institutions, critical infrastructure operators, and other key assets. And we provide a holistic all-threats, all-hazards approach to cybersecurity in what we do; and it's in that regard that I'm here testifying to you today.

So on a daily basis, state government networks are attacked over 10 million times. And that's just our networks and applications; that's not even all the individual users that get phishing, and spam, and all sorts of other attacks that we have. So 80 million attacks in a given week against state government networks.

But those attacks, in a lot of cases, are indiscriminate. They're not necessarily targeted at state government. In other cases, we know that

municipalities, we know counties, we know businesses are also the subject of those same types of attacks. We obviously don't have insight into all of them, but we provide incident reporting services. And, you know, over the past three years -- actually, over the past four years, we've received 1,500 reports of cyber incidents from individuals and organizations that have been impacted. And we provide services to help contain, eradicate, and then recover and restore services to those organizations. So in that regard, we're talking about the number of attacks that we see, the number of incidents that we see. But we also know that they're underreported.

And I know the Senate, this Committee, is considering S-297, which would require municipal and public sector organizations to report cyberattacks to the NJCCIC -- to the New Jersey Office of Homeland Security and Preparedness. And the reason for that is, what we want to do is have a common operating picture to work from instead of having ad hoc reports, voluntary reports that are made to us. If we do have that common operating picture, then we can come up with a strategy of how to provide services.

There's no public sector network that's not connected to another public sector network in the state. So a school system connects into the township, the township connects into the county, the county connects into the State. And as a result, we are all at risk as a result of that.

So a breach of a township or a municipality can result in, obviously, the compromised credentials of people who log into State systems or other types of systems. Those credentials can be used to further additional attacks.

So what we want to do is be able to collect that information, be able to help respond, obviously. But also prevent others, by providing other

municipalities, the public, businesses, critical infrastructure with that threat intelligence that they need to protect themselves.

So that's why I'm testifying. I fully endorse the Bill that's being submitted and considered by the Senate. It's also one way that we can do a whole-of-State approach to cybersecurity. Cybersecurity is brand new, and it's not going away anytime soon. We continue to depend on technologies for everything that we do -- critical infrastructure; from government services, to our homes, our network, to State government, as well as all other aspects of computing and online technology.

Today we're in this world of converged physical and cyber devices. And differentiating between the two is really difficult to do. You go back five years ago, there were no connected doorbells or connected thermostats. Elevators weren't connected by computers and networks, and the same thing with HVAC systems and the like. But today, everything, including intelligent traffic systems to business manufacturing systems -- they're all connected, and they all provide some risk because our attack surface keeps growing and the threat environment keeps growing.

That threat environment is not just a local threat environment like we would see in a physical crime where a bank was robbed, let's say, down here in Trenton. You'd have to be physically present. These attacks that we see come from throughout the world, at any time of day or night. There is no 9 to 5 business operations for online systems. And as a result, being able to prevent and defend against them, but also respond to them, is really what the NJCCIC is about. So it's that resilience. We're not going to prevent every attack from happening, just like we're not going to prevent hurricanes, or tornadoes, or other types of natural disasters. But we want to make New

Jersey more resilient to these attacks by providing these types of services -- whether it is that threat intelligence, whether it is the best practices, whether it's the response resources that we have.

I'll give you some numbers just to work from, and I know I put some things in your book.

On a weekly basis -- and we're talking about Russia/Ukraine for the last, you know, few months -- we receive about 500,000 attacks, just from Russia, on a weekly basis. China, Iran, other geopolitical hotspots, the same thing. So it's not necessarily that Russia is attacking us; it's just that infrastructure being used, and the Russian Federation is being used to attack New Jersey -- New Jersey State government networks. We detect, and we block them.

At the same time, we also know that, with this expanding attack surface, there are lots of vulnerabilities out there. Some of the services that we've been trying to provide -- and do provide to municipalities, counties, school systems -- include what we call a *Statewide Threat Grid.* That threat grid puts an intrusion detection center at the perimeter of each of the county's networks, so if a county up in North Jersey is being attacked, we're notified, as well as the Department of Homeland Security; as well as other counties so that they know these attacks are happening and they can prevent them from being victimized as a result.

We scour the dark web, and we harvest compromised credentials for New Jersey public sector organizations and critical infrastructure organizations. Since May of 2020, when we started this service, we've notified these organizations of more than 23,000 compromised credentials that are being used. So, for instance, a compromised credential would be my

State government e-mail address, that I use to log into a system, and that password. And that password just happens to be in plain text available for anybody on the dark web to use. Oftentimes they are used to gain access, because logging into a system with somebody's credentials is a lot easier than hacking into a system through some vulnerability or some other technical exploit that people are doing.

We also provide all sorts of attack surface management and risk management services. So we provide municipal governments and public sector organizations in New Jersey with access to security scorecards, and what they look like from the perspective of an attacker. And they range, just kind of like a FICO score or a school score -- that you would get an *A* through *F,* as far as *A* being good, and *F* being failing, and you're an easy target -- and those types of things.

We also provide them with what their exposure is -- all the vulnerabilities. And we've notified individual public sector and private sector organizations of vulnerabilities that we know are being actively exploited, and that they've probably been compromised. In a lot of cases, that has turned out to be the case.

So one of the problems we have throughout government and private-public sector organizations is there's not enough cybersecurity personnel, or that expertise, to really understand, monitor, prevent, detect, and respond to those attacks. And so we provide all sorts of services. We've trained over 7,000 individuals on things such as intrusion detection, computer forensics, incident response, and the like -- so we can do that. We understand-- And I understand, as the State's Chief Information Security Officer, that my job is not only to do cybersecurity today, but it's to grow a

workforce for the future. So we spend a lot of time and effort focusing on universities, colleges, high schools, and cybersecurity education. We partnered with just about every university in the state.

We sponsor, and partner, and develop all sorts of internships at the high school level for cybersecurity. We do high school-level cybersecurity camps. Today, we have 3,500 high school students competing in a national cybersecurity competition against all the other states. And we've been doing that for the last -- this is the fourth year running that we've been doing that. New Jersey has come in the top three for each of those last four years that we've been doing it. And so providing that cybersecurity education; getting people involved at an early age so that they understand what a career in cybersecurity is really about.

And we do that across the board, with all sorts of underrepresented communities that don't really have that access to cybersecurity services, or really what it is. I know, across the board, in the cybersecurity industry, it's about -- 18 percent are females. In the NJCCIC, we're at 50 percent. And so we target those underrepresented populations so that we can bring them into the fold, provide them those opportunities for cybersecurity careers and the like.

So with that, there's a lot that we do; a lot more that we need to do. There's no such thing as *security*; there is *resilience,* and that's what we want to get to. We can't promise you that there's not going to be a successful attack tomorrow, but we can promise you that we'll be ready; we'll be able to identify it, contain it, and eradicate it, in short order, so that we can recover from it and restore services.

And with that, I'll take any questions.

SENATOR GREENSTEIN: Thank you.

Well, hearing the numbers is daunting; I mean, the number of attacks that you mentioned. You did say, just as an example, we're not attacked by the Russian government, but we're attacked by entities in Russia that may want to attack New Jersey.

In a way-- I see everything that you're saying, but what is the most damaging thing that can happen, if, for whatever reason, you are not able to push back an attack? What has happened already that may have been damaging, if you can speak about it? I mean, I'm trying to get a sense of the extent of the damage that could happen if you're not able to beat back an attack.

MR. GERAGHTY: So I think two of the more well-known attacks that happened, happened last summer with Colonial Pipeline -- they were hit with ransomware. And JBS meats, which is an international meat supplier, food supplier -- they were hit with ransomware. And what the ransomware does -- it obviously encrypts all the data in the system, making them unusable. So the operations issues that it provides are really damaging. So obviously Colonial Pipeline -- they had all sorts of fuel shortages in the southeast of the United States. JBS meat -- their processing was taken offline.

But closer to home we've seen this with hospitals, where services and surgeries are delayed because of these types of things, and appointments are cancelled. Within police departments -- we see police departments getting hit with ransomware, making their services -- their network services-- And I think of officer safety. If an officer pulls somebody over on the side of the road for a motor vehicle stop, and that person happens to be a wanted felon,

there's no way, if your systems are down, that you're going to be able to relay that information, for officer safety, to the individual officer making the stop.

So all sorts of other financial impacts. Obviously, schools have been -- days in school have been canceled so that they can recover from these attacks. So municipalities, also, have had these attacks, impacting their operations, their ability to collect taxes, their ability to provide services to the citizens of the State and to the municipalities themselves.

SENATOR GREENSTEIN: So if a New Jersey agency is being attacked-- I mean, that sounds like it's very malicious in the sense that it isn't clear what they're trying -- what they're really trying to disrupt. I mean, what are they usually trying to disrupt?

MR. GERAGHTY: So it's not necessarily that it's a targeted attack all the time. Sometimes it's a crime of opportunity, as they say. You happen to have an IP address that's on the public Internet and you're vulnerable. It's not necessarily how *valuable* you are, it's how *vulnerable* you are.

And I go back to the Colonial Pipeline instance -- and they allowed remote access into their internal network. And the way that the bad actors got in -- and it was a ransomware group, obviously from Russia -- was that they collected the compromised credentials that were on the dark web. And those credentials -- username and password -- were for an individual who had left Colonial more than two years earlier, but the credentials had not been disabled and the account had not been disabled.

Those are the types of things that they prey on -- mistakes that we make or vulnerabilities that we're making.

SENATOR GREENSTEIN: I see.

Senator Sacco, do you have anything?

SENATOR SACCO: No, thank you.

SENATOR O'SCANLON: I do.

This is really encouraging to hear. I know you guys are out there, but this is the first time I'm hearing any detail about how comprehensive what you're doing is. And if you're in our positions, you hear about these attacks, and it's terrifying. And you wonder, are we really, proactively, understanding what's going on? I know there are always new attacks, but it's really encouraging -- it should be for the public -- to know that this work is going on.

It is stunning-- I think you said 500,000 attacks per week, or attempted attacks per week, just from Russia?

MR. GERAGHTY: Russia.

SENATOR O'SCANLON: Is that nationwide? That's not just New Jersey.

MR. GERAGHTY: That's just state government; executive branch networks and applications. That's not the legislative branch, that's not the judicial branch.

SENATOR O'SCANLON: That's not--

MR. GERAGHTY: That's not private infrastructure, either. That's just the executive branch of state government.

SENATOR O'SCANLON: That's scary. But it means that we're stopping -- because we hear about something -- but we're stopping most of them. So that is good to know.

So help me understand-- You mentioned Colonial Pipeline, right? And they just -- they were lax in their security by not purging people

who are gone. How often is that the case? We know, like, with-- We have a rash of car thefts in many areas of New Jersey. Ninety-some-odd percent of them are idiots who -- and some of them in this room; me, occasionally. Not anymore, since someone tried to steal my car a couple of weeks ago (laughter) -- they leave the key fob in the car. Now, you'd think, with all that's out there and the news stories, we would stop being boneheads and lock our cars, and bring the key fob with us.

How often are these successful attacks where these entities are like Colonial, leaving the key fob in the car?

MR. GERAGHTY: It is no different in the cyber world. I won't call them *idiots*, but they--

SENATOR O'SCANLON: I will. And I'll apply it to myself, too, so it's-- (laughter)

MR. GERAGHTY: Using common passwords -- *password* is a password, *123456*, not locking down Wi-Fi; not updating -- doing basic cyber hygiene practices. And we talk about hygiene -- we're going through this pandemic -- washing your hands to keep germs away, brushing your teeth to keep tooth decay away. The same thing in cybersecurity are some basic steps that you would take as far as having a strong password. And I'll say this -- the number one thing that anybody should do is use multi-factor authentication to protect their accounts. Anytime you have sensitive information, you should be using multi-factor authentication, because passwords are not secure anymore.

SENATOR O'SCANLON: And I didn't know what that was until a few months ago, and it's easy to do. And you're right -- you have two

devices confirming, and it's not a big burden. So yes, I get it, and that's great advice.

So really, it's -- we have ways to defeat these things; we just need more people to take advantage of this proper cyber hygiene. And by the way, you mentioned washing your hands. I'm vaccinated; I don't have to wash my hands anymore. (laughter) So that's not a problem.

So last question -- and again, I'll probably contact you in the future, because, again, I find this really encouraging. And I don't come to Trenton -- I don't find a lot of things this encouraging these days.

Ransomware and public systems. Right now, we have a disincentive for public systems that are compromised with ransomware to go public and to share it. I know there are school systems that have been attacked. They realize they left their key fob in the car, essentially, and the ransomware is successful. And public tax dollars are used to pay off criminals in Russia in order to get access to -- re-access to their encrypted files. If the public knew how often -- I know of a few instances -- if the public knew, they would be shocked. It is going on, on a pretty regular basis, right?

MR. GERAGHTY: It is. And typically, it's a cyber insurance provider that's paying the ransom, if a ransom is paid.

SENATOR O'SCANLON: I have to imagine that's pretty expensive insurance, at this point.

MR. GERAGHTY: Insurance keeps increasing exponentially over the last few years.

SENATOR O'SCANLON: So it's still tax dollars. These entities need to know that they have to practice this proper cybersecurity so we don't hemorrhage people's tax dollars. Again, when I heard it, I was outraged; and

I thought, like the Chairwoman, that it was a targeted attack on the school system. And I thought, "Well, let's pass a law that says they're forbidden from paying ransom to these criminals." You think, "Okay, good. That will dissuade them from going to the trouble to attack in the first place." But your answer was the one I got. It's not targeted; it's -- they're going to come anyway, and they don't care whether your systems are melted down and have to be redone. You can't stop them from paying, because it means they're just going to lose everything, right? That's accurate?

MR. GERAGHTY: You know, we have ransomware mitigation strategies. And I know I put folders on each of your desks, and stuff like that, as far as what you can do to prevent it. Obviously, the cyber hygiene part of it. Having good backups and storing those backups offline so that if you are impacted, you can recover from them. So those were all those best practices that we talk about. Does everybody do them? No, not everybody washes their hands, whether they're vaccinated or not. (laughter) Not everybody brushes their teeth and those types of things.

So we know we have a job of communicating that and then helping people do it. You know, sometimes we talk about cybersecurity, and the person who is responsible, in a municipality or a school system, just happened to be somebody who had a computer background but may not be an expert in all things -- enterprise cybersecurity and stuff like that. Those are the types of services that we're trying to provide. We know there are not enough expert cybersecurity people out there for each municipality and school system to have one. So let's use a shared resource, like the NJCCIC, so that we can provide those services.

SENATOR O'SCANLON: And I definitely need to help get the word out there that they need to do this.

And look, it gets back to this Bill, right? Reporting these things, knowing where they are is important. Because right now, I know there are attacks that go on, and they're not telling anyone because they're embarrassed. And they pay big taxpayer dollars to buy their systems back online. And that is just abhorrent to me.

So them reporting, knowing how big the problem is, knowing exactly how they're being hit, and you being able to go out there and fix these things before they happen -- I'm all for it.

So, good stuff.

Thank you, Chair.

SENATOR GREENSTEIN: Thank you.

Senator? No? Okay.

I did want to ask-- You've talked about the Bill that we're about to do, and it's just one of many that we hope to do.

Can you give us an idea of what we can do, on the legislative level, to move your operation forward and to make things better for you? This Bill was one thing that you did recommend, but are there some others out there that you might think we could do, or look at it?

MR. GERAGHTY: I don't have any other bills to consider, at this point. I mentioned shared services. Obviously, most schools and municipalities don't necessarily have those cybersecurity functions embedded. They are costly if they wanted to do that. So why not develop something where we can have a shared service, a statewide cybersecurity

operations center that monitors networks for municipalities and school systems--

SENATOR GREENSTEIN: That's a good idea.

MR. GERAGHTY: --where they don't have those. That's a pie-in-the-sky idea that I have, but it's something that is, I guess, more cost-effective than trying to develop it within each, and would provide the service, public value.

SENATOR GREENSTEIN: I think that's--

MR. GERAGHTY: Again, before I leave -- and I know Lieutenant Hoppock is going to come to speak -- one of the things that we pride ourselves on is our collaboration and partnerships that we've developed. We have a great partnership with the New Jersey State Police Cyber Crimes Unit, the FBI Cyber Task Force, Department of Homeland Security, New Jersey National Guard, and the Board of Public Utilities, because we are all in this together. It's the only way that we're going to be able to be successful in this realm, in cybersecurity -- is that we all work together going forward.

So thank you for having me.

SENATOR GREENSTEIN: Thank you very much; thank you very much for being here. We really appreciate hearing from a top official in this field.

Thank you.

And today, we also have Ryan Hoppock, Deputy Director of the New Jersey Regional Computer Forensics Laboratory.

Thank you very much, Ryan.

L I E U T E N A N T R Y A N J. H O P P O C K: Thank you for having me here, Senators.

So first of all, I just want to say thank you for asking the State Police to be here today. We don't get a chance, often enough, to talk about what the Cyber Crimes function does with the public, unless the person is a victim.

So my name is Ryan Hoppock. I am a lieutenant in the State Police. I am currently assigned as the Deputy Director at the Regional Computer Forensics Laboratory, which is a Task Force with the FBI.

Prior to that, I spent 15 years -- which is the most of any active member in the State Police at this point -- with the Cyber Crimes Unit, developing our capabilities, expanding them out, giving us a little bit more power to serve the citizens of this state to protect against some of the things that Mike Geraghty had spoken about at the CCIC.

So what I was asked to do was describe the functions of the Cyber Crimes Unit. I decided I would basically use what the Unit's mission statement is to start off with; I think it's really the best way to describe it.

The Cyber Crimes Unit at the State Police is a 24/7 on-call Unit that conducts and assists in investigations where computers, networks, telecommunication devices, and other technological instruments are the vehicle or target for the commission of criminal acts against network resources critical to the function of corporate or government entities.

A little bit of a mouthful, but essentially what the Cyber Crimes Unit does is they are able to look at a wide variety of criminal activity, both originating from the emergence of technologies or in the assistance of traditional crime. So we help out a lot of units, let's say, for crimes that have been around since the dawn of time -- say, homicide, for example, or theft --

while, at the same time, we have capabilities to look at crimes that originate from the development of technology, like computers themselves.

Some of those matters Mike had already talked about -- Mike Geraghty talked about, from the CCIC. You'll hear where we intersect or overlap with some of the responsibilities.

First of all, I want to mention that we have some excellent relationships with our Federal partners and other State agencies. We are involved with the Federal Task Force -- the Cyber Crimes Federal Task Force at the FBI. It's been a very successful relationship, passing back and forth some good visibility into what occurs in New Jersey, what happens on a daily basis with our citizens. We've been able to take some successful cases to that level. We coordinate quite often with the New Jersey CCIC, or the Cyber Integration Cell. They oftentimes are a repository, or the initial lobby, let's say, for people to communicate that they've experienced an adverse event or incident. And then from there, we can filter out how the Cyber Crimes Unit can be of assistance to these folks.

We also, at the Cyber Crimes Unit, are the coordinator of New Jersey Cyber Terrorism Task Force. Now, this takes 26 member affiliates around the state, identifies them as subject matter experts, or person and/or persons who are capable of performing on-site data acquisition in the event of a very serious cyberterrorist event. So we take these cross-sectional skills from various computer-related functions that our counties, local municipalities have, and we cross-train people, and they're provided with equipment and such so that in the event that we needed to multiply our effectiveness, we have, essentially, that capability beyond the State Police.

So some of the types of criminal activities -- this is actually very difficult to do for us, because we see so many different types of criminal activity aided, and abetted, or facilitated by cybercrime. However, in the last 15 years, there are a clear grouping of crimes or criminal activities that we tend to receive from the citizens, more than not.

First and foremost is definitely ransomware and phishing incidents. I'll speak a little bit more about how we deal, at the end -- how we deal with these ransomware and phishing incidents, because it isn't always something we can necessarily hold attribution, hold a character or group attribution to. So we end up handling those cases -- typically, they're financially motivated, so we handle those cases from the aspect of helping serve the victim with information, guide them to where they need to be. We do not mitigate. We're not a service -- a free service to mitigate situations, like a fix-a-person's-vulnerabilities. But we can identify them, point them out, and push them in the correct direction -- okay? -- in the role of cybersecurity.

So stolen credentials, identity theft, impersonation, other types of thefts -- this is very common, with the level of anonymity that the Internet affords the public, the world. People oftentimes are stealing other person's identities and purporting to be those people online in many different ways. And that's something we see and have to handle quite often. Some of those cases do result in investigations and arrests here in the states, including New Jersey.

So another main thing we've seen -- a denial of service attacks. We assist with any kind of business entity, organization, both public and private, that experiences an attack where some portion of their network

services or cyber landscape has been affected; it's no longer available as a result of an attack. We can identify how to walk people through-- Where do you need to go? Where can we seek help? A lot of these folks who I'm talking about are medium- to small-sized businesses; people who don't have in-house resources or don't have the power to retain third-party services -- for lack of a better term -- because the resources just aren't there for those businesses' sizes.

So another area very important to the Cyber Crimes Unit, due to the nature of our training and what we cover, is the identification acquisition of digital evidence. So this will cover any aspect of criminal activity that requires expertise to come in, and weigh in on where evidence may be, how do we safely obtain it, and do it in a way to where it's admissible in court. It has to be done in a verifiable manner, right? So we're talking about the integrity of evidence, digital evidence. We refer to that as our *investigative forensic capability*.

We also have that ability in mobile data extractions. And I use the word *extractions,* not *examinations,* because, again, that's about the acquisition of mobile forensics -- data that's on our phones. Today we walk around with phones that are obviously getting ever-so-more powerful. Victims leave their phones behind; perpetrators use their phones, for whatever reason, in the commission of crimes. And someone may have the need for an expert to come up and speak on the behalf of what we can get on that device and what we can't. And that's a skill set -- mobile device extraction is very important for a multitude of units, local municipalities, and cybercrimes units. We've been providing that service now for at least about 10 years.

Computer forensics and malware analysis. So even though at the Cyber Crimes Unit at the State Police -- it's an investigative body and investigative functions. They are cross-trained, which is to say, *we* are cross-trained -- I'm no longer there, but I was there for so long -- we all were cross-trained. The RCFL, or the Regional Computer Forensics Laboratory at the State of New Jersey -- they are the number one, or the primary, forensic examiners in the State for investigative purposes. However, because of the cross-training, we have the capabilities in-house to conduct what's called *forensic investigations* on a triage basis. So we're able to look at things to identify, "Hey, was this really used in the commission of some type of criminal activity? Do we need to take this offline, narrowing the scope down, being less intrusive for the citizens, less disruptive for businesses that are victims, to eliminate things and essentially get the focus and the attention of where it needs to be for an investigation?"

A couple of other matters.

Forensically, we deal a lot with motor vehicle infotainment and telematics system forensics. So, essentially, that's your infotainment systems in your motor vehicles today. Our cars are equipped-- They are basically computers. They're equipped with networking devices that roam over cell phone tower networks. We can input data into them; we can also retrieve that data. Anything that forensically goes into those machines hypothetically can be taken out. It's not an easy task; it involves, like many of these functions, a high degree of training. But obviously it would be advanced in that category.

We also assist other agencies regularly. I can't stress how much we're called upon, or how much of the day, every day, is dedicated to assisting

another agency. It doesn't have to be a law enforcement agency; it's everyone, both public and private -- especially public. We see a lot of folks out there who are reaching out, maybe by word of mouth. They've heard of us before. "Hey, we're experiencing this problem, what do we have?" And 90 percent of the time, or such, we know right away -- they're experiencing an incident or an adverse event that requires some mediation. And we take those opportunities to reach out and have positive contact with the public.

So these all, really, sum up our incident response capabilities -- the Cyber Crimes Unit, each member in there. There are 10 currently. Those members have what we call an *instant response capability*, or, more specifically, a *digital forensic incident response capability.* That means, 24/7, they can be called out to an incident, understand it, triage it, communicate to others, determine next steps, best actions, what they can do to make this situation move into a remediation phase -- because that is the investigation phase -- and recover. What, ultimately, are victims to recover?

Now, we also provide some education services. So in the past, we've developed, in-house, what we call *high-tech crime investigations courses*. Those courses designed internally at the State Police -- and externally to other law enforcement to help them understand what they might be missing in their investigations; which better serves the public -- their victims especially, right? So these high-tech crime investigation courses -- I wish we could do them more often. They do occur once or twice a year. And we've gotten excellent feedback for over a decade on the amount of material we cover. Essentially, this goes from *A* to *Z* -- how to identify evidence; what evidence is, digitally; how to recover it; and how important it is for us to handle that correctly so that we don't have a problem with the admissibility in court.

Cyber presentations, corporate outreach -- I would like to do more of that; that's definitely something that's important for us to have relationships. We've had some very successful cases as a result of the relationships we've built with the business leaders -- just going out in the field and having our face known, let them understand that we're there for them, that we have the relationship with the FBI, we have a relationship with other Federal partners. If there's an issue that falls under their purview, we're going to be happy to get them to where they need to be. We're not a barrier; there's no jurisdictional competition.

Law enforcement investigation assists. There are times where we're more committed to actually helping at a local law enforcement or a county law enforcement agency to further their aim or mission, because they're just not able -- due to the resources or possibly subject matter expertise -- to cover an investigation to the degree of thoroughness that we would. And it doesn't matter the type of criminal charge or what the case appears to be, we will go out there and assist, and spend a lot of resources.

So in the future, right now, it looks like the Unit is evaluating how they better can serve the vulnerable populations of the state that are falling victim to social engineering attacks, in addition to all the other things I talked about. Which, by the way, is including what we do, but not the entirety of what we do. It's worth mentioning -- the elderly persons, many other groups and communities in this state, face unique challenges to understanding how the Internet could be a vulnerable place for them. Maybe they're not getting the messages correctly. To the credit of the Cyber Crimes Unit, it just so happens that we speak at least, at last count, six different languages, from Turkish, Mandarin, to German. We've actually had that

come in handy quite often, having folks call us out to assist them. Because we have a lot of areas where businesses and folks have a better preference for the language. It's easier for them to communicate.

Cryptocurrency is another area where we have a lot of subject matter expertise. We've had a tremendous amount of success driving education and awareness as to how cryptocurrency functions. Those questions come up every day, and we've been able to be very concise and effective with that message.

Also, more so in the future, we're looking at -- I don't want to say *solve* the problem, because I don't know that it's solvable -- but confronting the challenge of money mules. There are complicit and implicit money mules: persons who transfer money from point *A* to point *B*. This is a term basically that could be talking about somebody who knows what they're doing is wrong, or someone who is a victim themselves, and we have to treat them as such. And we've always encountered these cases and not quite known what should be done with them. And we've looked at them individually, as an individual case. Well, they really fall in those two categories. The money mule is a victim, or the money mule knows what they're doing and they're going along with it. And they're facilitating the transfer of ill-gotten funds, typically oversees. The FBI dedicates a lot of time and resources to investigating this type of crime. What goes underserved is tracing victims' money and recovering it. So that's been a function that we've been working out, the Cyber Crimes Unit -- we're coming up with a tried-and-true tested means of intercepting funds that are being sent overseas, and recovering them to citizens here in New Jersey.

So one of the things I want to mention about what I just spoke about -- because it applies everywhere, in every category of cybercrimes -- is that attribution can be elusive. And metrics that we use to define success, typically, in law enforcement, don't necessarily apply very well to cybercrimes. And that's because our orders -- there are none. It's a global community online, and it's a global fight. So we have to fight the urge to think about holding someone accountable or being attributable to what criminal activity we see -- and rather, focus on the victim. It's always important for us to focus on the victim. Sometimes we can serve the victim better, through some of the things we encounter, by spending time with them and walking them through something to get to a point, perhaps, where they recover funds or services get restored.

We walk a fine line between being able to mitigate and assist people with some cases. But it does work; it's been a real success.

I think that's about all I can mention as far as--

SENATOR GREENSTEIN: You were great. We really, really appreciate all the information.

I just -- I have one question, and then I'll see if anyone else does.

In terms of your protocol, who gives you the different tasks to do? For example, if there's a stolen identity, an individual can't come to the State Police for help, right? Can an individual who's had his identity stolen come to you, or does it have to come through an agency?

LIEUTENANT HOPPOCK: We definitely, Senator, act as a filter. So it depends. We get that call -- which we do, very often; there needs to be a conversation, an educated conversation on the behalf of the detective, to find out how can that victim best be served. Do they go to their local

municipality first, perhaps, and create a record of the incident, something like what we call an *operations report*; and then perhaps we would move on it, or it may go to the county. So essentially, we do let the county, depending on the services that are available, the county governments have the first bite of the apple to help these folks. Because, as I mentioned, we are a small unit, and there are quite a lot of people in the state, so we couldn't handle all of those cases. But we will act as a filter and direct them to where they need to be.

SENATOR GREENSTEIN: Great. And then, the same question I asked Mr. Geraghty. Is there anything that you can see that might be done legislatively that could be of help to your operations?

LIEUTENANT HOPPOCK: There certainly can, I'm sure of it. I couldn't speak specifically to this Bill, because I'm not supposed to.

SENATOR GREENSTEIN: Not so much this Bill, but just any other ideas that you might have.

LIEUTENANT HOPPOCK: Absolutely. So I think just more cooperation and more communication. There are some budgetary -- reoccurring budgetary concerns where we may not have access to all the resources we need sometimes. But I think that's a normal challenge for anywhere in government, let alone law enforcement.

Yes, I think communication -- having the ability to drive recommendations, trends' reporting. We see a lot -- the detectives see a lot in their interactions with the public. And it might be useful to take a look at that, to push that information to a centralized location.

SENATOR GREENSTEIN: Thank you.

Does anyone have any questions?

SENATOR GILL: I have.

SENATOR GREENSTEIN: Senator Gill.

SENATOR GILL: Yes.

Good morning. That was very interesting.

Could you put-- What's a *money mule*? I understand what a drug mule is, but what's a money mule and how does that work?

LIEUTENANT HOPPOCK: Senator, I can recall asking that question myself (laughter), probably about 15 years ago this month.

So it is a term that's used to describe someone who is sending and receiving -- or receiving and sending is a better way to think of it -- funds that come from somewhere else. Maybe they set up an account for that specific purpose, and they're taking a certain percentage of that money -- let's say 5 percent -- and keeping it for themselves, under the direction of someone else. A lot of those people -- I would say most -- are victims. They, in some way, have been manipulated to facilitate these financial transfers. It could be several hops before, it could be several hops after, and those are touchpoints where the money account would land in an account, until the money reaches the persons who -- it may be organized crime, for example, overseas -- where that money is destined. That's a money mule. A money mule would be somebody who would set up an account, send and receive funds, and-- That's the best way I can explain it.

SENATOR GILL: Thank you.

LIEUTENANT HOPPOCK: You're welcome.

SENATOR GREENSTEIN: Senator, go ahead.

SENATOR O'SCANLON: Two very quick ones.

How often do you actually catch perpetrators? Is it-- Hey, look, 98 percent of the time they're outside the borders, and you can just mitigate. Or would we be surprised at how often you do, actually, charge folks?

LIEUTENANT HOPPOCK: Not as often as we would like.

But we do, and I think you would be surprised as to how we do and when we do.

It's hard to quantify it, because of the landscape that you see with cybercrimes -- it's hard to quantify it, how you measure that. Is it by the cases we take in? We have so many complaints, there's so much activity out there that we have to filter -- that word keeps coming back up -- we have to filter what cases we take in order to allocate our resources, but most effectively. So we are successful; if you look statistically, we're very successful because we're selective.

SENATOR O'SCANLON: Got it; interesting. Nice to know that someone's being held accountable, sometimes.

LIEUTENANT HOPPOCK: Absolutely.

SENATOR O'SCANLON: And just for-- You said you try to go back and claw back money for money mules or other people who have been ripped off. Is that an area where we're-- You think that once someone hits "click," it's gone. Are you successful at recovering?

LIEUTENANT HOPPOCK: It could be -- that's the answer, if you say once somebody hits "click," it could be gone. What's happened is, is we've inadvertently recovered funds for victims over the years. And those times it's happened, and a pattern began to develop, we saw a pattern with how to recover those funds. And we began to learn how the financial institutions are treating these matters, or their lack of attention to them. It's

both. They have attention, and they don't have attention in some areas. And because of that visibility into how money is being transferred, how the social engineers -- these people who perpetrate crimes who get people to send money -- how they behave, we were able to figure out a couple of ways how to retrieve funds back for victims.

Speaking to your first question, where we can't necessarily go find somebody -- pick a place around the other side of the planet -- who's responsible for having our citizens send money overseas. But we may be able to intercept the funds, at least partially, and have them returned to the victim. We've been successful with that. So when we look at the total dollar amounts growing, we said, "Hey, this might be something we could--" We're doing this by chance almost -- coming across these things, and then seeing an opportunity to recover funds, and we take it. Because it's great for the victim.

SENATOR O'SCANLON: Got it.

LIEUTENANT HOPPOCK: But what if we focused on that? That's the idea.

SENATOR O'SCANLON: Thank you.

It's probably-- The few thou I sent to a Nigerian prince the other day, that's probably on the up-and-up, right? (laughter)

LIEUTENANT HOPPOCK: It's probably too late, given that Saturday and Sunday have passed already. (laughter)

SENATOR O'SCANLON: Thank you very much.

SENATOR GREENSTEIN: Senator, do you have anything?

SENATOR STANFIELD: Yes; thank you, Chairwoman.

Lieutenant, more of a comment than a question.

I was Sheriff of Burlington County for 18 years, so I worked very closely with our local police chiefs. And I just want to say what a great resource you and your team are. As you mentioned, most local departments don't have somebody on the department that has the type of expertise that's needed in so many of these instances. And you guys, with both your hands-on technical assistance and your training, have been phenomenal.

So I just wanted to thank you and your team.

LIEUTENANT HOPPOCK: Thank you, Senator; I appreciate it. Burlington's a great partner.

SENATOR STANFIELD: Yes.

SENATOR GREENSTEIN: Thank you.

Anybody else have anything? (no response)

Okay; well, I want to thank you very much. We really appreciated your testimony, and we're just starting our hearings on this topic. So we had the two of you today, and then we will probably go from there.

So thanks again.

LIEUTENANT HOPPOCK: Thank you, Senator.

SENATOR GREENSTEIN: We really appreciate it; thank you.

Okay, so that will conclude the cybersecurity part for today. We had two great speakers, and hopefully we all learned a few things.

(MEETING CONCLUDED)