OFFICE OF THE ATTORNEY GENERAL

Adam Paul Laxalt, *Attorney General*

100 North Carson Street
Carson City, NV 89701
Telephone - (775) 684-1100
Fax - (775) 684-1108
Web - http://ag.nv.gov

MEETING MINUTES

Name of Organization: **Technological Crime Advisory Board**

Date and Time of Meeting: **August 15, 2018 at 10:00 a.m.**

Place of Meeting: **Video Conferenced Between:**

Attorney General's Office
Mock Courtroom
100 N. Carson Street
Carson City, Nevada

Attorney General's Office
Sawyer Building, Room 4500
555 E. Washington Avenue
Las Vegas, Nevada

Attendees:

Las Vegas:	Carson City:
Members in Attendance: Adam Laxalt, Chair Bill Olsen, VP IT NV Energy William Wong, proxy for Sonny Vinuya, Asian Chamber of Commerce Greg Weber, VP IT, Valley Bank Captain Harry Fagel, proxy for Christopher Darcy, LVMPD **Members Absent:** Assemblywoman Sandra Jauregi Jacob Cinco Greg Herrera **Guests in Attendance:** Hector Sepulveda, FBI Rod Swanson, AGO Ashanti Lewis, Ferrari Public Affairs	**Executive Director** Patricia Cafferata, AGO **Members in Attendance:** Adam Laxalt, AG, Chair E. Andrew Campbell, CCSD Alan Cunningham, WCSD Senator Mo Denis **Members Absent:** David Haws Chris Lake **Guests in Attendance:** Laura Tucker, DAG, AGO Greg Zunino, DAG, AGO Bob Dehnardt, EITS Sherri McGee, AGO David Linterman, FBI Kevin Vest, FBI Michael Hickok, FBI Lee Marsters, DPS

1. **Call to order and Roll Call.**
Meeting called to order at 10:00 a.m., Marsha Landreth called roll and confirmed there was a quorum present.

2. **Public Comment. Discussion only.**
None.

3. **Welcome and self-introduction of Technological Crime Advisory Board committee members.**
Attorney General Adam Laxalt welcomed everyone to the meeting, and members introduced themselves.

4. **Approval of minutes of May 10, 2018 meeting.**
AG Laxalt asked for approval of the May 10, 2018 meeting minutes. Bill Olson moved to approve the minutes. Harry Fagel seconded the motion, and the motion passed unanimously.

5. **Discussion and report on how the Attorney General's Office handles technological/cybercrime complaints.** Rod Swanson, Chief of Investigations, AGO. *(Attachment Two (2) – Consumer Complaints).*

Rod Swanson: The Attorney General's Office receives complaints in a number of ways: electronically, on our website, mailed in and sometimes people come in person to file their complaints. With respect to the technology crime aspects of what we see, we look at the complaint from a technological crime standpoint versus a cybercrime standpoint. The Attorney General's Office has jurisdiction for technological crime matters. That includes activity that is conducted on computers. Electronic devices are used in furtherance of that activity. Under NRS 228.178, gives the Attorney General's Office has jurisdiction and the authority to investigate those types of crimes. Typically, what the computers and other technology that is used in furtherance of those crimes are usually in forms of theft, forgery, embezzlement, consumer fraud, and deceptive trade practices. The goals of our office with respect to the complaints that we receive, assuming that the complaints are viable, are that the investigation is completed; we put together a case that is prosecutable, and results in the conviction of the bad actor. The other outcome that we are looking for is restitution to the victims to the extent possible. An example of these cases is elder financial exploitation. In many cases, money is transferred from the elder's account without the authority to transfer that money to a personal account of a bad actor who is committing theft. Child identity theft is something that we see. These criminals use social security numbers of children and actually obtain loans; or sometimes, home equity lines of credit. We have seen credit cards in the names of infants. Mortgage fraud and title misrepresentation is another example of these crimes. When purchasing a home, depending on who your mortgage company is, everything is done electronically and some notary shows up at your house one night and you sign all the documents and you just close the sale. We also investigate internet and telephone scams. Most of you have probably gotten the messages from the IRS that you are going to be arrested if you do not pay money in a couple of hours. Some may have received the grandchild call scam where they say your grandson or granddaughter is locked up in Mexico or some other place and you have to send money in order for them to be bailed out. I use those two examples, because there are others, but they are similar and almost without

exception. These crimes are being committed by people who are not even in the United States. They are using Voice Over Internet Protocol phones and masking who they are and where they are from. There is virtually no way, in most cases, for any law enforcement, state, local, or federal agency to effectively track those scams and identify the people involved. That is my overview on how the technological aspects impact criminal activity within the jurisdiction of the Attorney General's Office. We will take reports from anyone and are on the lookout for different kinds of scams, so that we can prepare and release public service announcements (PSAs) about the dangers.

Bill Olsen: At the power company, we have seen a significant uptick in the number of scams where customers are being called and told their power bills are delinquent. They need to pay their bill immediately to prevent their power from being turned off. We have been referring customers who call us to local law enforcement.

AG Laxalt: The biggest thing we can do is join forces and create a PSA of some sort. You can reach your customers whereas we can reach a slightly different audience and create awareness.

Swanson: It is inappropriate for call scams to be referred to local law enforcement agencies.

Captain Harry Fagel: The prevention model needs to be really robust. If private entities such as NV Energy are dealing with customers directly, this has to be part of the education of the customer. We occasionally get lucky; we have local actors who do this, and we arrest them, but the calls are usually from out of town or out of the country. The education piece is really an important part of the whole picture, in my opinion.

6. Discussion and for possible action on cybersecurity trainings in October 2018. Laura Tucker, Senior Deputy Attorney General. (*Attachment Three (3) – Cybersecurity Trainings*).

Laura Tucker: Last year for cybersecurity month (October), we offered several trainings all over the state. Last year's theme was *Cybersecurity for Small Business*. This year, the theme will be *Cybersecurity for Senior Citizens*. There are a lot of seniors who are online now and they have a lot of issues that they face. I set up some dates for these trainings in October – Attachment Three (3). We have good representation around the state. We have trainings scheduled in Southern, Northern and Central Nevada. We are asking for a similar format as last year: A representative from the AG's office, an IT professional, and a local law enforcement representative. Please look at these dates and see what works with your schedule and what you might want to talk about to share with seniors all over the state. They were all very excited. Every single senior center I called said this would be extremely valuable to have these presentations at their centers.

Patty Cafferata: I would like the record to reflect that Senator Denis has joined the meeting in Carson City.

Tucker: Please let me know if you are interested and send me or Patty emails and we will try to get everyone scheduled. Then for those law enforcement representatives that are here, if you have someone that you can send in your jurisdiction, please have them contact me. I

will reach out to local jurisdictions to get someone to come down to talk about trends they are seeing in their areas. My email is LMTucker@ag.nv.gov.

AG Laxalt: Attendees can also email Patty and last year was successful. We presented at small businesses and LVMPD and IT folks were great partners. Anyone can join or attend any of these; they do not have to be a presenter. If there is a particular idea on how you would like to target the Asian Senior Community to speak to Laura and Patty about where there is another venue that you think we should try to contact. The same goes for any other member. Although we are trying to focus on seniors this year, if there are other ideas on how to reach seniors, then please let them know.

William Wong: The Asian Chamber is coordinating with the Spring Valley Metro, and they have formed a team regarding the Spring Mountain Corridor business owner, restaurant owners, and different businesses. He said that this may be a topic of concern to the community and to the businesses.

7. **Presentation on FBI's priorities in cybersecurity from the headquarters to the local level.** FBI Supervisory Special Agent Hector Sepulveda.

Hector Sepulveda: In the top 10 national priorities for the FBI, cyber ranks #3, but #2 is counter intelligence operations. As a program, cyber was started in 2002 and we investigate crimes related to computer intrusions. It tends to be a bit different from just traditional cybercrime. We get involved if it is anything that relates to data that came from a computer intrusion. There are 56 field offices and a huge international presence with over 70 offices worldwide. We have attached people in the consulates who pursue the leads we send them. Our mission statement is: Identify, Pursue, and Defeat. Our programs extend to cyber-adversaries because we cover national security as well. The FBI has an investigative purpose of financial matters. The Department of Justice, compared to all the other agencies that are out there. Our mission is an investigative mission. The Department of Homeland Security (DHS) also has an investigative component. The service also has an investigative purpose of the financial matters. Then, there is the DOD and NSA – all the overseas authorities. We also collaborate through different coordination centers and are one of sixteen intelligence agencies in the nation. We have different methods that we share, similar to the PSAs that you are developing. These are available on our websites. If there is a particular problem in an area, we tend to provide a heads up or do something potentially more proactive in certain crimes. I am going to talk about the things we are seeing in the country and in Nevada.

We have an internet crime complaint center where we receive complaints through email, through a portal, or phone calls. They are referred out to each field office. Here in Las Vegas, we have seven agents that are split 50/50 national security and then cybercrime. We have a Las Vegas Cyber Task Force which includes full-time representation from LVMPD, Henderson, and then we have other part-time members as well.

Typically, computer intrusions cover a whole gamut of things. What groups are doing the hacking? It is everything from nation-states to financially motivated or ideologically motivated intrusions. Types of cyberattacks include attacks based on collecting data for financial means; others are destructive in nature, also for financial means or for national

security issues. Zema Compromise and Ransomware are the top two that affect states. The latest numbers we have are 5 billion dollars in losses cyber committed crimes.

If people do not report, we do not know and this includes many overseas numbers as well.

On ransomware, since we started tracking them, the numbers have lowered, and the losses have been lowering. It is more of an issue with people stop paying the ransom – becoming aware with PSAs and campaigns

AG Laxalt: Are those numbers from here in Nevada?

Sepulveda: They are for the whole country. I can provide specific Nevada State numbers another time. Who are the victims? Everyone. Every aspect of industry and private individuals. We see it in mortgage firms and law firms because of all the wire activity that occurs. For example, an email from an address that you recognize requesting a wire transfer with instructions does not necessarily mean that they have access to their computer system. Many companies put out surprising amounts of information about their top-level employees using social engineering, or just going to their website, so you can find out who their auditor is, or what the name of the CFO is. Until we investigate, we do not really know if there has actually been an intrusion. As of 2016, we had about $3.1 million of self-reported numbers and last year it was about $675,000. I think that is mostly due to public information, PSAs, and companies have to set up ways to verify that wire transfers are legitimate. I just bought a house here in Nevada and I saw how they are handling it. It is just one account for every single wire transfer; it will never change, those are the instructions for them to work it that way.

One of the latest operations out of the Department of Justice was targeting business email compromises. These were all from overseas and the majority of these individuals were arrested in India or Nigeria and some in the U.S. collaborating with those groups. So, back to your question about the numbers, those are what we call "spoofed" numbers. They can be calling from a call center in India or Africa; we would not know. These cases are long and take a lot of time and investigative resources. I will switch over to more of the National Security aspects of some of the things we do. One of the first ones was the Sony attack, which happened in 2014. It was directly attributed to North Korea. The United States Government ended up issuing sanctions to North Korea based on these attacks. Here in Nevada, we had one a while ago, which is the Sands. What that really establishes for the FBI is the model of these types of attacks, how we investigate them. Here is one that targeted PRC, the People's Republic of China. These people were hacking activities for the state to acquire classified information or information for defense contractors across the United States.

8. Update on the security posture within the state. Robert Denhardt, EITS Chief Information Security Officer.

Robert Denhardt: I wanted to give an update on some of the things that they are doing at the Enterprise level as far as security goes. I have updated the security awareness training that we offered. It used to be a package that was static and had not been updated in several years. We have gone now with a new vendor and this training is being rolled out to all state employees. This is a product that is being updated fairly consistently and will have at least a couple of updates every year. It is an interactive training and I cannot stress enough how important security awareness training is; especially in light of phishing attacks. We have technology in place that blocks malicious software that we know of and blocks known phishing techniques and campaigns, but there is always something that might get through when it gets to a person's desk. If they click on it, that creates a bad day for everyone involved. The security awareness training is really the best defense against phishing attacks. If we give our end users the tools and knowledge that they need to know not to click – to identify suspicious emails and give them a mechanism for safely reporting, follow-up and analysis to find out if it is truly malicious or not – that goes a long way in protecting our state from attacks. Most recent statistics I have seen say that 45% or thereabouts of all cybersecurity incidents start with a phish.

We have expanded our continuous monitoring within the state. Our previous license with our managed security service dealt mainly with the perimeter of the state network and is great for dealing with things coming in or going out, but it does not do much for something that is inside that may try to move laterally within the state. We now have the capability of monitoring network devices and servers within the state infrastructure. We have filled a position on my team at the Office of Information Security which is a government risk and compliance position.

Some upcoming initiatives that we have is that we are piloting several programs to ensure IT security within the state. The secure service has a blacklist of known malicious sites and it will block anyone from getting even close to them. It does it automatically; it is all behind the scenes.

We are focused on cloud and mobile work force security strategies because those are state level initiatives. There is a lot of interest in moving to the cloud from agencies along with finding ways for our work force to work mobile and more flexibly. Those things introduce risk, so we want to make sure that we are doing that in a way that we make sure that it is managed.

Senator Mo Denis: I was just recently talking to someone about their business. One of the things they have is a secret shopper sort of thing; they will set up a phishing thing they use that as part of their training, that they can control it. They will tell their employee to not answer the question. Is there anything like that as part of the state training?

Dehnhardt: That is part of the new package and the agency information security officers are excited about that part. I had one rubbing her hands and saying "I am going to phish my director every day." It is a great way to reinforce the training phishes that they send out just

like a normal phishing attack would be. If you click on the link, it will pop up with a short 2-3 minute training that will explain what you missed and what you should have looked for. I know Alan has been using something, but I do not know if you are using such a program.

Alan Cunningham: We took our click through rate from 17% to .2% and we have 76,000 users from staff and students, so it works really great. It was really interesting to see how the numbers fell off quickly once they utilized that video training.

Cunningham: It is a balancing act. I am waiting for the first snow day because that is when the snow day phishing will go up because everyone will click on it. A hacker is going to look for things that target senior people within an organization.

9. Meeting set for 2018 at 10 a.m. in the Attorney General's offices:

- November 14, 2018

AG Laxalt: If anyone has any new topics to address at future meetings, please forward the information/topics to Patty Cafferata for coordination and addition to the agenda.

Senator Denis: I am available to work with anyone who needs any assistance with BDRs or other special projects.

10. Public Comment. Discussion only.
None.

Cafferata: I want to have Lee come up and introduce himself. He is running a new state agency division that has to do with cybersecurity and he just started working for the state.

Lee Marsters: I am Lee Marsters and I am with the Nevada Office of Cyber Defense Coordination. It was established last year and was set up in January. There are four of us and we are looking at the entire State of Nevada. Right now, we are just laying the groundwork by going around and looking at programs, how we can coordinate, and what we can do to make the entire state of Nevada cyber safe. Or at least a little bit safer, we hope. My administrator is Shaun Rahmeyer, our IT person is Jesse Lemos, and we are happy to be here.

AG Laxalt: Glad to have you. Is there any further public comment?
None.

11. Adjournment.
The meeting adjourned at approximately 10:50 a.m.

Minutes respectfully submitted by Marsha Landreth, Office of the Attorney General.