Introduction

Kirsten Barber: Hi, and welcome to the NCDPS Safety Scoop, a podcast sponsored by the North Carolina Department of Public Safety. There are great people, programs and resources within the department. In each episode of the Safety Scoop, we'll share how NCDPS employees prevent, protect and prepare North Carolinians and help enhance safety in our state. We hope you'll listen along and learn something you may not have known about the largest state agency in North Carolina.

[Music]

Julia Jarema: Hi, I'm Julia.

Kirsten: And I'm Kirsten!

Julia: And you're listening to the NCDPS Safety Scoop, a podcast sponsored by the North Carolina Department of Public Safety.

Kirsten: NCDPS is the largest department in the North Carolina state government with some amazing programs and resources…

Julia: …as well as phenomenal personnel and volunteers.

Kirsten: Listen along as we take you behind the scenes and dive into how the people, programs and resources within this department enhance the safety of the people of North Carolina—give you the scoop, if you will, of all things NCDPS.

Julia: NCDPS's mission is to safeguard the people of North Carolina through prevention, protection and preparation. As you listen to this podcast, we hope you'll learn something you may not have known about the ways the people of NCDPS are working to keep our state safe.

[Music]

Season 1 Episode 7

Kirsten: Welcome to the Safety Scoop! Today, we're talking about election security. With elections just around the corner for North Carolina voters, there's a lot of buzz lately regarding election security, so today on the Safety Scoop, we're talking with three people who have been working tirelessly behind the scenes to protect the integrity of North Carolina's elections for both the primary and general elections. Many people may not realize that the Department of Public

Safety has been working with the North Carolina State Board of Elections on cybersecurity issues for the past several years.

Julia: Joining us today are Patrick Gannon with NC State Board of Elections, Will Ray with North Carolina Emergency Management and Lieutenant Colonel Robert Felicio with NC National Guard. Pat Gannon joined the Board of Elections in fall 2016 as the Public Information Officer after a 17-year career as a journalist. He has an extensive background in covering state politics through his time as an editor of *The Insider State Government News*, Capitol Press Association and at the *Wilmington Star News*.

As Chief Information Officer for the North Carolina National Guard, Lieutenant Colonel Robert Felicio manages the information technology systems and communications for the Guard's nearly 12,000 members. He also oversees the state and federal responsive cybersecurity teams that are often called upon to support both private and governmental partners and address international and domestic threats.

Our third guest is Will Ray, Chief of Staff for North Carolina Emergency Management and former Assistant Director for Planning and Homeland Security. In this capacity, Will has been instrumental in coordinating resources to respond to all types of emergencies, including cybersecurity issues. Welcome, gentlemen.

[Overlapping mumbling]

Lt. Col. Robert Felicio: Thanks for having me.

Julia: So, the security surrounding elections in our country has been getting a lot of attention in recent years. What has North Carolina done to protect itself against cyber-attacks or security issues in elections, and is there any history of cyber-attacks on our election system in North Carolina? Pat let's start with you on that.

Pat Gannon: So, uh, first of all, we have no evidence that any cyber-attack has ever changed a single vote in North Carolina, and actually that goes nationwide. We also know that, or we have no evidence that, any cyber-attack has ever really affected an election, uh, per se.

We do so many things it's–it's hard to know where to start. First of all, um, I think what I'd like to stress the most is that every voter in North Carolina in the March 2020 primary and the November general election will vote on a paper ballot. Uh, 93 of the 100 counties will vote with hand-marked paper ballots; the other 7 will have ballot-marking devices that–that are touchscreen machines that then print out a paper record. So, there will be a paper record for every single vote cast in 2020 in North Carolina that if something were to occur, you would have that back-up paper to be audited.

We secure elections before, during and after every election. Before elections is with things such as what we call logic and accuracy testing which tests every machine with sample ballots that we put–pass through the machine to make sure they're counting correctly. Every single voting machine, uh, that–that is used in this state is tested. During the elections, we have observers. We have people from the political parties monitoring every step of the process. After the election, we have post-election audits of the results, a series of those, um, that are conducted. We have an investigations division that if something were to go wrong, we start getting reports of some type of fraud or malfeasance in an election, the investigations division can look into that.

Julia: And Lieutenant Colonel Felicio, did you have anything that you wanted to add?

Lt. Col. Felicio: With respect to cyber security in general and the elections itself, I–I think it's important to understand that there isn't really one element working at anything alone. Collectively as a state, collectively as agencies from state and local counties, Emergency Management… I think it's important to understand that we're–we're all looking at not just election day, but we're looking at that months prior to election day, all the steps leading up to and then all the events after that.

Julia: Okay, well, and that brings up a good point, kind of brings me to my next question. So, which agencies or entities *are* involved in protecting our elections, and can you kind of elaborate a little bit on the importance of these agencies working together? And Pat, we'll go back to you.

Pat: I feel like I'm taking all the–all the time from…

Kirsten: [Laughs]

Pat: …these important partners seated next to me, but, um, so we have many partners, both federal, state and local. Obviously, we work with 100 County Boards of Elections. They're kind of the boots on the ground, the people that handle the day-to-day, uh, aspects of elections administration. We have a very strong partnership with the Department of Homeland Security, uh, as well as the FBI.

If you're listeners didn't know, elections are now considered critical infrastructure in, uh, our country which, uh, puts them on par with the energy sector, the–the water, uh, sector, nuclear, um, very important, uh, part of our country for obvious reasons. And with that designate–that designation, the federal government is working more and more, uh, these days to help secure our elections. We have, like I said, we have a great partnership with the Department of Homeland Security, and then our state partners. Uh, Department of Public Safety is with me here today. The National Guard who's with us here today, the Department of Information Technology, all of us are working together to secure elections, to share information. The federal partnerships are very important because they provide information of things that might be

happening in other parts of the country that then we can act upon here and– and update our systems or–or, um, fix things that might–they could be, uh, a vulnerability.

Um, so, our partnerships are extremely important. I think the average person out there, the average voter, would be shocked at the amount of coordination we have with our state and federal partners, the number of times we meet, the, uh, training exercises we've had, the close, uh, proximity that they are. They're within a really quick phone call or text away from us. And there's a constant, uh, sharing of information that goes along with that. So, it's extremely, extremely important, and again, I think the average person would be very surprised at the level of coordination and cooperation that we have here.

Julia: You mentioned the Department of Public Safety. I think a num–a number of people might be surprised to learn the Department of Public Safety has a role in election security. Will, can you tell us a little bit about what DPS's role is in election security?

Will Ray: Sure. So, I think, um, again, as–as Pat and as Lieutenant Colonel Felicio mentioned, I think any–any response that we are engaged in, any preparedness activity that we do on the front end of that is–is successful because of partnerships that we have, both those here today on the–on this podcast, um, as well as partnerships, um, that are ongoing across our State Emergency Response Team every day. And so, as it relates to elections, I think our focus from the department standpoint is a couple things. One, specifically as it relates to cybersecurity, um, how do we marshal the resources effectively to help, uh, the State Board of Elections as well as local boards of election from a trading technical assistance, uh, support role, both the state and local level? And then, I think broader from a consequence management standpoint, um, how do we marshal the resources of the State Emergency Response Team and those wider state agencies to a-address any needs that may come up during elections? Certainly, as it relates to cybersecurity like we're talking today, um, but also as it relates to, um, something like severe weather, like Hurricane Dorian.

Uh, we happened to be activated, uh, at the state EOC for Hurricane Dorian, and there was a special election that was occurring during that same time, and so there was some–some support of moving resources and people across the state, again, to make sure that citizens of this state were allowed to continue to vote and–and allowed to exercise their rights. So, I think our support is more from a consequence management side, less from a technical side, as it relates to elections. So, in the–in the department, the North Carolina National Guard and our North Carolina Information Sharing and Analysis Center, which is our state's fusion center, um, have a lot of technical capabilities by both a state and reach-back federally on a cybersecurity standpoint.

I think other divisions like Emergency Management or the Highway Patrol or ALE or State Capitol Police, some of the other agencies across DPS, bring resources to bear to support our lead agency for elections. In this case, it would be–it

would be the State Board of Elections. So, again, just reinforcing that I think it takes partnership, and it takes lots of people sitting at the table, both blue sky, day to day, as well as during an event, to make sure that any event that we're dealing with here, North Carolina is successful, whether that is response to a hurricane, whether that is, uh, ensuring a safe and secure election, um, or whether that's dealing with some other incident that–that may come, uh, down the road.

Julia: Um, Lieutenant Colonel Felicio, tell us a little bit more about the National Guard's role specifically in this arena.

Lt. Col. Felicio: With regards to elections being identified as critical infrastructure, um, free and fair elections are the cornerstone of American democracy. So, the United States government, at a federal level and a state level, is committed to protecting the integrity of the United States' elections. It's being critical infrastructure, it fits right into our wheelhouse. Regardless of we're talking about power plants or electricity, whatever one of the sectors you're talking about, we play a role in protecting that and supporting the integrity of that. So, elections falling right in line with that, I think it's important to note that, as Will mentioned from a DPS perspective, us all coming together, it's not just at the state level. So, we lean on those federal partners, and we have those relationships with the FBI. We have those relationships with all the other federal agencies. So, building upon those relationships when events take place, we're able to leverage those during the event and after the event to make sure that we validate whatever issues arise, right? We call them indicators of compromise. If there's any such things, um, we validate those with not just ourselves, but the other partners, and that–those partners may be within DPS, they may be outside of DPS at a federal level or at a local level, but we definitely focus in on whatever they may be. We validate those things.

Julia: Okay, thank you. And I know, I think, you have been–the National Guard has been called upon before to help with cybersecurity issues at the local level, um, to support different, uh, communities and cities and counties in North Carolina as well.

Lt. Col. Felicio: Mmm-hmm.

Will: And I think there's something, too, that's important to point out to that. I think, you know, we talked about some of the–the state partners that are at the table and–and certainly our state leadership across the number of departments, um, it very much wants to, uh, support elections and safe and secure elections, and that's very much a state-level priority. I think it's already been touched on some of the reach-back we have to some of our federal partners across the national security area, but I do think it–we do need to call out that much of this is also done at a local level.

We have partners, um, that are meeting regularly to talk about these exact issues on a local level. How do they support each other? How do they support

their communities? Again, as we talked about, not just related to cyber or elections, kind of all-hazards events, but we have–we have some communities in this state that are very forward-leaning, very progressive and very interested in supporting each other, and so I think, as you look at the tiered response and tiered capabilities here in the state, you know, everybody, I think, always defaults to a federal or state capability, but we have some incredible local partners in our counties and in our towns and other municipalities in the state, um, that I think, uh, bring additional force multipliers to the table when we talk about cyber, when we talk about incident management, when we talk about, uh, moving resources and–and–and personnel, um, into areas that need it.

Lt. Col. Felicio: Also, the–to–to highlight some of the things and organization, I think that's important to note is the NCLGISA. NCLGISA is an association of the North Carolina Local Government Information Technology Professionals. It is an organization made up of county I.T. professionals, so across the state, all the I.T. professionals, they know each other. They have the relationship. They know each other's systems. They know the requirements. So, when issues arise, they have a fellow partner at the county that they can talk to that probably already has dealt with whatever issue that they might be dealing with in their own county. So, we've been working alongside with those lokey–local professionals to help develop the best strategy whether it's before election, during or after; before a cyber incident, during or after an incident. It's really important to know, as–as Will said, I really think a good thing to point out is we are looking at federal and state assets to work with, but those expertise do lie in the counties as well, and the professionals are here throughout the entire state.

Kirsten: As a citizen, what can I do to ensure that my vote is secure?

Pat: Uh, the number one thing, uh, that we like to stress is actually get out and vote. That's the most important thing you can do, uh, in my opinion. If you stop voting because you don't feel confident in the election, you're giving in. You're giving in to the people who want to make you feel like you're not confident in the election. We're here on this pack–podcast, and we work every day to ensure that the election is secure, uh, that every election in North Carolina is secure. So, vote. Encourage your friends and family who are eligible individuals to vote as well. Check your ballot before casting it. Make sure you've filled in all the ovals correctly, um, and that you've actually selected the people that you, uh, wish to vote for. Report problems if you have issues at the polling place. Report problems to somebody who's working there, a precinct official or a–or a poll worker. They're the people who can get in touch with the county board if there's a systemic problem, or they can address an individual problem, if you have a problem, an individual problem as a voter.

Get information from–about elections from elections officials and other government partners. That is incredibly important given all of the misinformation on social media and elsewhere these days. You're going to hear a lot about elections. The best place to go to get it is from your County and State Board of Elections and other reliable sources. Finally, I would say verify

information on social media before you believe it or–or otherwise spread it to–to others. This is an uphill battle. It's a difficult situation because there's so much misinformation out there, and there are people trying to lead you to believe one thing or another whether it's true or partly true or not true at all. So, always make sure you–you verify things for yourself. If–if no–if for nobody else, I mean, you–I would think people would want to know the truth and not–not be misled.

Kirsten: That's a great point. I think as we've seen, uh, social media can definitely be a great tool to connect and to bring people together, but it can also be a source of the spread of misinformation. So, that's a really great point that you brought up.

Will: Well, I think it's important to note social media and the platform itself does a really good job about spreading information as well as opinions.

Kirsten: Definitely.

Will: But understanding the difference between an opinion and a fact is kind of one of the things that we can all do a really, a–a better job at, uh, before spare–spreading more opinions, understanding sometimes that we need to get to a fact.

Julia: Point well taken.

Kirsten: So, as people are considering their candidates, Pat, you mentioned to educate yourself about those who are running and to fill out your ballot correctly. If someone is interested in learning more about those who are running in their county or in the state, where can they go?

Pat: The best thing to do would be to–to find your sample ballot, uh, through our voter lookup tool on our website. If you go to ncsbe.gov, go to the voter search or voter–voter lookup tool. Just type in your first and last names, and it'll pull up a record, and then you click–click through. It's pretty self-explanatory. Click through, and you'll end up with your sample ballot whether it's… If you're a Democrat–Democrat in the primary, you can only vote the Democratic ballot. If you're a Republican or Libertarian, you can only vote those ballots. If you are unaffiliated, you can choose either the Republican, the Democratic or the Libertarian ballot, uh, in North Carolina. So, those are gonna show up in your voter record, uh, through our website, your actual–a sample of your actual ballot that you'll see when you go to the polling place. So, that's the best way to see who's running, what contests are–are on the ballot and who's running in them, and then you can search, you know, local newspapers or the candidate's websites themselves, uh, for information about particular candidates.

Kirsten: And so, I could find my polling place on that site as well?

Pat: You could, yeah.

Kirsten: We've heard a lot in recent years about election interference on social media, like we discussed earlier. Is there a way we can tell which information is legitimate and which is not—fact verse opinion? How would you advise our listeners to ensure the information they are digesting and sharing is real and accurate?

Pat: I would say, just reiterated from before, go to trusted sources whether they be elections officials or media that are–that are trusted. If you haven't heard of the source of a particular news item, uh, it might not be true. Be skeptical if you've never heard of the source. There's a lot of that going on online right now, people trying to spread misinformation. Read the "about us" section of a–of a website or a social media page. That will tell you a little bit about the source, potentially, and what political leaning they may have or who may, um, fund the organization, and that should give you a sense of what, you know, where they're coming from in the information they're providing.

Look for simple things like spelling errors, all caps, weird punctuation. All those things can mean this isn't a very legitimate source. Check the date of the publication. There's a lot of stuff that gets regurgitated on social media that may be one, two, three, ten years old, but they present it as if it's just happening now to try to elicit emotion or, uh, some kind of an opinion from a voter or individual. And if you see something that seems particularly outlandish or hard to believe, it probably *is* not true, so Google it. Try to find another source or a reliable source that's actually publishing that information. And if there are multiple sources, reliable sources, then you can probably trust that the information is true. But if you can't find it reported anywhere else, you can pretty much assume that the vast majority of what you're reading is probably not true.

Julia: So, it sounds like, uh, like you mentioned before, a good place to start for that information is, again, their local news *or* the North Carolina State Board of Elections website, ncsbe.gov, or the county, wherever they live, whichever county they live in, their Board of Elections website.

Lt. Col. Felicio: I think from a citizen's perspective, understanding that this is nothing new. Opinions have been out there forever, and we just need to follow the same process. If you know the–the weather alert that's, or the news, based off of the weather that's out there, we generally check multiple news stations to validate that the weather, or we go outside and we check the temperature ourselves. Just getting back to the basics and understanding that this really is nothing new. Opinions have been out there forever, just now we have, um, some efficiencies with technology, so that drives the speed in which the information gets out there and gets spread. So, if there's an information–a piece of information, whether it's right or wrong, technology's there to spread it as fast as possible. Don't just focus on the technology challenges that are out there, but really focus in as a person, have I been solving this problem in the past? It's really no different.

Julia: Very good information.

Will: And I would say just, again, to reiterate that there needs a level of personal ownership in this, recognizing that your vote counts. Your vote is valuable. This is an important exercise and to take that responsibility on yourself to, as Pat and Robbie have mentioned, to do your own research, to validate things you're reading, to really take the time to do that research and prepare, uh, to cast your vote.

Pat: I'll mention one other thing: get outside of your echo chamber. Social media, a lot of times, you're in–you're in a group of like-minded individuals who think the same way, and they're just gonna reinforce and reinforce your view as it is. Get outside that comfort zone and–and see what another source might have, another news station or another advocacy group or some other viewpoint, and then, you know, make your decision based on all the available information, not just the information that's in your small little circle.

Kirsten: Great point. Lastly, what can you tell us about how potential cybersecurity threats are identified and dealt with?

Lt. Col. Felicio: Potential cybersecurity threats, whether they're at state, local or federal levels, are generally dealt with a whole-of-state, whole-of-nation, whole-of-county approach. So, from a National Guard perspective, we have a Cyber Security Response Force. Now, that Cyber Security Response Force is built with approximately 30+ individuals who have civilian-acquired and DOD-tested, uh, cyber experience that allows the National Guard to make a unique contribution to cybersecurity. Now, we fit this Cyber Security Response Force working alongside with the county partners, Emergency Management, DIT, and when a threat is identified, we all assess and evaluate the right approach to dealing with that threat.

So, whether it's a domestic or an international threat that's targeting critical infrastructure, it is really irrelevant. We have taken a group approach to solving those problems because we understand that while we all have our specialized areas of focus, knowing that the entire team can help deal with those threats, and we've dealt with a lot of those. The team has been working alongside our partners for quite a few years now. Specifically with the threats, I think some of the things that we can talk about is while we've dealt with, uh, potential or actual attacks at the county level, the team has responded along with our partners, uh, and while we've responded, we have worked through in identifying what I've called indicators of compromise previously. So, these indicators of compromise are shared amongst the other partners.

And so, it's important to understand that while we're dealing with a threat, whatever that may be, and we identify those indicators of compromise, once that victim allows that information to be shared and clears that information, that then goes through the fusion center and gets published to where they have allowed. And the reason why I bring this up is–is this is the way our state deals

with it. Once the victim says, “Yes, we’re okay with sharing this information,” and it gets out, we’ve seen huge dividends on that stopping other attacks. So, we've seen specifically in one event, um, a victim was allow–allowed to share ten different indicators of compromise. Within three hours of them sharing that, across the state six other entities within the state had seen those indicators, and they had stopped the attack from then taking further growth in their environment. So, they actually stopped it before anything actually happened.

Julia: Okay, so you’re talking about a victim. And it… I'm assuming then that you’re talking about a local government or a company or something like that. This is not a person or a family. And if I understood you correctly, that sounds like y-you're working as a team approach in that with that victim, as you said, or company or agency or government or whatever, to identity, okay, here are some of the flags that we saw. Here are some of the indicators that we saw, and then you're able to then share that information out more publicly to similar groups so that others can then say, “Wait a minute; we saw that too.”

Lt. Col. Felicio: That's ex–that’s exactly right. But I think, one thing you said I want to just make sure is clear, so we are one government entity helping another government entity.

Julia: Sure.

Lt. Col. Felicio: So, with respect to private entities or companies, we really focus on critical infrastructure, as well as local and county.

Julia: So, you’re talking local and county. Local, county governments. Okay.

Lt. Col. Felicio: Yeah, that’s exactly right.

Julia: But those are the victims you're talking about, as opposed to not a business or a family or another individual.

Lt. Col. Felicio: That is correct.

Will: State government, too.

Lt. Col. Felicio: Or state government as well.

Julia: State government. Yep. Okay.

Lt. Col. Felicio: Yep. So, back in 2014, uh, there was a memorandum of understanding that was developed between Emergency Management, Department of Public Safety, DIT, as well as the North Carolina National Guard. That allowed this team to stand up, to develop and to start working together. So, this has been going on for a long time.

Will: And so, day to day, I think what that looks like is you have DIT, Emergency Management, National Guard co-located together, talking about responding to, planning for, training on how we would respond to cybersecurity incidents, um, anywhere in our state. And then, I think, uh, during an event, um, should something happen, should sort of incident or disruption occur, there is an all-hazards framework for these resources and personnel to be put into action. And I think, as you had alluded to earlier, you know, this is an existing framework that we have to respond to all hazards, to include cyber, and so making sure that, I think, listeners understand that there is a framework for us to respond to these events, um, there is a system, um, and an infrastructure to do so. And I think it is important to note that, again, that is only successful through the multi-agency approach that–that we've talked about, um, bringing all of the resources to bear to be able to respond to whatever the incident is.

And if it's a cybersecurity incident, we have some incredible resources in the National Guard, in DIT, in some of our cyber unit that's linked between EM and the and–and the fusion center. And our role in emergency management is really to let them do what they do, allow them to be the technical expert and subject matter experts, identify, mitigate, deal with the threat. Um, and from a consequence management standpoint, how do we come alongside and make sure that the rest of the county infrastructure or town or city infrastructure is–is supported? Um, that daily life continues to move on? That services continue to operate, that people still are able to access the things that they need to have on–on a day-to-day basis? And again, I–I–I don't think we can say it enough here today. I think partnership and–and people communicating about both what's going on and about what needs may be is what's going to make all of this successful.

Pat: I think one additional piece I really want to hone in on is this is, Will said it earlier, but we do not treat this any different than any other event. So, with regards to securing or the cybersecurity requirements for an election or responding to a hurricane, Will hit the nail on the head. We want to ensure everybody understands there's no difference. So, if you need support, you–there's local emergency management directors that are there. That information, they're there to be used. They have resources at the state level, and then we respond accordingly. So, with regards to the state election or a local election or a hurricane or snowstorm, it's all the same. We follow the same processes 'cause they've been tried, they've been successful and we get response back to the citizens of North Carolina extremely fast using the process that's already in place.

Lt. Col. Felicio: Just so, um, the listeners get a kind of sense of this, the scope we're dealing with, this could be anything from a local emergency management department delivering fans to a polling site where they're having humidity issues and the–the ballots aren't going into a tabulator to responding to a major cyber-attack or violence at a polling place or–or whatever. These are the types of things, this is why we have this partnership, not only to–to solve the little things that happen in just about every election or to help us with more boots on the ground or

more–more people to help assist and things like that, but also to be prepared, uh, as much as we possibly can to a major event, um, if it were to happen.

Kirsten: There's all these different variables that need to be considered, it sounds like, and so this partnership, again, to reiterate, just sounds very important. And, um, as a citizen of North Carolina myself, I do appreciate all the effort that's being taken just to protect my right to vote. Thanks for joining us, and if you'd like to do more research, find your polling place, see all the candidates running, go to n-c-s-b-e dot g-o-v. That's ncsbe.gov.

Conclusion

[Music]

Julia: Thanks for listening to this episode of the Safety Scoop. To learn more about NCDPS, go to ncdps.gov. Tune in next time on your favorite podcast app to hear more behind-the-scenes stories from the North Carolina Department of Public Safety.

[Music]