

Introduction

[Music]

Kirsten: You're listening to the NCDPS Safety Scoop, a podcast that dives into the stories of the people, programs and resources within the North Carolina Department of Public Safety. Each episode will give you the scoop from department personnel on how NCDPS enhances the safety of the people of North Carolina.

[Music]

[Pause]

Season 2 Episode 14

Kirsten: In previous podcasts, we've put a focus on discussing natural hazards and sharing advice on how the people of North Carolina can effectively prepare and safely respond to them. In this Safety Scoop episode, we're pivoting a bit and focusing on the prevention and protection portion of the Department of Public Safety's mission. In this episode, our guest, Rachel McGrath, critical infrastructure specialist, gives us a peek behind the curtain of how her section within the Division of Emergency Management responds to all hazards, natural and man-made.

Rachel McGrath: Hi, my name is Rachel McGrath. I'm a critical infrastructure specialist here at North Carolina Emergency Management within our Homeland Security section. I've been in this role for two and a half months. So not a lot of time. Before starting with DPS, I worked in federal government.

Kirsten: November is critical infrastructure security and resiliency month, but what does that really mean for you and me? This recognition period highlights the importance of the 16 critical infrastructure sectors considered vital to the safety and security of our nation. These are: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial bases, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactor materials and waste, transportation systems and water wastewater systems.

These critical infrastructure sectors essentially make our world go round day to day. When things are going well and the individuals and tools entrusted to protect these sectors are effective, no one blinks an eye. However, when something goes awry—a storm impacts one or more of these sectors, or a bad actor targets and infiltrates any of these—we notice. Going into this recording, I knew very little about any of these critical infrastructure sectors. It was fascinating to speak with Rachel, and I walked away with a little more knowledge of what goes on to ensure my lights turn on when I hit the switch, the grocery store shelves are stocked and the state cyberspace is secure.

We're really looking forward to hearing kind of your perspective of all things infrastructure within Emergency Management. Can you give us an idea of where does the infrastructure section fall within the Division of Emergency Management.

Rachel: Our critical infrastructure portion falls within our Homeland Security section. And so, generally our section kind of has dual hats where we do the infrastructure side of the house which is where I work. That's going to be more traditional, physical infrastructure, things like water, roadways, power, electricity, that sort of expertise, and then the other portion of Homeland Security focuses more on cyber threats. So, we work together to kind of provide a more holistic view of hazards that impact North Carolina and North Carolinians. And we are our own section, but we work very closely with our partnering sections, so, like, when we're activated as a critical infrastructure specialist, I report within the operation section, so we also have that flexibility and duality there. So, we work very closely with them. We also work with our plan section, logistics, et cetera. So, we all work together pretty—pretty closely for activations and other kinds of tabletop exercises we do and trainings.

Kirsten: But when you say “activated,” can you kind of define that for our listeners?

Rachel: So, and as I'm also new to this, my understanding is: as the state EOC, we have different levels of activation that we have here. So, if you think about, like, I don't know, in like a very aggressive, military version, like DEFCON. You have, like, DEFCON 1 through 5, where you have different levels of how intensely engaged you are. Not nearly to the extent here, but we have enhanced watch, and we have activation. So, when we're dealing with different hazards that the state experiences, we have different activation postures. So, maybe a better example would be like with Hurricane Idalia, so we were fully activated for that. That meant that my sections, as well as our, like, counterparts, we were all here in the building working with our partners. And we all sit in the same room and work together, so when we're dealing with things like power outages, we have contacts in the room that we can talk to and resolve issues that might come up.

We also work in infrastructure. We work primarily with, I think, 12 essential functions which we call it ESSFs. So, in critical infrastructure we deal with ESSF 1, 3, and 12, mostly, which are transportation, water and electricity. Those are the partnerships that we work with frequently, and when we're activated, we work with those partners. Different activations have different focuses. So, hurricanes are kind of like a traditional natural hazard that we deal with. We'd be working with similar partners for things like winter weather. So, if there's a big ice storm, you're out of power. We work to try and help our partners with state resources that they may need, as well as providing information-sharing, so that we're all on the same page and can help you as a North Carolinian get your power back.

Or, you know, dealing with flooding, et cetera, so it's not just power, but a lot of infrastructure things, when they're working well, you don't notice them being

there. You expect when you flip a switch that your power is going to turn on or that you're going to have running water, that your roadways are not flooded. And when those things go wrong, they really impact your day-to-day living. So, we help kind of smooth those things out and provide, like I was saying, information-sharing and—and resources, so our successes are our partners successes. We really just help facilitate, and so that's a little bit of what we do on kind of the natural hazards side of things.

Kirsten:

To add to Rachel's statement, tucked away off of Blue Ridge Road in Raleigh, in the same secure facility as North Carolina National Guard's Joint Force Headquarters, is the North Carolina State Emergency Operations Center which is also where Rachel and her team work. In fact, many members of the North Carolina Emergency Management team work here daily, but in times of emergency or during disasters this building is transformed into an operational war center of state and federal agencies, nonprofit relief organizations, faith-based organizations and sometimes private sector companies. Known as the State Emergency Response Team, these partners work to protect the people of North Carolina under the command of the SERT leader. The state EOC is partially or fully activated depending on the magnitude of an event. The North Carolina emergency management sections that work with federal, state and county level partners during these events include operations, logistics, information and planning, Joint Information Center and the business EOC.

Can you take us into how your section upholds North Carolina Emergency Management's mission to prepare for all hazards and build a more prepared North Carolina?

Rachel:

Yeah. Our section is definitely very pro-all-hazards, and having that perspective, which really isn't any different than a more traditional focus on natural hazards, it's just opening up that aperture a little bit wider and using those same skills and partnerships to look at other issues that might be affecting North Carolinians. So, as I mentioned before, cyber is something that our section works with, and you know if your school system or hospital system is hit with ransomware, that takes you out just as much as a power outage does or flooding, and those things really have cascading effects. So, it's taking that more traditional lens and expanding it further.

Another thing that we do is support election infrastructure. So, we work with state board of elections. Yeah, we with partners not only with getting power back or rerouting roads or that sort of thing; we also work with partners on intelligence. So, we use intelligence to inform how we respond to things, and one of our critical infrastructure sectors is with government buildings. And so, if you were to have, like, a civil disturbance or, you know, a civil disturbance that blocks roads, like, that impacts infrastructure. And so, that's a different lens to look at things, even though that's kind of more within a traditional law enforcement space, there is an intersection with infrastructure as well. So, we work with those partners and kind of providing that—that extra perspective that

goes beyond kind of a siloed approach of, you know, “what is this hazard, what is this dealing with.”

Kirsten: Though the critical infrastructure team has amassed a group of subject matter experts with years of experience in their specified areas, no team is complete without their suite of tools at hand. Rachel had a few examples to share. Two of these include the threat and hazard identification and risk assessment, also known as THIRA, and the stakeholder preparedness review, or SPR.

Rachel: In Homeland Security, we also use the THIRA-SPR process, but essentially, it's a threat analysis tool and vulnerability tool that we use that helps kind of identify gaps that our partner organizations might have within their infrastructure or, you know, kind of within their general security posture, and allows for those vulnerabilities to be identified so that they can be filled. So, one of the—when we're thinking about THIRA-SPR and vulnerability assessments, we generally think about three general categories, one being natural hazards, that's going to be your hurricanes, wildfires, winter weather, that sort of thing. You have, like, a technical threat which I don't love the term “technical,” but essentially what they mean by that is an issue with system. So, if you were to have a tanker truck with hazardous materials that tips over, right? It's not really anyone's fault, but accidents happen, and then you have to deal with a cleanup of, you know, HAZMAT. And then, we think about a human-caused issue which is going to be like an intentional harm that's done. So, that would be like a terrorist attack or sabotage or something like that where we're able to, from our perspective and using that process, try and look at what are possible scenarios that could happen and how would you be able to reasonably change your systems or your protections to be able to stave off something like that, right?

So, it's not just, you know, one thing, but a lot of different things, and we partner with not only our, like, local and private partners, but we also have federal partnerships that we work with as well. So, one of our partners is DHS and, specifically, CISA, and, like them, we help with safe assessments which are security at first entry, and that's a type of assessment that CISA provides to local and other partner facilities. So, that's more of a physical security assessment that's done. And so, we work with them in that and help support DHS in that mission as well. That's a lot of words that I've said. But generally, like, there's a lot of ways in which we can engage in all hazards. A lot it is preparation and how we were able to help in kind of response to things like that happening, but we also want to provide the tools so that people are better prepared for things like that that could happen and providing those tools on—the front end and trying to connect our partners with those types of tools that would be able to help them.

Kirsten: Definitely. And I love all these examples that you're giving. You're painting a really good picture of how Emergency Management, even though we see a lot of coverage of Emergency Management professionals when natural hazards happen. I mean we all know that North Carolina sees a lot of hurricane activity, and we're about to see the end of the Atlantic hurricane season. But there's so

much more that goes on behind the scenes and, kind of like you said earlier with infrastructure, you really want to kind of be an invisible force that's helping things move along to prepare and protect but not really be noticed. Like, you don't want roads to be blocked for people to not have electricity because that is something that really goes noticed and can really impact lives, can impact hospitals, schools, just making dinner! And the work that you guys are doing are really helping people go to sleep at night and to feel rested when they wake up the next day knowing that the things that they rely on to live and to work are going to work.

So, that's really interesting that you gave all those examples because things that people might not even think about that could happen and have a severe impact on their day-to-day. So, now that you've provided all these examples and we've talked about the preparation component, can you kind of take us behind the scenes, where you can, and tell us what happens day to day in your sections and what can cause things to be elevated or lead to these activations like you talked about earlier?

Rachel.

Sure. One of the things that I really enjoy about this role is that your day-to-day can really vary. And so, there are 16 critical infrastructure sectors, and they're everything from the chemical sector to dams to food and agriculture, energy, transportation, water wastewater, so there's a lot of different pots that we get to put our hands into. So, everyday can look quite different from the previous day. One of the major parts of our role is to build relationships, and by building relationships we're able to, you know, really have a force multiplier when we encounter, you know, activations or kind of unexpected situations because we have those relationships where you can call up your partner and say, "hey, what's going on," and be able to provide information-sharing and validate what's going on on the ground. You don't want to be in the middle of a hurricane trying to figure out who you need to call. By already having that in place you're able to facilitate the work that Emergency Management does a lot more effectively, and some of the ways we build relationships are by participating and providing different trainings.

So, we in Emergency Management do a lot of tabletop exercises with our partners, and we also will participate with our partners when they put on something. We also will put on different exercises for them to come here and for us to work through sticky situations or possibilities of "okay, what do we do if x, y, or z happens?" And providing a no-fault environment for those conversations to happen. So, that's one of the major things that we do kind of on the back end. A lot of it is, you know, kind of being involved with our partners when they have projects that are coming up and saying, "hey, what do you need from North Carolina Emergency Management?" We're here to help and to provide that support. We're not dictating to our partners what they should be doing, but we want to be a good partner to them and provide the resources that they need or a different perspective that Emergency Management is maybe better equipped to provide. And one of the things as, like, a critical infrastructure specialist, like, I'm not an expert in dams or water

systems or electricity, energy, that sort of thing, but through my position am able to get kind of more of an eagle-eye perspective and think about the interconnectivities between those sectors and provide that insight of, “hey, have you thought about this,” or “here is a way in which this one instance could impact these other sectors” that are maybe beyond what each of those individual entities is tasked think about. Right? And no one can do everything, right?

[Laughs]

So, we're here to provide that extra perspective and be able to connect those partners that maybe wouldn't necessarily have those conversations and, you know, be able to help create those—those relationships as well.

Kirsten: Definitely. I mean, I'm hearing collaboration, teamwork, subject matter experts. I mean, you said there are 16 critical infrastructure sectors. I mean, there is no way. I mean, maybe someone out there knows enough about each one of these, but the probability of that is very small.

Rachel: And you have so many smart engineers and subject matter experts on—in all of these sectors. And we are able to learn from their expertise and use that in order to help North Carolinians and also, like, the work we do isn't only in North Carolina. Right? Like, these critical infrastructure sectors are not necessarily connected to state borders, right? So, like if you have a waterway that goes between Tennessee and North Carolina, what happens in Tennessee or Virginia, or if we have an issue here that could also affect South Carolina, like, we're not only working in a vacuum either you know, we're dealing with our partnering states and, you know, other states elsewhere that maybe don't border us but have dealt with similar problems. So, it's definitely interconnected beyond just beyond between sectors but also geographically as well. So, we're one part of, you know, a major system.

Kirsten: In 2023, are there specific infrastructure risks or threats that you want people of North Carolina to know about? Is there anything that they can do on their end to help protect our state's infrastructure?

Rachel: Not necessarily rocket science, but you know, always having good cyber hygiene is, you know, something that's recommended. And being aware of your company or your business's cyber policies and, you know, doing things like having a strong password and not sharing those passwords with other individuals and using two-factor authentication. Those things can really make a difference. And being aware of what kind of nefarious activity your company or if you could be targeted with things like phishing and ransomware and, you know, generally being aware of ways in which you or your company could be targeted in a cyberspace and, you know, doing easy things like having a strong password and changing your password up, and, you know, not—not falling into some of those easy-way-out kind of things that we're all tempted to do. But, you know, really keeping good cyber hygiene is definitely something that pays

dividends, and you don't necessarily see it until you have an issue, so it's definitely an ounce of prevention, a pound of cure. So, that's, you know, something that is always worth, you know, keeping in mind.

Kirsten: Very good reminder. You've spoken about the types of partnerships. Anything else to add about how they help your team achieve your mission day to day?

Rachel: I think just, again, like, when our partners succeed, we succeed. And what we do is really to help support our partners. We want to be a conduit for information-sharing and working together and providing that support, and all of our partners really help us with that mission, and I've had such a pleasure getting to meet our partners and work with them and learn from them and be able to expand my own knowledge base and, you know, be able to provide different perspective and, you know, be able to have those conversations that really pay dividends down the road, so yeah. We have so many partnerships.

[Laughs]

And they all are, you know, really valuable to us. And so, we also, like, thank our partners for working with us and being willing participants in those conversations because it really does help. We all want to work towards a safer, more secure future for North Carolinians.

Kirsten: In the two months you've been with DPS, or I don't know if you've heard, any "success stories," as I like to call them on the podcast. But anything you can share with our listeners about something that either you've experienced or you've heard that has gone really well, a job well done, from previous incidents.

Rachel: I think anytime that we have the ability to work together and, you know, resolve incidents is a success. And anytime we activate for a hurricane or other natural disaster, or we activated for different kind of all-hazards, we were able to support our partners with—at state board of election, you know, all of those things are, you know, successes for us. And when we can provide that support, that's a success to us.

Kirsten: Well, thank you for—thank you for coming on, really appreciate it. And in two months...

Rachel: Yeah. [Laughs]

Kirsten: ...you have really absorbed a lot!

[Both laugh]

Rachel: Yeah, it's definitely been quite the learning curve but honestly really fun.

Conclusion

[Music]

Kirsten:

This is the Safety Scoop, a podcast written, produced and edited by the North Carolina Department of Public Safety communications team. The mission of DPS is to safeguard and preserve the lives and property of the people of North Carolina through preparation, prevention and protection with integrity and honor. Follow the department on social media for a closer look at ongoing initiatives and resources. We're on Facebook, X and Instagram at NC Public Safety. If you've enjoyed today's episode, be sure to subscribe to the Safety Scoop on your favorite podcast app. I'm your host Kirsten Barber. Thanks for listening.

[Music]