John, let's start with you. Can you discuss the importance of substation physical security and outline some of the technologies in place to keep the grid safer?

Sure thing. Uh, a- as you know, electricity is tied to everything we do on a daily basis. Uh, knowing that there's bad actors out there looking for vulnerabilities and opportunities to disrupt or destroy our critical infrastructure, it's important that we act- adequately protect our substations against these possible threats that are out there. So, in order to effectively do this, we're constantly assessing the current threat environment related to our substations. We not only look at current threats but also at new and evolving threats we foresee becoming a concern. We conduct thorough, uh, security risk assessments at our most critical substations to determine if our current security posture is adequate. And if not, what additional security measures could be deployed to mitigate any vulnerabilities and threats.

These assessments aren't just a one-time effort. We conduct these on a reoccurring schedule so that we are constantly- so that we constantly get a fresh look at each of our sites. We also conduct security risk assessments at other high priority substations in our footprint as needed to ensure we have the appropriate security measures in place at those sites, as well. Our security motto in protecting our substations is based on the principles of deter, detect, delay, communicate, and respond. And I'd like to step through each- each of these one by one, if I could.

First off, we want to have measures in place that would deter any potential attack. This could be the height of the fence or other visible measures like seeing cameras and lighting all around the entire perimeter of the site. The goal is to demonstrate that a site's very well protected and that a successful attack would not be likely, not to mention the chances of being apprehended while conducting an attack are very high.

We also want to ensure we have adequate measures in place to detect an attack in progress- in progress and quickly get law enforcement out to the site to investigate. We have multiple measures and layers of defense in place to detect any likely attacks in the area. The detection is critical to the next category, which is delay. Our goal is to be aware of someone's presence prior to them attempting to breach the perimeter.

These physical security measures at the perimeter are intended to delay one's effort to break through the site and enter into the substation area. One measure that's always in this category, of course, is our security fence. We want to make sure it's difficult to climb, to go under, or to cut through. This delay, in combination with the earlier detection, allows law enforcement adequate time to respond to the scene and apprehend the offender.

And then the last two categories, communicate and respond, they kind of go hand-in-hand. The ability to effectively communicate the details of a breach to our security team, operations teams, and law enforce- law enforcement is critical. Each of these groups also play a role in the proper response. We have a very robust law enforcement outreach program where we meet with local, state, and federal law enforcement to discuss things like response protocols. We provide presentations on substations, kind of like a substations 101. And then, lastly, we provide tours of our most critical substations so that they have some familiarity with the sites. This is important as we don't want their response to one of these sites to be the first time that they've been there.

And then, lastly, for the second part of your question, regarding discussing some of the technologies in place at our substations, for obvious reasons, you know, I won't go into a great amount of detail on this, but I can assure you that we have some of the best technologies in place for detection. Everything from HD cameras, full access control at entrances, and a slew of layered detection measures. Our technical

security team's also constantly looking at new technologies out there and deploying new measures, when appropriate, to further enhance our current security model. I hope that covered your question.

It does. Thank you, John, and it's fascinating to hear how much truly goes into keeping our facilities safer. Thank you so much for your insight. Turning to you now, Adam, corporate intelligence and security utilizes a converge security model which puts both physical and cybersecurity into the same department. Can you explain how that keeps, uh, excuse. Can you explain, uh, the benefits of that model?

Yeah, you bet, uh, Nadia. I'll- I'll back up, um, into my career in government to- to sort of answer that, because I think it's not just, um, sort of a change in dominion energy's thinking about security, uh, and security even is a bit of an outdated term. I think, these days, it's really enterprise defense. And we use the- the notion of enterprise defense because we're really trying to shift the strategic understanding of risk, security risk, to large commercial enterprises from, uh, responding when bad things happen to actually preventing them in the first place. And we see that in our compliance standards and John, I think, brilliantly went through how we scope our compliance obligations and meet them, and in most cases, exceed them.

Um, but compliance is really just an undergirding, uh, safeguard from which we jump off into enterprise defense, which is a much more nimble and proactive way of managing risk, uh, to- to, uh, to commercial space. In my time at government, I joined the FBI cyber division in 2005. The division stood up, uh, in 2003. So it was only two years old when I arrived there, serving in a chief of staff position to the assistant director.

And the biggest challenge that we faced, uh, as a brand new division was to engage those elements, uh, whether they're key national assets, critical infrastructure, or just large commercial enterprises in a way that they were willing to share their threats, gaps, and vulnerabilities as they saw them with us as we were trying to manage the threats, um, from a national security and a criminal perspective- perspectives. Um, and they frankly just didn't want to talk to us, uh, when I was at FBI, for obvious reasons.

There's reputational risk attended a clear understanding of- of gaps and vulnerabilities that commercial enterprises hold. They don't necessarily want to be on the front page of The Wall Street Journal showing that they had a major gap and how they're administering security around their networks and other things. So, flash forward now 20 years, and companies like Dominion Energy ... and it doesn't just have to be, uh, critical infrastructure. It can really be any large Fortune 500 or- or even medium-size companies.

hey must, in order to manage risk and- and convince their- their shareholders and- and their boards of directors, they must demonstrate that they're partnering with government to manage those risks, that they're getting the very best threat intelligence, that they're getting the very best in incident response. When something does go wrong, government's going to show up, whether it's federal, state, or local government agencies, they will show up in the event of a major incident. Whether it's a cyber incident or a physical threat, um, attacking one of our substations or surveilling with a, with a drone device or some other type of surveillance device. Um, we've certainly seen all of the above, even in my- my short five years here at Dominion Energy, we've seen all of that. John manages that in his day-to-day work, every single day.

So, um, you asked specifically about converging security. So, if you think about the- the threats and you think about them from sort of a mission center perspective, if you're dealing with a nation-state threat actor or you're dealing with a terrorist organization, or you're dealing with a radical environmental extremist organization, or you're just dealing, frankly, with somebody disgruntled about the cost of their bill. Um, there's not some singular way that that threat actor is going to try and achieve, um, harm on

Dominion Energy. They may attack through the cyber vector. They may attack physically. They may do both. They may do both in concert. They may, in fact, try to get a job at Dominion Energy so that they will have placement and access to do harm to the company as an insider. Um, and we've seen that, too.

So, if you don't have a clear understanding of everything that's happening on your network, who's accessing what type of proprietary sensitive, uh, customer PII type of data, and you're unable to marry that up with cameras and access controls and, um, employee information, uh, performance data. If you have somebody who's precipitously dropping in performance, they're engaging in behaviors of concern, they're threatening or disruptive to their colleagues and co-workers, you want to know real time what they're doing on the computer network, as well.

So, managing those threats means that all of the security disciplines are talking to one another, that they're all sharing information so that we have a very clear understanding of what the threats are to our company.

Thank you for going over all of that, Adam, and for sharing your background and how all those dots connect. John, what challenges does your team face when implementing those security standards? And Adam, can you talk about how Dominion Energy stays current on the threats that you just mentioned, pose to our critical infrastructure and what those threats might look like.

Sure thing. Uh, yeah, we- we have a very robust security program at Dominion Energy. I would argue that it's- it's one of the best in the country. We've developed a real strong relationship with both our operations and constructions teams. And so we have a pretty good refined process from start to finish and getting our security measures implement. Uh, we work closely with our engineering standards group to ensure we have the most appropriate and cost effective measures in place for all the different levels of substation security in our footprint. Not all substations get the same security measures, so we have- we have a process in place, uh, utilizing specific criteria to help us gauge what sites get what levels of security. All this helps ensure our implementation process is smooth and efficient.

On the side of, uh, understanding the threat and being able to put it into context, um, I'll just start, uh, sort of expanding internally to- to our external relationships and how we get smart on the threats, uh, that we face. Internally, folks like John, many of our leaders, um, across, uh, CIS here at Dominion are former law enforcement or leaders in law enforcement, more particularly. And they understand what information is critical to defending our company. They understand risk. They understand the language of law enforcement, which is where we get a whole lot of our understanding about threats that, uh, could potentially impact our company and- and our workforce.

So, we have a really, really smart, uh, really, really, um, uh, experienced, uh, team of former law enforcement, former federal government folks, uh, in our CIS organization. Um, those- those law enforcement leaders, those government leaders, have been able to tap into the areas of, uh, information. Whether it's the Virginia State Police-led Fusion Center here in central Virginia or my former, um, uh, agency, the FBI, where we have, uh, the- the ... just speaking about Virginia, but we certainly, across our footprint, have other field offices. But we have the Washington field office, we have the Richmond field office, and we have the Norfolk field office serving, um, our footprint here in Virginia.

We have relationships, very close, real-time information sharing relationships with all three of those offices. And we also have information sharing with the FBI's cyber division at FBI headquarters in Washington, DC. We have, uh, a real-time, uh, virtual presence, uh, in our threat center, uh, with DHS. Its intelligence and analysis, um, division, and, uh, CISA. The Cybersecurity and Infrastructure Security Agency. Uh, both of those elements within DHS share information with us. And we share information with them, and it- and it's- we don't share our- our, uh, proprietary information. What we share are indicators that we observe in the network that, uh, reveal a potential threat. And then we will work with

them to unravel, uh, what we're seeing and make a determination, is there some mitigating steps we must take to manage that? Is it, in fact, a threat? Something that we need to address?

We're not going to be able to do that on our own because the only thing we know is what we see within our own networks. We need to use those government sources to make sense of it, and that's what those relationships, uh, are for for us. Um, we have the national security agency, the NSA, constantly scanning the perimeter of our network, looking for vulnerabilities to make us stronger. Um, when they find those vulnerabilities, they communicate them to us and we close those gaps and we get harder as a target, uh, for a hostile, uh, threat actor. So, those relationships are not just a shared value. They're frankly essential for John and his team and- and our cyber teams and our- our insider threat program to be able to put those pieces together to understand the threat. We can't do it, we only have one perspective. So we need all of those other perspectives to make sense of the threat issues we face.

Thank you, Adam. And outside of those strategic relationships, how does your team ensure our strict cybersecurity protocols are implemented properly?

There are a variety of ways. Um, there are the sort of obvious, uh, ways that any responsible company tries to prepare its workforce for encountering security, um, issues in their daily work. So, we provide training. Some of that training is required. Our regulators require us to issue certain training, uh, to our workforce to meet the regulatory requirements. We go above and beyond that. We- we're always mindful that we're not bombarding our folks with training and being inefficient in how we deliver it. So, we've come up with creative and shortened and efficient ways of delivering the most, uh, impactful information to our workforce to make them smarter about cybersecurity threats in particular, but all our threats, really.

Um, the other part of that is not just training them but, but building within Dominion Energy a security culture. One of the things that was most attractive to me when I joined, uh, Dominion Energy, uh, five years ago as a corporate officer ... In fact, I'm the first, uh, corporate officer responsible for security, um, at Dominion Energy. And one of the things that was most attractive to me was the safety culture here. And- and frankly, the overall sort of esprit de corps and identification of our workforce as Dominion Energy family. Um, if you will. But also, the things that came with that were really disciplined, uh, practices and an understanding that, um, we're only as good as a company as we are able to keep our operational folks working in- in hazardous environments, uh, safe.

Well, part of that safety culture is also making sure you're secure because security threats, let's face it, at the end of the day, result in, uh, injury at some level. Whether it's outages causing injury to our customers, um, whether it's, uh, communications failures that cause potential vulnerabilities for folks that are unable to- to communicate with their ops centers or their leadership, or- or just day-to-day communications with their teams. That puts people at risk. So I've tried to align our- our security culture with the safety culture, and I think we've had a lot of success in doing that. As I move around the company and talks to folks, they seem to really put those things in the proper context. Um, but also, uh, you know, that's- that's the- the great stuff.

Um, the stuff that's not so great are trying to identify within our- our workforce and frankly, uh, oftentimes within the context of folks, uh, working in the field, uh, people doing bad things to other people. And, unfortunately, we live in a- in a time and a society where people do sometimes do bad things to other people. So, we've really doubled down on our, uh, field worker protection initiatives. Um, we've tried to, um, using John and his team and our- our threat intelligence group, to identify those areas where our employees are at greatest risk and then really focus in on delivering to them the tools and the training that they need to keep themselves safe when they're working out in the communities.

Uh, we built also an insider threat program where, um, we're not just reliant on, uh, call centers and things for folks to identify people that they're encountering in their day-to-day work that make them

uncomfortable, um, are maybe engaging in behaviors of concern. Um, are potentially, uh, stealing proprietary data or misusing their access on their networks. Um, working from within against the interests of Dominion energy and our customers and our employees. So, we built a capacity for doing that. Um, we are not spying on our employees. It's an anonymized process.

So, only when risk indicators trigger, um, uh, a, an analyst to take a closer look at something, and when they do that, it's still anonymized. They're simply looking at the activities. And if it's in- innocuous, um, you know, sharing your- your, uh, uh, tax form with your Dominion Energy, uh, email account so that you can print something off here in a Dominimus use, uh, type of a- a thing to just, uh, sort of live your daily life, well, that might trigger because you're not supposed to do that, but it's- it's not going to end your- terminate your career at Dominion Energy, right?

And so- so we're sort of separating all of that sort of innocuous stuff from the stuff that does give us concern, which is exfiltration of proprietary data, um, taking, uh, um, intellectual property from either Dominion Energy or one of our key vendors, um, and sending that somewhere where it's not supposed to go. Um, that type of activity, we're- we're very keen on trying to identify that and manage it, um, to protect not just our company but its workforce.

Thank you for outlining those, Adam, and great segue into the last question, which is, how do these security standards, and Adam, you touched on this a little bit, protect our company and our customers? John, I'll start with you and Adam, kindly weigh in, as well.

Sure thing. Yeah, having effective security standards in place is, you know, critical to protecting our company, customers, and the grid overall. We don't want to wait for events to happen to address security vulnerabilities and threats. We're constantly out to find- ensuring we have the appropriate security measures at our many different sites. And as I previously mentioned, uh, conducting frequent security risk assessments is one way to ensure our standards match up with the current threat environment. Security standards aren't just developed and forgotten. We constantly review them and update them as needed. Uh, and lastly, we're fortunate to have a dedicated security team responsible for protecting, uh, just our substations. Uh, and as Adam mentioned, you know, much of our personnel has a strong background in law enforcement. This particular team is no exception, with all the members having extensive law enforcement experience and thus bringing the expertise we need to this very critical field.

Yeah, John- John hit the nail on the head there. I think the best way that we can, uh, meet our compliance obligations to the company, which we've always done. Dominion Energy has always been an excellent steward of, uh, of its customers and its shareholders, uh, and frankly, its employees by making certain that all of the things that our regulators tell us to do, we go in above and beyond to meet all of those, and in- in most cases, exceed all of those.

Um, the things that aren't in those compliance standards are exactly what John, uh, just mentioned. Is, having law enforcement background where folks have decades of experience separating out, um, things that aren't particularly concerning from a- a safety and security point of view to those things that could either escalate quickly or reveal, um, a larger problem, um, that- that may be lurking somewhere, that somebody without a trained eye would miss.

And so we've populated our ranks, uh, here with folks like John who have that sensibility and make us, uh, much- much more nimble in making the smart decisions, uh, about where to place our resources and protect in the most effective way our employees and our customers. And I couldn't be more proud of the work that they do and the examples are too many to even to into here of smart decisions made by people with deep experience that have mitigated a threat that, uh, would have either harmed one of our employees or one of our customers or escalated into a systemic problem that would have created,

um, even greater risk for our company. So, um, it's the- it's the tangibles and the intangibles combined that I think make us, as John cited, uh, an industry leader, uh, in security.

Nadia, thanks for- for doing this. I think, uh, any opportunity we have to, um, bring our workforce along to the things that we do, uh, hopefully make them, um, more comfortable in their day-to-day work that somebody does have their back and somebody is ensuring that while they're here, they're as safe as they possibly can be. And Dominion Energy has invested deeply, um, in that as part of the employee experience here with our company. And, uh, you know, we take that very, very seriously. And I think uh, um, we- we live up every day to that trust. And, uh, so thank you for doing it, and I think it's great, uh, that we can have that conversation.