Below is the text version of the November 7, 2022, Distributed Energy Resources Cybersecurity Report and Threat Briefing.

WHITNEY BELL: Hello, and welcome to the distributed energy resources cybersecurity report and threat briefing. I am here with ICF and will be your host today. First a few housekeeping items for today's webinar. This WebEx meeting is being recorded and may be used by the U.S. Department of Energy. If you do not wish to have your voice recorded, please do not speak during the call. If you do not wish to have your image recorded, please turn off your camera or participate by phone. If you speak in the call or use a video connection, you are assumed to consent to recording your voice or image. All participants are in listen only mode. If you have technical issues or questions, you may type them in the chat box and select send to host. We will not have enough time for questions and answers today, but you can submit questions using the chat function. If you need to view the live captioning, please refer to the link that will appear in the chat now. Finally, we will post a copy of today's presentation on the distributed energy resources cybersecurity report and threat briefing webpage by tomorrow, Tuesday. The recording of today's webinar will be available in about two weeks.

We are excited to kick off today's discussion with introductory remarks from Monica Neukomm, the acting principal deputy director of the office of cybersecurity, energy security, and emergency response. Welcome.

MONICA NEUKOMM: Thank you, Whitney, and thank you to everyone who's joined us today for our recent report on cyber security considerations and the current threat landscape for distributed energy resources, or D.E.R. I lead the Department of Energy's office of cybersecurity, energy security, and emergency response, or as we like to call ourselves, C.E.S.E.R. The mission is to enhance the security and resilience of the U.S. energy and for structure from all hazards, and that includes securing all energy resources from the many threats that they face such as national disasters, other physical threats, and cyber incidents. We are committed to improving the security and resiliency of the grid today and planning for the grid tomorrow. Part of the reasons we've worked with our colleagues in the office of energy efficiency and renewable energy is because our nation is experiencing rapid transformation on the electric grid with an increasing number of distributed energy resources. The clean energy grid of the future is evolving to address the impacts of climate change and society's energy needs. The way Americans produce and consume energy is shifting as we embrace a cleaner, more efficient, more sustainable future. As we make this transition, we do not have to choose between a clean or secure energy future. We can and really must achieve both to make the Energy sector resilient to anticipated threats. This transformational change presents a unique opportunity to design systems securely from the ground up, and to provide applied principles. We are really focused on ensuring that these new systems are resilient and secure from the start. D.E.R. systems use unique software and networks to integrate with the electric power operations, which makes them potentially vulnerable to cyber-attacks, which could pose a reliability challenge. Because we know D.E.R. are so diverse from electric storage, intelligent energy devices like smart lighting or thermostats, illiterate vehicles and charging equipment, and rooftop solar arrays, we know there are many aspects and solutions director together. Today there are about 90 gigawatts of D.E.R. installed nationally, half of which can be attributed to over 3 million rooftop solar systems. D.E.R. deployment is expected to quadruple in the next three years, with 380 gigawatts expected to be in line by 2025. We know we need to get started working now on deploying solutions. The finding of the new D.E.R. report opens the door for collaborative innovation to support a more secure future for D.E.R. devices and systems. Above and beyond making strategic recommendations to secure current and future systems, the report outlines D.O.E.'s intentions to find research on next-generation D.E.R. defenses, and as a jumping off point for conversation within the industry. For me this is one of the most exciting things about this report. I believe it can kickstart increased collaboration with key stakeholders like all of you to tackle the new challenges. We are so appreciative of the partnerships we have, and those we see between trade associations, labs, and others within industry who are working to help develop and deliver innovative solutions. And really deliver on tackling the potential D.E.R. cybersecurity problems. The connections being made now between and among key players in the distributed energy and renewable energy communities will foster technology, tools, and innovations that will benefit Americans for decades to come. These partnerships will be critical to making the grade of the future resilient and secure.

The D.E.R. report we are here to discuss today is full of insights and information that can help all of us as we strive to make meaningful security advances in a changing world. The report is an excellent resource that maps out recommendations, but as we all know, this is just the beginning step. As our nation's clean energy industry continues to innovate and develop new products for deployment on the grid of the future, we have the responsibility to ensure security is top of mind in every step of the process. In today's world and the world of tomorrow, which will be filled with technology capable of fulfilling a standing good or equally admonishing harm, it is imperative that we focus on ensuring cybersecurity is as fundamental as reliability and safety. This will require partnership with many stakeholders, including utilities, state and local governments, and vendors. The bipartisan infrastructure law called upon C.E.S.E.R. to develop a more in-depth analysis of D.E.R. assets, the threats they face, and how to best protect them. This work is already underway, and C.E.S.A.R. will be seeking input from key industry stakeholders as we develop a more conference of look at the threat and preparedness posture of D.E.R.

As you listen to today's briefing, I hope you will consider where your work intersects with the effort that lies ahead of us, where there may be opportunities for you to participate, and where we can build new partnerships. We look forward to your feedback and feature conversations. Thank you once again for joining us today.

WHITNEY BELL: Thank you, Monica. We now welcome Megan Egan, control systems cybersecurity analyst at Idaho national laboratory.

MEGAN EGAN: Hello, everyone. Thank you so much for having me, and for incorporating the briefing into this presentation. I think it makes for a great addition, although the report talks about really great examples of the threats that face D.E.R. , having some examples, which I will present to you today, I think really drives that point home.

With that being said, I would like to dive into this brief on cyber threats, specifically to renewable industry bootable energy technologies. Next slide. Here we have a timeline of just a smattering of the cyber incidents that renewable energy companies have faced, dating back to 2014 when there was a Chinese cyber espionage campaign targeting a solar company, solar world AG, running all the way up until the president back in August of 2022, with a ransomware attack. You will notice that a lot of these listed are ransomware attacks. That certainly makes up the bulk of what we hear about, partly because with ransomware, you know when you get hit by ransomware because that is the goal of the attack. However, that is not the same that there aren't a lot of other campaigns going on, and we do have examples of those as well, with a February 2020 campaign against Azerbaijani wind turbines, the February of 2022 attack against and archon wind turbines, and more recently the campaign looking at wind turbines in the South China seas. I just wanted to present to you, you know, sort of an overview of what is happening in the sector, but also show you that this is an ongoing and continuing problem. It's not just that we have the examples that I will talk to you about today, but these attacks are constantly coming in the renewable energy sector, and across the Energy sector more broadly.

With that I wanted to dive into first an overview of current adversary capabilities while targeting medical infrastructure, and then I will dive into a couple more of those examples in depth to talk about some lessons learned, and how we can take those lessons learned into the security of renewable energy at large, as well as D.E.R.s specifically. The current assessment of adversary capabilities is coming from the U.S. intelligence community's annual threat assessment. These assessments are being made by the U.S. intelligence community. So, they are not specific to renewables or the Energy sector, they do shine some light on how the major adversaries of the U.S. are working to improve their abilities to target critical infrastructure, of which the Energy sector is obviously a very big component.

First up we have Russia. The U.S. intelligence community assesses that they are particularly focused on improving their ability to target critical infrastructure including industrial control systems. ICS is a term that you will see a decent amount here, meaning control systems, whether that is communications, or remote monitoring, all of those types of things. Any computer system that is able to have control capabilities over assets in the field is really what we are looking at. So, Russia is particularly focused on being able to target those control systems, and thereby have an effect on the downstream assets of that system. Russia utilizes cyber as a foreign-policy lever, including as deterrence and as a military tactic. We have seen this play out with the conflict in Ukraine, whereby they will jointly use both kinetic and cyber effects in order to have a hybrid approach to their warfare. With that being said, deterrence as well. This may be a consideration for future conflicts in whether or not they want to push back on a country potentially considering action against Russia or that type of thing. The U.S. intelligence community assesses that they will use cyber in those instances as well.

Moving to the second-largest adversary that we have in this space come over you can put them on the same playing field, apologies, we will go back to talk about China really quick. So, U.S. intelligence Trinity assesses that China is almost certainly capable of launching cyber-attacks to dislodge critical infrastructure services. We have slightly less fidelity and what they are looking to target as far as China goes, because we have more examples coming out of Russia. But when you look at China, the U.S. intelligence community assesses they are almost certainly capable of this right? So, as far as intelligence analysis goes, really high level of fidelity there in China's capabilities in this space. In addition to seeking to disrupt critical info structure services, potentially including the Energy sector, they also are a broad and persistent espionage threat. As I mentioned in this first slide dating back to 2014, one of the areas that we saw the Chinese espionage threat targeting was renewable energy technology. That was as part of our economic development plans, and market penetration, and that type of thing. Next slide.

Next up, we have Iran. The U.S. intelligence Trinity assesses that Iran currently takes an opportunistic approach to cyber-attacks, and that can make critical infrastructure owners assessable susceptible to being targeted. This is a lowest hanging fruit type of deal. The Iranians in their cyber activity will target what they can, and so if your assets are online, if your control systems are exposed to the Internet, if it is relatively easy compared to other, you know, members of your same sector to target you and your environment and your assets, you know, that's the type of victim that Iran is looking for currently with their cyber-attacks targeting critical infrastructure. They have also been targeting Israel with cyber-attacks in recent years. Israel, by most assessments, is a superior cyber power to Iran , so their willingness to sort of punch up and to target someone who is arguably better in the cyber warfare space than they are does reflect that Iran is willing to take risks in this space, which does not bode as well for the U.S. , because we would be in the same sort of category of a more advanced cyber power, but that does not mean that Iran will listen to that or adhere to that deterrent, and they could intentionally be targeting us as well. Again, a more opportunistic approach than we see from Russia and China.

Lastly, we have criminal actors, who are, you know, probably the largest category on that first timeline that I showed you with all of those ransomware attacks. Criminal actors are innovating their targeting to focus on victims whose business operations lack resilience, or whose customers cannot sustain service disruption. Their goal from these cyber-attacks is to be paid. That is why the ransomware ecosystem is so robust, and continuing to grow, because the criminal actors are seeking a payout at the end of this. If you are unable to sustain a disruption to the systems that they have targeted and they have encrypted and they are holding for ransom, you are going to be a lot more likely to pay that ransom in order to speed up your recovery process, and therefore that is the exact victim they are looking to target with ransomware operations, or other criminal operations, whether it be a denial of service attack or those types of things. Criminal actors are certainly looking for those critical in the structure sectors and assess for owners and entities who cannot sustain service disruptions. That is who we have sort of looking to potentially target the renewable energy space, and their current capabilities cording to the U.S. intelligence community.

With that, I will dive into some specific incidents in the renewable energy sector, and we can take some lessons learned from those incidents. So, the first one I wanted to talk about occurred back in March of 2019. There was a Utah renewable competent power company called sPower. They intermittently lost communications with their solar and wind installations due to a denial-of-service attack. A denial-of-service attack is essentially when you can flood a network with communications that are not supposed to be there with communications that are supposed to be there, and that will limit the ability of that system to send for communications that actually need to occur, so you are essentially flooding out all of the legitimate communications with things that are not supposed to be there. During this specific incident, the unidentified attackers, as we have not attributed this to anyone, but the unidentified attackers were able to exploit a known vulnerability in a Cisco firewall. This is a relatively sort of benign thing, right? You have a vulnerability in a firewall. That may seem benign to your installations and your company network overall, but what this allowed the attackers to do was disable communications with a dozen different generations sites in five-minute deferrals intervals over several hours. Although they were not able to impact control systems, nor the power coming off of the assets, what it did impact was the ability of sPower to communicate with their installations. This is a theme that we will see in other examples we have as well. The vulnerabilities in these communications. One lesson we can take from the cyber-attack on 2012 is at publicly known vulnerabilities can be exploited within hours to days particularly if they are on assets that are exposed to the Internet, and this can happen either by unsophisticated or by state-sponsored actors.

There are a myriad of cyber adversaries and cyber threat actors are looking to exploit these known vulnerabilities, and often times with known vulnerabilities, you know, proof of concept exploits will be published. You know, it can take a couple of days for that to happen. Sometimes it happens even faster. We saw this particularly this past year with the log for J vulnerability, and the amount of time that it took cyber threat actors to hop on that vulnerability and start exploiting it. I mean, the time is getting faster with every large known vulnerability. These are very important to pay attention to, especially in cases like this where they can impact a company's ability to communicate with their renewable energy assets in the field. Next slide.

So, next up we have two ransomware attacks that happened pretty close to each other a couple of months ago. The first one was on March 31st, 2022 when the Nordex Group, which is a major wind turbine manufacturer was hit by Conti ransomware. The next one, a couple of weeks later – April 11, 2022, there is a German company called Deutsche Windtechnik and they provide maintenance for wind turbines, they were also hit by ransomware. We had a spate of these in 2021 and 2022 as you saw from the timeline on the first slide. Ultimately both companies lost their ability to connect to their wind turbine assets. Nordex Group, it was the wind turbines they manufacture, and Deutsche Windtechnik it was the turbines they maintain but they could no longer access them via remote connectivity in order to monitor the health and operation of the turbines. Similar to the last example, and this will be a trend, the assets remained operational and were not damaged in this case. They are still generating power, and they are still feeding power to the grid, but the companies are responsible for certain components of their operation or maintenance and that type of thing can no longer have visibility to those assets. So, the lesson that we can take away from these two ransomware attacks are that there is a widespread ecosystem of trusted partners. Nordex Group is a turbine manufacturer, yet they maintain connectivity to their assets. We have maintenance companies. We may have one, there may be multiple across one company's assets, but either way, there are a lot of companies involved in this space, so the widespread ecosystem of trusted partners can provide a cyber actor with many excess fat errors to the assets themselves commit to the renewable energy assets. Therefore, the entire network is as secure as its least secure partner. So, ensuring that the other companies that you are doing business with, and that have access to the assets, that they are adhering to the same level of security and all of that type of thing. They all need to be protected. All right. Next slide.

Okay, switching gears just a little bit because the last two were unidentified actors, and some ransom workers and that kind of thing, now we work and move into the more prevalent and capable cyber adversaries. From April to June of 2022, there was a China-based cyber threat group. The companies that wrote about this attack called this adversary TA423. Sometimes we get really good names for cyber threat groups, and sometimes they are more bland. In this case, we have TA423, which you probably won't remember, but the context is most important. We have a China-based cyber threat group who is targeting not only the vendor, as we saw in the last case with Nordex Group and not only the maintenance company, as we saw with Deutsche Windtechnik, but also the installer. They were targeting all of these companies for offshore wind turbines that are located in the South China Sea. These attacks began with phishing emails, something that gets harped on a lot in cybersecurity, and I know it makes an appearance in this report. Through these phishing emails, they were able to deliver a malware called ScanBox. If you are interested in learning more about this campaign and the malware itself, the proof point on this is really great. I'd encourage you to go check it out. What this really shows us is that these adversaries know that this is a widespread ecosystem. They note that there are a lot of companies involved in this, and again, this makes a highlight in the D.E.R. report that you will hear about in just a bit, but the entire supply chain of renewables was targeted in this campaign. This was a couple of months ago. Cyber threat actors understand the ecosystems that are involved and are willing to target all of the different companies involved. Not only do we have that in the supply-chain aspect of the renewable space, I also wanted to highlight that reconnaissance and espionage is a first step to various follow-up activities, whether it be until actual property theft as we saw with solar, apologies, the 2014 campaign, or learning more information about an operating environment to be able to deliver more targeted malware, or more sophisticated accessories and that type of thing, whether it is a short game or long game, reconnaissance and espionage as a first step. It's great to be aware of when that may be taking place in your environment, whether it is through initial access vectors like phishing emails or those types of things. Next slide.

Okay. This is the last example I have to give you, and I think there are really a lot of lessons we can learn from this one. In February of 2022, there were Enercon wind turbines across sent central Europe, really, that lost their remote monitoring connection. This was due to a Russian state-sponsored attack on satellite communications. Again, you'll hear this throughout, you know, the incidence that I gave you, but it impacted remote monitoring connections. Understanding the communications that exist to assets, understanding whether or not there are backup methods, whether or not they are resilient to various types of cyber-attacks, what companies play a role in those medications, all lessons that I hope you will take away from this briefing. Ultimately, this February 2022 attack required replacements of modems, the satellite communication modems and 5800 turbines, which is a huge lift. It took them about two months to get 95% of these turbines back online and communicating again. So, this is actually a spillover effect from a Russian attack on Ukrainian command and control during the invasion, the Russian invasion of Ukraine. The Russians conducted this attack to impact military communications, and it just happened impact these turbines as well. So even though they were not targeted, you know, assets in this space can unfortunately be sort of collateral damage from others might you know the either national or global events that are happening, and the communications are a huge part of that. Essentially what happened here is there was a misconfigured VPN at the satellite, the SATCOM provider itself. The attackers were able to access the SATCOM control infrastructure through that misconfigured VPN appliance, and they sent a wiper to all of these modems that just wipe them clean. They were still usable in the end, but it did require Enercon to go out to all of these 5800 turbines in order to fix this issue. A huge lift from the turbine company that wasn't even the target of this attack. One lesson that we can take away from this is that attacks at scale both in breadth and impact are possible. When we look at, you know, the other incidents in this presentation, you can say okay, well, if it only impacts, you know, one wind farm, or you know, one solar farm, that type of thing, that's one thing, but this is Enercon's entire network of wind turbines, and that is really what we need to be concerned about, which the report highlights as well, is the ability to impact, you know, the entire U.S. power grid, or significant swathes of it at scale through these attacks on renewables. This incident proves to us that that is possible. Another lesson to take away from this is that mass recovery efforts are difficult, but they are even more difficult when you have distributed and offshore assets. As offshore renewable energy gross, and has distributed renewable energy gross, trying to recover from these attacks at scale gets difficult, more costly, and more time-consuming. So, having a good understanding of what is required from recovery from an event like this and being able to plan for that is going to be, unfortunately, more critical moving forward. Next slide.

I just have some current and future security considerations for you, but a lot of these are highlighted in the report as well. The remote and distributed nature of renewable energy assets emphasizes requirements for secure and reliable communications. Again, you've heard me harp on this several times in the last several slides. Having this secure communications, ensuring they are resilient is important. Then just knowing who all has access to them. When maintenance is organized and directed from a remote-control center, and have a lot of trusted partners, whether they have direct access to your assets, whether they are using your data, understanding the security posture of all of the different companies.

Second, D.E.R.s for specific critical facilities can be targeted individually. In some cases, modest repeated renewables will power, you know, a specific other critical infrastructure sector, like a wastewater treatment facility, or, you know, military assets, or those types of things. You can target those distributed energy assets individually if that downstream facility is your ultimate target. Understanding the role that D.E.R.s play for the assets that they are powering, particularly when those facilities are of national security importance, or are another critical infrastructure sector is very important for understanding what may be most at risk.

The third thing, physical damage to renewables may be less concerning for human safety than in other industries. This is good news for the sector, because in a lot of cases, we do worry about potential physical damage from cyber-attacks, which sounds a little coming you, out there, but we unfortunately do have examples of it, and, you know, the proof of concept are out there as well. Fortunately, if we have a lot of, you know, wind turbines and solar facilities, you know, further away from population centers of the physical damage to them is hopefully less impactful to human safety. That being said, with distributed energy resources that, you know, are closer to customer sites, and, you know you are on people's homes and that type of thing, understanding the potential ramifications of physical damage from cyber-attacks is very important, so, that is just asset specific, and whether or not that is a concern, I think will absolutely depend on where it is installed, and the potential, you know, ramifications of the cyber-attack on that asset. Forcing, individually renewables pose little to no threat for the grid collectively, but, if you can attack them at scale, then you can have a far larger impact on something like the U.S. power grid. Furthermore, these networks are generally widespread, so again, as I highlighted with the Enercon attack, these attacks are possible. Second to last, efficiency is critical. I think anybody who operates these assets knows that, right? Extending the lifespan of these assets, making sure they are producing an excellent capability is very important, and what happens if a cyber actor is able to disrupt that efficiency. What are the business imprecations of the decrease in efficiency? Is it no longer a viable economic model?

Lastly, we have renewables and grid forming mode. This is something that D.O.E. has been exploring and publishing on, but as renewables take on more of the generation capabilities for the United States, as they are explored in new ways, like grid forming mode, the reliability of these assets is increasingly important, and therefore the security of these assets is increasingly important, and building that in from the beginning. So that is all I have. I have my sources on the next slide for anybody who's interested in reading more about any of the facts that I mentioned, but outside of that, I will turn it back to D.O.E. Thank you for having me.

WHITNEY BELL: Thank you so much. We really appreciate it. Now I'd like to welcome the cyber security office with C.E.S.E.R. , to discuss the distributed energy resources cyber security report.

GUOHUI YUAN: Thank you very much for joining us today. I'm excited to talk with my colleague from C.E.S.E.R. to go over the rest of the report, or the report itself, and thank you for setting it up perfectly for the discussion today. So, I am with the office of energy efficiency and renewable energy, and I'm going to go over, next slide please so for the rest of the briefing, is going to be three parts. I'm going to go over the first couple of slides to give an overview of the report itself, and then Mike will dive into talk about the approaches and detailed findings might if we have time, I will take it back into the context of other cybersecurity space. As Megan alluded to, there are many incidents of cyber-attacks on the renewables. This is not new, so, that is why we started looking at this space a couple of years ago. We were looking at a future scenario where the new technologies like wind and solar D.E.R.s that will be coming on the grid during this rapid energy transition, and we know that these new technologies are going to bring on new challenges for cybersecurity. We are glad to be able to publish this report in October and start this conversation. The main thing is to really raise awareness of cyber security for these new technologies so we can tackle them together. This is the beginning of the conversation. It's not meant to be having all of the solutions in the report, but hopefully it will help us to tackle these problems together.

So, why are we looking at this particular technology in D.E.R.? It's because D.E.R. is different from the traditional centralized generation, and there are a lot of new interactions, new interactions involved in the D.E.R.s that are not seen traditionally. Because the D.E.R. devices are also connected to the grid using communications, we need to understand them to be able to detect and mitigate the impact and be able to respond regularly. In the report, we said that today, D.E.R. may not present big challenges because of the number of D.E.R.s in the greatest a relatively small, and also they are confined, but in the last example from Megan, some of these larger attacks on a fleet of D.E.R.s can present a major impact and disruption to the grid. We need to understand that and develop solutions to address those.

This report is actually targeted at all of the people who are involved in D.E.R. technologies, including utilities, and what we call D.E.R. industry . The integrators and system operators as well as the vendors. I also want to point out that this is really a collaborative effort between the two offices in D.O.E., and the national labs, and the utility partners. We not only need the expertise in cybersecurity but also the expertise in these new technologies, as well as expertise in the systems. Next slide.

For this report, we actually have to define what D.E.R. is. It's not a single technology. It includes a diverse group of technologies, including solar, electric vehicles, home automation systems, so on and so forth. With different D.E.R.s, those smaller devices that are connected to the distribution grid are small, 10 megawatt, also considered in this report. As you can see, there are a lot of different technologies discussed in this report.

Some of the major findings here is first we want to raise the awareness and develop the requirements so that everybody is on the same page about what types of issues and challenges are going to be facing D.E.R. integration, and we want to design the cybersecurity into the technologies themselves. Secondly, we want people to know and understand that cybersecurity is not just technologies issues, but a process issue. We need them to be aware of these issues, and really take these cybersecurity challenges as a higher priority. Lastly, we want to go beyond the basic standard. We want to be able to incentivize the industry stakeholders to really raise their game and implement something that is more secure than the minimum requirements.

With that, I will hand it over to Mike, who will dive into the details of what we found in this report.

MICHAEL TOECKER: All right. I had some audio issues. Can you hear me okay?

GUOHUI YUAN: You sound great.

MICHAEL TOECKER: Perfect, thank you. To kind of underline what Guohui Yuan said, the D.O.E. approach on this was definitely a collaborative approach, with us and EERE. C.E.S.E.R. is responsible for vulnerability assessment and rapid risk mitigation for energy, including research and development on next-generation cyber technologies, and EERE is responsible for formulating and directing the programs designed to increase the production and utilization of renewable energy. We collaborated on this, and it brings an important set of viewpoints from just the right entities and just the right time. Next slide, please.

So, I am going to leave this up for a second. It is a lot to absorb for right now. I wanted to give kind of an overall assessment of where this report came from, is that it is an engineering informed assessment, but it is not itself an engineering report. It does not get into a lot of the nitty-gritty when it comes down to details. We can spend a significant amount of time on things like grid forming inverters or response to particular disruptions within the electric power grid that can be solved with various different D.E.R. type technologies. In an engineering informed approach, there are three primary things that engineers are concerned with, which is where are we right now and where are we going? What does the trendline look like? We are also interested in scale. How big is this problem currently, and where is it going to be going? And that is incredibly important when it comes to D.E.R. Then the last one is, who are the parties that we need to be bringing in in order to determine how to address this particular problem? Who are the parties responsible for the various technologies, approaches, discuss models? So, this brings in our traditional utilities, but it also brings in some new third parties as well.

Hopefully you've been taking in this particular diagram as I've been talking. This grid is evolving. Is going to be very, very different, even from today, as we move into the next decade or so of the main work associated with it. To our left we have basically the traditional energy system. It is kind of a one-way street where you have production on one end and consumption on the other, but the consumption on the other is changing, and is changing that only the way that we do things, but also in the scale of us taking this in. Many of us today already have smart thermostats, smart meters. We may have some energy storage or an electric vehicle in the garage. I've got one downstairs right now. There is a lot of capability there for those to be interconnected, and to be used in an energy system to do things that benefit us as a nation, as a community, as well as overall on a planet wide basis as well. All of these technologies are projected to be interconnected by some form of ubiquitous communication. This could be the Internet. This could be wireless. This could be some other form of communication that is more put together, on a more ad hoc basis, but coupling this with our aging infrastructure, the vulnerabilities of our emerging energy systems to disruption are not quite understood. Advances in energy and information technologies are changing the way that our energy is produced, delivered, and used. It's not just us. It's globally. Those third parties that we see up there are global, as are our adversaries. The power system configuration, the business models, and the operational strategies that we used to maintain the system are going to be vastly different than what we have seen before. On the left-hand side of the traditional transmission and distribution system, we can put hands on. To the previous set of slides related to the wind turbine issues, 5800 satellite modems, all right? A method of communication that connected all of these systems together, it took months to bring them all back online, hands-on type work. Can we go hands-on in every single home? Can we go hands-on in every single business? No. We need to be resilient to these types of events in the future. We need to be able to recover from these types of events in the future. We need to have plans for potential incidents as well, because the best laid plans get tested eventually. And then the vulnerabilities of these emerging systems are not yet well understood. The work that we've done in order to connect up all of these devices so far is going to project into the future. What does that look like? Have we appropriately addressed the vulnerabilities as we go? Have we been taking an adversary -type model when we are looking at these types of things to see, okay, what does a system like this look like to their mind as well? Next slide.

All right. I covered a little bit of this before, but it is, the electric grid is undergoing significant, rapid transformation, unprecedented in both its scope and scale. These improvements provide choice, the use of clean energy for combating climate change, these are often done on the meter as well, which is it in associated with Internet of things type technology, and that side of this is one of the major pieces that is going to be developed over the next several years. All of this has to be enclosed within an envelope of security. Work that we have done in order to ensure that things are safe, resilient, and reliable for our future use. Next slide, please.

As we move towards the future, we are moving as well within our D.E.R. type installation. So, very different from traditional generation. One that is highly configurable, but the other one is that currently the way that we work right now, currently the impact to the system related to D.E.R.s is relatively low, except in certain places. We do identify a couple of those places in the D.E.R. report as well. As we move in this infrastructure, we are moving from a nice to have, which is where we are right now in most areas, and we are moving to a needed capability to combat climate change and to offer consumers choice, and we will be moving from that to a critical resource on the grid. We will be using this to provide lights and charging infrastructure and other things. This is a good thing, but it is also a potential bad thing as well, because the output is software driven, digitally controlled, D.E.R. can react swiftly, in many cases swifter than existing resources, to provide important services at the time if there is a disruption or a blackout. There is action that can be taken on the D.E.R. side with appropriate planning that allow us to maintain service, and to provide, for instance, local micrograms or hospital based local micrograms or things that would assist in certain energy disasters, which is another reason C.E.S.E.R. comes into play. That benefit also comes with a responsibility to prevent uses that could degrade the service and capabilities of these resources as well.

This is where I go back to a part of my engineering discussion. Who is responsible at that point to ensure that we are preventing this types of uses? Next slide, please. When we get into roles and responsibilities here. By that I mean the roles and responsibilities of the various entities that are currently associated with the power grid, as well as what we think the future is going to look like as well. Before using this. New players are going to be entering the electric power sector, aggregators, the cigar out and say, all right, consumers, I want to see, I'm going to provide, or I'm going to get you a service that basically says hi, I can divide you benefits, all right, the air for instance a smart thermostat. You will be able to better control your use of energy and track your use of energy. You will be able to identify energy efficiency improvements that will save you money in the long term. In exchange for that particular capability, they are going to be able to access your thermostat and will be able to turn it up, turn it down, potentially turn it off in various situations as well, and there are many devices that are capable of doing this. Vehicles are one. Battery storage at the home is another. Solar installations at the home is another. Not to mention all of the other myriad of things that can happen over in commercial buildings or industrial settings. These D.E.R. services that are marketed divide considerable choice, and selection, use, and timing of electricity. There should also be a responsibility on that side from D.E.R. aggregators, owners, and the vendors of the devices as well, and to ensure that they are building products that are resilient, and that also are supporting the overall electric power grid itself, the reliability of that piece itself.

So, this coordination and cooperation between the traditional utility role, all right, those who are responsible for the wide area, but the electric system and the utility you pay your bill to every month, and the forecasted D.E.R. role, the aggregator, vendor, and owner, that cooperation is vital for taking advantage of the positive developments of D.E.R., as well as preventing the negative impacts, potential negative impacts of D.E.R. from a cyber standpoint as well. Next slide, please.

All right. Again, coming back from the trending standpoint is an engineer, where are we now? The past 20 years, we have seen the threat from malicious cyber attackers increase. There has only been year-over-year increases with a couple of minor jobs over certain years. These attackers are focused on a lot of different motives. One of the ones we have seen most recently is ransomware. They are powered by new incentives, most notably the digital ransomware type component. These cybersecurity challenges are not expected to abate. In fact, as we build new systems, and has rebuilding capability, and as we increase our technological sophistication, attackers come along for the ride. They are looking for ways to exploit, take advantage of infrastructure that allows them to exercise their own, quote, is this model at that point. Where they are going and understand what the threat looks like now is where we think where the threat will be in the next five years or 10 years is incredibly important for D.E.R., because we are using new technologies, new capabilities, we are leveraging cloud infrastructure in ways that we have not traditionally done before. The leveraging of those capabilities and the scale by which we work with them now, it's going to look very different than anything traditional that we've done before. I used to work in power generation, and if we ever had an issue in the power plant, we could go hands-on with that equipment pretty quickly, but I can't go hands-on 500,000 devices in order to fix things. That infrastructure, that ability to be able to go in and do repair work has to be there tomorrow in order for us to use it, you know, if we ever need it again. Next slide, please.

All right. And I stole my own thunder of course. The sheer scale of D.E.R. deployment, the wide range of communications options, and the level of access needed by various stakeholders needs a zero-trust model, and it needs one specific to D.E.R. based systems. We have to look at this from that only how we have worked in the past with traditional utilities, but we also need to be working with the stakeholders have been building these systems now for easily five years, sometimes longer than 10 years, and they've been slowly pulling together capability, and understanding of how things work, their own protocols, their own services, and we need to be working with them on a model that implements zero trust, all right, were we can say, okay, we are rejecting the things that we do not want. We are continuously verifying that these are things that we want, and we are taking proactive action to remove things from this system that don't meet this model. There is an opportunity here. We have an opportunity here through funding, through the unique relationship within C.E.S.E.R. and EERE to put this capability into the systems that the earliest stages of development rather than at a later stage when we are already seeing impacts. Next slide, please.

The future work, C.E.S.E.R. has been engaged as part of congressional request to develop a report on enhancing the physical security and cyber security of electric distribution systems. D.E.R. is going to be a part of that. This is scheduled to be completed by May of 2023. We already conducted the first workshop on October 5th and 6th. We have the powerhouse of the D.O.E. complex collecting information and suggesting a draft for this as well as working with our stakeholders in power, and that includes both traditional utilities as well as his emerging D.E.R. industry, which is a term we coined for this report in order to describe this new set of rules and responsibilities that are coming out.

Additionally, this is being done at the clean energy cyber security accelerator. The intention here is to enhance information and defend these new systems. We haven't really worked with these as much in the past. They differ from anything that we've done before and energy, and they are going to continue that way, and the intention is to prepare those for the high priority cyber security risks for when these systems are needed, when I was telling you about the trend as far as reliability and security goes, we are preparing them for those risks, the risks that we see in the future today, and then cyber testing for resilient and industrial control systems, or the CyTRICS programs. This is an OT program that looks at devices within the energy sector and tests them for vulnerabilities, both common and unknown at this time, and there are six national labs who are currently engaged on testing this equipment, and our intention is to use that capability as well for D.E.R. Next slide, I believe it to turn it back over.

GUOHUI YUAN: Thank you. In the next few slides, I'm going to go over some of the other activities that we are doing in the solar office. I just want to double down with what Mike said, there is an opportunity for us to work together to address the cybersecurity challenges. I would say that we must, we must work on, because D.E.R. and renewable energies are an integral part of energy transition. If we want to achieve our goals for the power sector, we will have a lot of D.E.R.s and renewables, and we definitely need to address the cybersecurity challenges.

In the next few slides , next slide please, I want to see what else we are doing to address these challenges beyond just the report. We know that D.E.R.s behave differently from the traditional energy resources. We developed this program called S2G, securing solar for the grid to really take a comprehensive look at the different gaps, in this case a solar cyber security challenge, a solar cybersecurity challenges. The goal is to ensure the cybersecurity of the grid with a high concentration of PV and other D.E.R.s. We are taking a collaborative approach. We know this is not just a cybersecurity issue, but it is also a power system issue, so we are working with multiple national labs. We are identifying the gaps, requirements, standards, best practices, and standard analysis. We are hoping to have the outcome of drafting requirements, standards, best practices, and testing protocols, actually something that Mike just alluded to, the CyTRICS program . We are already working with them to add, you know, solar passing and verification into those programs. So here is a detailed look at the S2G program. We are working with four national labs. We regularly meet and discuss the industry trends and facilitate non-consensus discussion and talk about the project priorities. We engage with the industry. We have an advisory board to inform all of these research topics. We also have a regularly scheduled webinar to disseminate and seek feedback on a continuous basis, because this field is changing rapidly. We want to get the results back to the industry and seek feedback from the industry in order to make it more timely and relevant. Next slide, please.

So here are the main thrust of the research areas. We are looking at cybersecurity knowledge and tools at three levels, the device level. What that means is basically PV inverters. At the plant level, which you imagine there are a lot of different inverters aggregated together to form a plant, which connects to the power grid, and then at the system level. This is really about how the systems interact with the grid and vice versa. We want to look at and understand the interactions between the devices, the plants, and the systems at different time scales, and understand the dynamics, and also understand how it impacts the grid. What kind of disruption is going to have? Is it going to be limited, or propagating widespread? These are the tools we are actively developing, and we are, you know, most of these tools are open-source, so we will wire these to the industries to play with and seek feedback on whether or not these are useful and relevant to address some of the challenges. We are very big on the standard development. We are big on education and workforce development, and supply chain management. Next slide.

So, this is my last slide, I think. This is really a further thrust into stakeholder engagement. We know that a lot of the decision-makers, so for example the state energy offices, and the regulators, they need to understand the pros and cons of the different approaches, and they need to choose, because in addition, we will develop the rules for cybersecurity, so we definitely want them to have the correct information and tools to make those decisions, so this is a project that we are finding in collaboration and working in collaboration with NASEO/NARUC to develop these educational training tools for this project team. As you can see the states are very involved in this project, but the goal is not just only working with these states. They have an ambition to really use it as a platform to engage with all 50 states in the U.S. about cyber security issues. We are really excited about this. Next slide. I think that is all for me. Thank you.

WHITNEY BELL: Thank you so much. That wraps up today's briefing. Thank you all for your time today. A copy of today's slides will be available on the distributed energy resources cybersecurity report and threat briefing webpage by tomorrow, and the recording will be available on that same page in about two weeks. Thank you for joining us today and thank you for participating. Take care, and we will see you next time.