CRITICAL INFRASTRUCTURE CYBER SPRINTS – WHAT'S NEXT?

VIDEO TRANSCRIPT

Jim Guinn:
I am phoning in from Israel out of our Tel Aviv office right now. So hopefully we will get a good connection, and we don't have any problems. And if not, we've got a handoff script that we're going to do. So, we have four really unique panelists, but all very similar in backgrounds because both have either worked in the defense industrial space or with the U.S. government or in the private sector. And each one of them brings some unique sets of experiences and thoughts to the table.
As everyone knows, under the Biden administration, they started the hundred-day sprints not too terribly long ago. They were really meant to be prototypes or to try to evolve cyber resilience in between U.S. government and industry and private sector, communication and best standards and best protocols for being able to increase our cyber resilience. And so, off the back of what's happened with Russia invading Ukraine and the increase in cyber activity that we feel and we can see, whether it is ideological actors that are taking a stance with one of the interested parties in the Russia/Ukraine situation or it's nation states that are going to be testing the waters to see how things go. We are seeing increases in these sorts of scanning activities, and so is the U.S. government.
They've had a number of different classified and non-classified briefings sharing that information. So, we asked Eric Goldstein and Puesh Kumar to join us, each one respectively from different areas. Eric is the executive assistant director for cybersecurity within CISA inside of DHS. So really appreciate you participating with us. And he also came from Goldman Sachs prior to that. So, he has got both sides of the house.
We have Puesh Kumar, who is the director of the office of cybersecurity, energy security, and emergency response within the Department of Energy, DOE. We're really excited to have him because he was actually formerly one of our clients at SoCal Edison, Southern California Edison, one of the largest utilities in North America that is definitely part of critical infrastructure. And we also have Adam Lee. Now, Adam flipped to the other side. So, he started his career with the FBI. A distinguished career where he ended as, I guess, the officer in charge of the Richmond field office and division. And now, since 2018, he's been the CSO for Dominion Energy, which, if you don't know what it covers, supplies a lot of critical energy and electricity to U.S. government entities in the D.C./Virginia area.
And then, last but not least, Rich Mahler. Rich was formerly the CEO of Revolutionary Security. And I don't know how I did it, but I convinced him that he should sell his business to us and join the team. Now he leads our global utilities business across all the different markets and market units, which has been a spectacular acquisition for us because we got some really, really smart folks and some great talent with unique experience. Rich, when he was with Lockheed Martin and with [inaudible 00:03:10], he did a lot of work in the defense industrial

base.
So, everybody's got kind of both sides of the coin here. I think that this will be a pretty interesting conversation and hopefully something that everyone on the call that's participating can get something out of. I'll also challenge you; if you have some questions, please put them in the chat. If we don't get to them, we will do our best to respond back to each one with the appropriate party, depending upon timing and sequence. But we will do our absolute best to get some questions towards the end of this discussion.
So, with that said, I'm going to do a little bit of a round-robin with different folks because we have talked about some of these topics, and they're very timely, given the prices that we're seeing unfold in Eastern Europe. So first, we're going to pivot back to the hundred-day sprints, and this one's for you, Eric, because you've been heavily involved in this. So, understanding that the sprints were somewhat of a prototype, what's next? What are we going to do to really harden critical infrastructure now that those have started and evolved and what's really going to happen next?

Eric Goldstein:
Yeah. Thanks, Jim. So first of all, great to be here with this amazing panel. Chatted with you in the broader group, so really looking forward to the conversation for the next hour or so. Taking a step back, why are we sprinting in the first place? The goal behind these sprints, which were started by the administration last year with a sprint focused on the energy sector with our colleagues, of course at DOE, and then subsequent sprints on the oil and natural gas sector, and now the water sector. The goal here really is to catalyze partnership between government and the private sector in a way that we can bring together and drive some focused action over a defined period. Also, what I'll say sprint into a marathon, recognizing that we are not going to fully address all of the cybersecurity considerations as a community that we need to achieve in a hundred days.
And so, the goal of the sprints was, in the first instance, to really bring together organizations to make material progress in advancing adoption of cybersecurity detection technologies. Driving real focus on some of those basic cybersecurity controls, for example, that we at CISA are codifying on our cisa.gov/shieldsup website. But then also bringing together partners to say at the end of the 100 days, let's keep our work going together. And so, at CISA, we're doing a lot of that collaborative work through our joint cyber defense collaborative, working closely with our colleagues at DOE through their ETAC, which I'm sure Puesh will talk about as well. But the goal here is really [to] use the sprint as a jumping-off point to make some material, quantifiable progress and then drive that into deeper and further collaboration going forward.
I think this whole effort should be seen under the umbrella of we know that our critical infrastructure remains an area of focus for our adversaries. We know that many organizations across sectors are making critical investments in security controls and processes, but every organization likely has gaps in their environment that could use some improvement and focus. So, by working across sectors and also organizations, public and private, big and small, we can work together to understand those gaps and collectively work together to make the investments that we need to draw down risk over time.

Jim Guinn:
Great explanation because it now will let us pivot to the here and now in the present, right? So, it talks about why and what the intent was and how to make it evergreen and continue to advance the cyber agenda. And we can't forget what's happening, like I said, in Eastern Europe right now with our colleagues and friends and people that we all know and work within various aspects of our daily lives. Given Russia's invasion in the Ukraine and related cyber threats, what advances, and this is really going to be for Puesh, yourself, and Eric both, because we get to see a lot of it when we participate in things. I know that some of our competitors and clients get to see a lot of it, but given what was intended with the cyber sprints and now what we're seeing with a heightened sense of cyber

challenges, given the situation in Eastern Europe, what do we really see in government and critical infrastructure collaboration trying to thwart these threats right now? Are we seeing some positive outcomes? So Puesh, I'll give it to you first.

Puesh Kumar:
Sure. And thanks also from my end for having us here for this important conversation. Certainly, in light of everything that's going on in Ukraine and Russia's invasion of Ukraine, but also, just because we are really focused on this space, OT cybersecurity is a priority for us at DOE. It's really a priority even bigger than that. Back in July of 2021, the president issued a national security memorandum really focused on cybersecurity of our critical infrastructure and specifically control systems. So, you're seeing a lot of attention, and you're seeing the close partnership across the inter-agency with our colleagues--Eric at CISA, with the FBI, with the intelligence community. Everyone's coming together to release a... we don't just need collaboration. We really need extreme collaboration between both industry and government to address the significant cyber threats that we're seeing to critical infrastructure across the board.
So, from the DOE end, we're continuing to be engaged very, very closely with owners and operators in the energy sector across electricity, oil, and natural gas. And we're leveraging those partnerships to not only share intelligence, but really, we're actually going beyond just sharing of intelligence, but we're getting to that place of understanding risk. So, what is the risk that we're seeing to the energy sector, and how do we mitigate the risk jointly? What's the government's role? What's the industry's role? How do we all actually work together to do this? And so, one of the areas that we focused on through the hundred-day sprint that you mentioned--I think we might be on day 300 something or another for the electricity sprint at this point--we've kind of moved into that phase where we did the sprint and now what we need to be focusing on is how do we really continue to drive cybersecurity in the industrial control systems environment? And so, to do that, we've really focused on four big lines of effort.
The first one is we really want to continue adoption of sensor technologies, of monetary technologies in the OT environment. And so, continuing to work with the sector to do that. We've already had 150 electric utilities commit to deploying some of that sensor technology so that we can get shared visibility across industry and then with government to really see what kind of threats we're seeing out in the sector. We're looking at financial incentives that we really need to address to get those sensors and technologies out there.
And then the second thing that we're doing is this joint collaboration of threat and intelligence. So, we're partnering with Eric's group on the JCDC and really thinking about the JCDC as this cross-sector, national collaboration across the 16 critical infrastructure sectors. But within energy, how are we [inaudible 00:10:38] after that? I'm certainly biased, having spent my entire career in energy, but it's a critical sector that every other sector is dependent on. So, we really need to be putting a lot of effort into this in terms of that joint collaboration. And so, we're piloting an effort that we're calling the Energy Threat Analysis Center or the ETAC. We're really piloting just getting industry and government together. Look at threat intelligence, talk about risks, talk about vulnerabilities, and how do we actually disseminate that information quickly in a timely and actionable manner out to the broader sector across the board.
The third big activity we're really focused on is developing a common lexicon for data sharing and a platform for analysis. So how do we really take these different data streams, whether it's different sensors that are deployed out there or whether it's data from more of a power systems modeling perspective and marry it up with some of the cyber data to actually understand what's happening on the grid, on the oil and natural gas sector. How do we actually correlate this and use the analytical capabilities of the national laboratories and the private sector to come together to do this?
And then the last line of effort is let's continue supporting some of the smaller utilities out there,

the munis, the co-ops. How do we ensure that they have the resources and the technical support to also really advance cybersecurity for some of those companies that are smaller. That may not have the resources. So really, it's across the board. Those are the big four activities that we've been focused on in partnership with CISA and the rest of the inter-agency.

Jim Guinn:
That's great and awesome. The last one. The one that you just brought up about the municipal utility districts and the smaller municipal organizations. They definitely do not have the funding to be able to afford sensor technology or monitor it or see it or even hire the skilled talent to be able to look at it. And we see that with critical infrastructure, especially in water, water, and waste. It's one of the toughest ones just because of scale and size, but it's extremely critical. On the flip side, we also have large organizations like Dominion Energy who have budget and can invest in these things and do provide critical infrastructure to U.S. government entities, and that's extremely important. Adam, from your perspective, how has this improved? Have you seen improvement, and what do you really think that collectively we can do better together?

Adam Lee:
Yeah. Again, I don't want to be repetitive, but thank you for having me. This is a great conversation. Puesh and Eric really covered a lot of the ground that I think sort of exhibits that things have improved since I've been in government. I think that touch, you're seeing it with CISA. I think from a large energy utility like Dominion Energy, we have real-time information sharing ongoing with DHS through their cyber century program. We have monitoring, vendor-supplied monitoring. We have telemetry into our own SOC from our OT environments. I think the toughest thing or the biggest challenge I think in that interaction between utilities and government is scaling it appropriately and speaking the right language to a major utility with a hundred billion dollars in assets spread across many states to those water districts because that's an entirely different language you're speaking. Yet, you're trying to divide solutions that can mitigate threats that span across all of those industries, and the threats don't scale. Our responses need to scale.
So that's, I think, the biggest challenge. Choosing ETAC as a nascent sort of idea as a collaboration, I think, is fantastic. Dominion Energy not only being a large critical infrastructure player but also being the supplier, the upstream target for key national assets. I think for us; we have a unique relationship with the intelligence community and with government. But I think again, that challenge is where we are already invested heavily figuring out how to engage with Dominion to learn and expand. To engage with Dominion, to learn and expand the understanding of who's hitting our outer perimeter, what's all that noise, where's it coming from, to assess the threats. And then cascade down solutions to those smaller utilities that aren't as invested. That's what I see as maybe a way forward for some of those very encouraging initiatives.
Jim Guinn:
I like that you bring that up because there are a lot of different size organizations in a diverse set of industries. They may not be front line like Dominion or Center Point or Duke Energy, or any of the large integrated utilities or power generation companies.
As Peter said, there's a lot of smaller-scale things that you have to pay attention to. But they can be like a third party. Meaning they supply something that's critical to someone else or they have something that is part of the supply chain that is critical, but they're smaller.
So, Eric, as I think about this from CISA's perspective within DHS, how are you going to pull together these different and disparate smaller organizations and companies and industries to have some consistency with information sharing? Because what we say all the time is if you can't see it, you can't protect it. And if you don't know it happened, then you can't go fix it. So, these smaller organizations might be the front line because we see these vectored attacks that come in from third parties

that are directed at someone else. So how do you see that unfolding from CISA's perspective with these diverse sets of industries?

Eric Goldstein:
Thanks, Jim. It's a great question, and I'll build on the good points from both Adam and Puesh. There's a few ways we can think about it. The first way is by really strongly encouraging organizations to continue to invest in understanding their supply chain and driving the right requirements down the supply chain. Particularly to those critical nodes and assets that maintain trust relationships with the organization or that maintains some critical function that, if degraded, would cause downstream impacts.
And so, as an example, as of the president's cybersecurity executive order last year, one area that we invested in as part of the U.S. Government Enterprise is working on updated contract clauses. For example, that can help organizations ensure that they're managing their supply chain, both from a security standpoint, but then also codifying those requirements in a contract and then modeling those across sectors. That can be a really valuable tool to ensure that an organization understands the breadth of risk that they're taking on across their supply chain and then driving that down in any way possible, prioritizing those vendors and suppliers that pose the most risk to the enterprise. Again, either through trust relationships or because of the critical function that they provide.
Now separately at CISA, we are also really invested in increasing the breadth and depth of incident reporting across the country. Of course, we were really gratified to see Congress pass legislation requiring CISA to promulgate a rule for organizations to report incidents to CISA. We are right now really encouraging all organizations to report not just cybersecurity incidents but even anomalous activity that might be indicative of an intrusion because that lets us then understand trends, connect dots, provide help, and identify the leading indicators of intrusion campaigns to contain them and drive remediation. And that is equally true for a large multinational corporation as well as for a small or medium business. Every organization should be reporting incidents to the government because that's the only way. Jim, to your really good point that we're going to be able to paint a tapestry of intrusions and threat activity across the country, connect dots between seemingly disparate acts and then figure out what our adversaries are doing, and take actions in our national defense. At CISA, we're also really focused on dot-connecting with our international partners. And this is just a point that bears noting in the context of the Russian invasion of Ukraine because we are really focused on understanding the evolving threat environment on the ground in Ukraine and in Eastern Europe. Pulling information back from our cyber defense partners in those countries and then using that to further connect dots with activity that may be happening here in the future so that we can be on top of the leading edge of intrusions here. And again, take action to protect U.S. companies.

Jim Guinn:
I'm glad you brought that up because you do in U.S. government five eyes, there's a lot of information collaboration between the intel agencies when something does happen and that'll only help increase the fabric or the tapestry that everybody can see more broadly. One of the challenges that we see that continues to be a problem, and it will never not go away. A kinetic bullet has energy and it will fall at some point because it runs out of energy. A cyber bullet never dies. It just gets repurposed and reused and other threat actors pick it up and dust it off and try to do it again and again and again and modify it. So that's the challenge, they just literally never go away.
But Rich, pull your thought into this for a second because you've had a very broad career with Lockheed, being the CEO of Rev Sec, now with Accenture. And you've seen a ton of clients both in defense industrial base and private sector. What should the industry be doing to be able to help this communication, interoperability, systems, technology, foundations, standards? What should the industry be heavily participating in to try to help drive the cyber agenda forward?

Rich Mahler:
Yeah, thanks Jim. I'm going to go back to my original system of systems engineering concepts. In order to make any of these hard problems work, there's dozens of systems that are all designed independently that have to interoperate into one big mission. So that's kind of the landscape I see things through.
So, the first part we have to do is get together and define which problem we're trying to solve for and what the boundaries are, right? Because everybody's got a different ... "Well, we want to get this part of it, we want to get that. End this part. So, let's lock in on, let's start with which level of sharing we want to tackle first, what the context of that is, what the boundaries are, and what the interfaces are, but not try to do everything or we'll never get anything done." That's the first part.
Along that same line is as you're going to move into an industry standard, a development process, you want to make sure you have enough diversity of thought to get a really good product. But again, not so much that you never get anything done. So that's where you have to bound those things with, "Okay, are we doing a first version and then we're going to build from there? We got to get to a minimum viable product? Or are we really trying to get the right answer?"
Our team's been fortunate to work with some of our utility partners and we've done a first pass on a data taxonomy R&D project for machine-to-machine threat and intel sharing for the electric grid side. So, can a utility selectively share what it wants to with its peers, with its government partners, potentially with its equipment manufacturers, and also be able to ingest that intelligence coming back in a way that really speeds up that cycle? And again, that's just one piece of a problem that needs to be solved. There's a lot more. We need a lot more thought on this.
And then we're going to have to get that context about the grid in there as well. It's not just that there's a vulnerability on a machine. Well, okay, does that matter to me or not? Where is that? How far in is it? What protections will I have in place? All those things that come into play in determining how critical this action really is. And then we have to make sure that it truly is an open standard, that everybody can participate in it regardless of what platforms they're using, regardless of, again, are they a large investor and utility or are they a small municipal or a co-op? Everybody's going to participate at different levels, but we want to make sure everybody can participate at the right level.
And then once we have that worked out, right, now the fun begins. You go into something that becomes operational, needs that care and feeding, needs a constant evolution. And then, a lot of times, we have to look at a lot of the value does come from classified sources. And people can only participate that at different levels based on their resourcing and clearances and all those other things. So, there are some organizations that really can take advantage of that context that comes from having those classified discussions. There's some people that if you gave them all that, they wouldn't know what to do with it anyway, right? They're small, they're understaffed, and so what they really need is just the tactical action of, "What should I look for and what should I do for my system?" So, we've got to structure it in a way that can benefit all of those parties and meet them along their scale and their maturity curve.

Jim Guinn:
So that's a journey. I mean, that's not just a small thing. That's a large thing with a lot of complexities.
To that point, and one of the questions that already came in, I want to flip a little bit and talk about ETAC and JCDC for just a moment. So, one of the questions that already came in, and I'm going to merge some things together here, so just bear with us. I'll ask Puesh if you can comment on this to start with.
There's a lot of interest from various organizations, part industry and then technology providers to participate in ETAC. Rich just talked about ... I mean Rich, you hosted a panel of different investors, investment community, talking about a whole host of various technologies by names, the Nozomis of the world, the Dragos of the world, the ... I mean

Microsoft and ... I mean there's a-

Rich Mahler:
Tenable and Forescout. Yeah.

Jim Guinn:
Yeah, there's a ton. There's a lot of them. And it gets very complex very quickly. But Puesh, if someone wanted to participate, let's talk about client side or industry side first. If someone wanted to really participate in ETAC and try to help nudge along or co-create the standards. I think one of the most impactful things that I've seen U.S. government do in the industry segments for cybersecurity was under executive order 16636 under Obama for PPD-21, where they said, "NIST, you've got to go create a bunch of standards and everybody can measure themselves against the standards." That was the first time ever that we had a common set, a baseline. We had a foundation. Literally something we can build off of. And so now with ETAC and what's happening with JCDC, we get a lot of questions. And like I said, one of them that already came in is, how do industry providers, how can they participate in both of those initiatives? And I'll flip to the second question in just a second.

Puesh Kumar:
Sure. And that's a great question. So let me take a step back before I answer the specific ETAC question because you all were hitting on a really important point. For a very long time, the focus of the energy sector was working with the utilities. The electric utilities, the oil and electric gas companies. And the reality is when we think of the energy sector, it's a much more complex environment. It's vendors, it's manufacturers, it is various cyber technologies. And so there was a term that we introduced in a report that DOE just published in February called the Energy Sector Industrial Base. So, what is the larger energy sector and who is connected to it? What are the different pieces of it? And so, when we think of the ETAC pilot efforts that we're trying to do with our colleagues at CISA, with the JCDC, we are really thinking about how do the manufacturers commit to [inaudible 00:26:37] to this.

It's not just the great work that we need to be doing with the cyber technologies, the Nozomis, the Tenables, the Forescouts, the Dragos, and the other great companies that are out there. And they're a really important community. But what about the Hitachi's of the world, the Schneiders and Schweitzers of the world?
And so, we're really thinking about this really broadly in terms of where do they plug into the threatened information sharing intelligence mitigation measures. I will tell you that in some cases, when we find vulnerabilities with a manufacturer of large industrial control systems equipment, the manufacturer probably is best to fix the vulnerability. They know their systems intimately. And so, we need to partner with them as well. And you're seeing a focus from us here at the department, and I know out by CISA as well to work with the manufacturing community in terms of bringing them into the fold as they think about this.
But more specifically, in terms of the ETAC conversations. Right now, we're starting to still stand this up and say, "What does this look like?" We're going to be putting out information where we would like feedback. That's one thing DOE has done well for so long, and we intend for more of this to get feedback from a broader community to say, "How do we think of OT security going forward?" And so, you're going to be seeing more of that coming out from the department and asking for input on what does a taxonomy look like going forward?
Because again, we don't think we should be developing it just ourselves. We should be getting a lot of different types of input to help us think through what an OT data taxonomy is. The work that Rich mentioned is something that should really plug into it. If you've already done some really great work, let's do that. And you know what, from Dominion's end, I expect you all have thought about this as well as you have all these different systems. So, we want that input, and we're going to be asking for it going into the future as we start to flush out some of these concepts.

Jim Guinn:
You brought up a point about energy. I tried to

write it down as quickly as you said it.

Puesh Kumar:
The energy sector. Energy sector industrial base.

Jim Guinn:
Perfect. Energy sector industrial base. The other thing, I've spent the vast majority of my career working in critical infrastructure. If you think about the wellhead or where it's coming from when that pipeline shuts down, think about storage capacity. Thank goodness there was good storage capacity in the particular refineries that were feeding Colonial because had they not had storage capacity, you'd have had to shut things in. And that's going to be a real problem. And we were talking about, there were some different sessions today, both on incident response where we've had to help industrial-based clients, heavy industrial asset intensive clients, and they've had to shut things down out of an abundance of caution when they saw that things occurred in those environments and in those networks. They don't come back up very easily. They're meant to run and not stop and start.
So, when you think about that, it's not just the cybersecurity aspect. It's also the business and economic, and even environmental impact that can occur in some of these critical infrastructure entities.
That can occur in some of these critical infrastructure entities. So, Adam, I'm going to ask you this. Do you see where standards for critical infrastructure, can you see this coming together in support of ETAC and what they're trying to do? Because he talked about the Siemens', the ABB's, the Schweitzer's, the Yokogawa's, as well as all of the anomaly detection systems and commercial products. How do you see standards and environments coming together to help support this in ETAC?

Adam Lee:
Yeah, you do sort of clinch a little bit with a notion of standards because for a company like Dominion to standards resolve to compliance standards, which becomes for us largely an administrative exercise to document the things that we were probably already doing. I don't think that's the spirit behind ETAC, from what I've heard. I love the idea of the large critical suppliers like Dominion sort of participating in collaboration with the government agencies. I think one of the things that I think I'm seeing. Eric and I shared dinner the other night with some folks and talked through this. We are at a time where the threats to Dominion Energy, the things that keep me up at night are nation-state attacks. I think 99.9% of the noise on the outer perimeter of our network does not keep me up at night.
And so, the government needs to consider this stuff as asymmetric warfare and provide leadership. And I think that's the kind of thing that Bush is talking about with ETAC is to consider this stuff as protecting the United States and where can government, as opposed to just sorting through the best vendors and maybe giving, picking winners and losers of who has the best tool on a certain flashpoint of time. I think we really... I really do want to credit DHS on the Cyber Century Program because that solved for us a problem; we don't want a profit-motivated company delivering to us our critical intelligence, especially at the TSSCI level. We want that from government. We want a relationship where they're sharing to protect in the moment of an attack or asymmetric warfare threat. We want that direct connectivity with government. We don't want to be dependent on the promises of a vendor selling us a product. We want government's leadership in that area. And I think what you're seeing here, and I think this conversation evidences the fact that that's the mindset [being] creating with the post-Colonial world and where we're going with Russia, Ukraine, and what it's doing to influence how the USG is interacting with large providers like Dominion. So that's where I see it going, and I'm hopeful that that's going to develop into more real-time sharing and more mechanisms of sharing the Cyber Century Program.

Jim Guinn:
That's awesome. I would agree. I would say even we do a lot of support for infrastructure for

a lot of clients, and I don't think it's right for any vendor to be in between the absolute owner and operator and who has the right intelligence at that time. I think once it starts getting filtered and diluted and pushed down, information gives you speed and accuracy for decisions. And so, if it gets diluted or it gets filtered or there's a winner or loser chosen, well, even like I said, Rich, you hosted a panel that was talking about acquisitions. The vendor you choose today might... I think it was Dale, Dale Peterson was talking about the vendor you choose today might get acquired by company B tomorrow and now you got to redo everything again, so I like that. And it gives you a kind of thought.
Rich, if we woke up one day and we said, "Hey, we're going to go invest in this. We're going to really pull together everybody we possibly can, U.S. government, there's a lot of really smart people, the vendors out there, both the OEMs, manufacturers as well as the leaders, Adam, yourself and other critical infrastructure providers." How would you start a program like that? What would you do to create a program for these critical vendors to get collaboration started?

Rich Mahler:
Yeah, I think the first thing is to make sure that we partner up the people that are in the industry, the utilities themselves, the asset owners who are driving it, who have to use whatever comes out of it, that are setting the requirements for the industry, that they get a big voice in there. And again, we have a diversity of scale and maturity. For this, let's focus on intelligence and that kind of information. There are some of the top-tier utilities in the country that are actually not just appropriately consuming intelligence; they're actually producing their own. They're mature enough to be able to take pieces that they're seeing, enhance it, marry that up with what they see on their operational systems, and come back with new intelligence that they can share with the rest of the community, with the government, and with their peers.
That's huge. But that's not everybody. That's a very small percent. You're into the less than 20 utilities in the U.S. that are of that scale and capability. So, we've got to make this a way that everybody can benefit and participate even if they don't have that level of capability. But where those that are really out on the leading edge, I'll say, get a little bit of a louder voice because they can drag the rest of the industry along faster. So that's kind of the industry side of it. From the vendor community. We discussed this morning the amount of money pouring into the industry is unprecedented, really over a billion dollars for OT security tools in the last year. It is just, it's unimaginable two years ago, and we're seeing these scales now. Some of them, I think we want to include them in the idea generation side but then really have the asset owners decide what they need for the industry.
So, we don't want to lose those inputs. We want to collect those inputs, but we want the asset owners to really drive what are the requirements of the industry, not what the vendors want to sell. But all of the vendor community that we're talking to. I've got at least, I don't know, four or five of them that have said, "If you're involved in a standard-setting thing, we want to give our input. But once that's set, we will put that money into our product and make sure we can participate in that part." Because they're obviously financially motivated, but they're also a bunch of people who want to do the right thing as well and help advance the industry.
And so, they've got the capital, they've got the motivation. They can help accelerate a lot. They'll do development on their own side. They'll advance these things. They'll build the tools. There's competitive pressure for them to keep leapfrogging each other, so we're going to see the maturity of the tool sets in the market just continue to increase at a really good pace. And I think that'll really helps bring everybody along and lift up and make sure that the supply and the demand really come and fit together well. Things that are being built are the things that the industry really needs, and that the industry is getting the benefit from that investment that's flooding in.

Jim Guinn:
Absolutely. And yeah. Yeah, please.

Puesh Kumar:
I just want to jump in on just two quick things that Rich and Adam mentioned. First, on just the intelligence piece. Now how we're looking at it is the vendors, the cyber security tool vendors out there, they are enablers. They're enablers of actually looking at the intelligence on industry networks because, for a very long time, I think we've always thought intelligence solely is within classified networks and so on. And I think what we're saying is there's actually, yes, there might be some good intelligence there, but there's a lot of really good intelligence out on industry networks. Those are the networks that are actually being hit every single day, every single second. So how do we start to connect the dots on what's happening on those industry networks with what we have on the classified side, and how do we start to connect the dots and really understand what is happening in critical infrastructure across the United States?
And so, I think those tools actually enable us to do that. So, I don't want to discount the value of those tools because I think they really do help us get to that place. And then the second point, just to clear up any dispersions or disperse any concerns about the ETAC, ETAC is not regulatory. One thing with DOE is we are not the regulator. We have FERC for that. And we actually find that we have better partnerships by not being the regulator. We actually can partner with the sector without the concern that we might actually regulate it. Just in case anyone is listening and thought ETAC would've been any sort of way of regulatory.

Jim Guinn:
No, no, no. I think hopefully everyone knows that, but it does create an interesting question for you, Eric, which ties into how you guys are about to journey off into the regulatory sort of climate in a bigger way. I think it was September of last year, sometime around September you published the ICS Critical Infrastructure Performance Goals and Standards that we quickly grabbed hold of because we agree it needs to be done. It's something that's very important. But how should industry be thinking about that when you're working on these things? When CISA specifically is working on these things, not just the cyber sprints, but also the extension of the NIST cybersecurity framework. The regulatory bodies that are now going to fuse. You just mentioned FERC; everybody knows who FERC is. Sometimes they're winked at and waved at, and sometimes people turn around and go the other direction. They don't really want to collaborate a lot because it's a regulatory body.
But Eric, when you think about that and now with DHS, CISA dealing with pipelines and air and rail, how should the industry start thinking about critical infrastructure and engaging as you guys advance more into the kind of regulatory space?

Eric Goldstein:
Yeah, thanks, Jim. So, taking a step back, CISA is not today a cybersecurity regulator. We have no ambitions to be a cybersecurity regulator. We are profoundly a voluntary partnership-based agency. We have a small regulatory program in the chemical sector called CFATS that is not focused on cybersecurity. We are a partnership trust-based agency at our core. And I think the performance goals that are derived from a presidential memorandum last year really are very congruent with this overall strategy. Our goal with the performance goals is really to help organizations answer a core question, which is, as organizations utilize the NIST cybersecurity framework or a relevant ISO standard or whatever framework they want to use, how do organizations help answer the question internally of how am I doing? How do we measure maturity towards security outcomes in a way that organizations can use in narrating to their board, to the business looking externally to their insurers, their counterparties, their customers? That's really the goal here.
It's something that I actually feel very strongly about because I saw in my prior role in the financial sector the challenge in narrating cybersecurity maturity to those who are not practitioners, that having a common set of benchmarks and baselines to have that narrative conversation about maturity and progress towards outcome-based goals. That's really our objective here. We are doing this in a profoundly

transparent and even industry-driven way because of the voluntary nature of this work. If these performance goals are not useful to the organizations we want to adopt them, this will all be wasted work. And so, our goal here is when we publish the next iteration of the common baseline performance goals later this year, it is something that will have already been accepted as credible and useful by the private sector, so it will be adopted as just another artifact to support maturation of cybersecurity enterprise risk management programs.
And that is why we got extraordinary feedback on the first draft of goals. I think we had over a thousand comments, which is awesome. We are now adjudicating those comments. We're going to come out with a new version of the performance goals that will go through another round of feedback. And then from that, we hope to have a product that we can then publish. But this will be a living product that we'll want to update over time, just as NIST is doing with the separate security framework.
And then, I think really excitingly, once we have the common baseline performance goals done, we're going to work with the sector risk management agencies like Puesh and his colleagues at DOE to think through is there a value in sector-specific goals for each given sector. And there may be some sectors that say, "We think these common baseline goals are great; we're going to use them for our purposes." There might be some sector that says, "We use IT and OT in a certain unique way. We have a unique risk environment. And so subtle adaptations or nuances to the baseline goals might be useful." But again, we are really eager for this effort to be part of the voluntary body of knowledge that organizations can use to mature their enterprise risk management programs in a voluntary transparent way.

Jim Guinn:
Now that's... And from my own personal perspective, starting in the industry and moving to consulting much later in my life, probably half and half my professional career, there's been a lot of static in the media lately about what was mandates, executive orders, security directives, whether they're good or bad or rolled out effectively. None of this is clean. It's always going to be messy, especially with the ever-changing cyber climate in times that we live in, it's only gotten worse, and it's going to continue to accelerate. It's going to be sloppy every once in a while, meaning it's not going to be perfect. It can't be perfectly thought out. You can't have your bomb, and you can't just go engineer everything from scratch because, by the time you build, it's already moved. So, there's going to be some hits and misses. So, I appreciate you sharing this is what our Evergreen plan is. We're going to continue to evolve these goals and standards for industry and even potentially have sector-specific industry standards.
Because I think, at least in our experience with the clients that we have the opportunity to serve, every industry has the same set of baseline problems. They all do. Every one of them they're common. But as we saw with Russia, Ukraine situation, and the invasion that Russia has taken on, we had to go develop industry-specific countermeasures to protect the most critical assets by industry. Swift in banking, what do you do, and how do you do it? It's the electric grid and certain geographies, and then it's pipelines, and how do you manually deal? How do you pivot from a control room that operates globally to individual regional control rooms in the event you have to? I think it's good. I appreciate your just thinking about it that way. I want to ask, and this is a totally off-the-cuff question because something came in Adam, and a totally off-the-cuff question because something came in, Adam, and this is going to be directed to you. As Eric talked about standards and Puesh has talked about what ETAC is trying to provide, when you think about the information cross-industry or standards, or whether it's NIST CSF or, as you said, Eric, ISO, right? I mean, NIST has elements of ISO in it. As you think about those, how do you baseline your board? Is it standards-based? Is it methodology based? Do you say, "We've reduced our cyber risk by 27% and we've invested proper dollars in this area?" I know I had a conversation with Yanni from Oxy about this earlier today, but how do you do that? How do you leverage the standards,

understanding the goals that the USG is trying to help with the critical infrastructure goals? How do you communicate that, and how do you represent that to your board?

Adam Lee:
Yeah, that's a great question. I think the two ways to approach the board are to bury them in metrics and hope you get out alive, or you can tell them a story, frame it up. Try and build essentially a risk register across your IT/OT environments and say, "Hey, here's where our greatest risk is." Then try and get them smart on the areas where you need to make investments and you need to build capacity to manage the threats to your company. It's going to be different across the company. I mean, Dominion Energy, many of the large utilities and energy companies in the United States, are holding companies, right? They're legacy siloed operating companies that are held together by an enterprise. Dominion's not that way. We are a top-down company. A CSO has the ability to make policy, a CSO, CISO role. You can achieve certain things across your enterprise that you wouldn't necessarily in a holding company or in a small utility that doesn't have the dollars to invest.
For me, it's really framing up for them where the greatest risk is. One of the recent investments obviously is in those devices, to identify anomalies in our industrial control systems and to give ourselves telemetry in our sim for the OT environments. Those are things that we had to build. I think also bringing the board along, since the topic here, the theme of our discussion, is around sharing information with government. Companies are reluctant to do that. When I was in the FBI Cyber division in 2005, that was the trickiest thing we had to deal with. Here we are many, many years later and having to solve the very same problems we identified back then, which is how do you get that meaningful interaction between government and large corporate enterprises.
The board sometimes doesn't necessarily ... they're looking at incident response. They're looking at some of these things like how we manage risk, and sometimes engaging conspicuously and loudly with government creates risk, as they see it. Trying to demonstrate to them that government's ability to assist companies ... and Colonial's an example of that, what the FBI can do, what DHS, DOE, TSA in our gas business, what they can do to help you manage these situations [inaudible 00:48:27]. Then if you do have an event, bringing them along so you can manage your program, and you can do it as a CSO or CISO threat manager without being concerned for your job if you're doing it right.

Jim Guinn:
I know that we're coming close to the end of time, but one of the questions I just received you started to touch on, and I really want to go around the horn and have everybody [respond]. I'll start with you, Puesh, because you started it about DOE is not our regulator, FERC is our regulator. I know this came from one of our utilities clients. I'm certain of it because of the way the question is worded. Then, Eric, to you, because within DHS there are regulatory bodies. You have TSA, and they've set standards and they've set SDs that you mentioned, Adam. And then Rich, I'll finish with you. The last question I do want everybody to take a crack at, because I think it's really important because the theme of this, as you said, was industry and government information exchange and collaboration.
The question is how can I help my organization navigate government collaboration, when there's an internal concern for potential regulatory and compliance fines or challenges if something occurs? It's a really good question, because you do want, if something does occur ... especially now that it's signed into law, Eric ... but if there's an event, whatever the material is, and you got to go through the rulemaking process, et cetera, but you have to notify CISA, right, of what happened. I know, having advised clients, "Look, if something goes wrong, the quicker that you get it out in the open, the quicker you can resolve it." But that doesn't always go over well. Puesh, I'll start with you, because DOE is not a regulatory body. What would you give that particular viewer, that listener? How would you coach them when they're worried about their

senior executives with regulatory affairs and issues by doing this collaboration and talking about threats and vulnerabilities they might have?

Puesh Kumar:
Yeah, it is a challenge, and having been on the private sector side, I know there's always that fear of additional regulations, additional standards, and it possibly being more of a paperwork drill than it actually contributing to security. I appreciate that, and I expect Eric, coming from the private sector, has also seen it on his end as well.
At the end of the day, what I urge a lot of companies to think about is if you put aside what you need to do from a compliance, regulatory perspective, really if you can help your boards and councils understand the posture of cybersecurity, doing assessments and really understanding where you are as a company from a cybersecurity perspective, having those honest conversations with your board and leadership is going to help you, because it can get your funding to actually do more across the organization.
I know one of the tools we really push is our Cybersecurity Capability Maturity Model, or C2M2, and that's a great way to communicate to your board in terms of, "Here's where I'm doing well, here's where I need to be investing more into my network, into my systems." And change the conversation from that compliance conversation to really thinking about what is my posture as a company and what more do I need to be doing so that you can actually get the resources to actually accomplish this very important mission you have as a company.
I think that's the thing I've seen with the electricity sector and the oil and natural gas sector, is at the end of the day, the folks who are leading these organizations from a chief security officer perspective, chief information officer perspective, they all want to do the right thing. They understand the criticality of their networks, and they want others to understand it without the fear of compliance. That's where I would shift the conversation, is to maybe think more about communicating the posture of your cybersecurity programs and what tools do you need to invest more into it.

Jim Guinn:
I like that. That way, it's a positive reinforcement. If I go talk to the person that regulates me and they share information, then I could get a fine because I didn't meet a standard, [inaudible 00:52:24], and there's a ton of them, right? Eric, what are your thoughts? Coming out of Goldman Sachs, you did have regulatory when you were there, so how do you help someone think through that question?

Eric Goldstein:
Yep. First of all, I fully endorse everything that Puesh noted. I think it's really well stated. I think the use case for sharing information with CISA should be seen as really distinct from regulatory obligations. Sharing with CISA is really for two very simple purposes. The first is so that we can offer assistance to help an organization if they so desire it. We know, realistically, many organizations, particularly large ones, are going to have an IR firm on retainer. They're going to bring in their third party. They're going to do what they need to do.
The broader use case, which really I can't amplify enough, is the fact that we know that adversaries every day are executing intrusions into American networks using the same infrastructure, the same vulnerabilities, the same TTPs, and the more that we can understand what our adversaries are doing across the country and then we can share out that information quickly, that is going to harden the terrain for these adversaries, reduce the likelihood of further intrusions, and help every organization be more secure.
There is both a business interest and a national interest here. Where I think we all agree is that there are too many cybersecurity intrusions today. There is more that government can do to turn that tide. But we also need information from the companies that are actually being targeted, so we can understand what our adversaries are doing and then take action in response.
At CISA, we have robust authorities for information shared with us, such that that

information is not used for regulatory purposes. That is something that Congress provided to incentivize information sharing and, again, to enable us to serve our core purpose of helping to protect others. The goal here is not to penalize the victim but to help prevent other victims from being compromised across the country.

Jim Guinn:
You said it very well because your mission is information sharing. It's not to go find somebody. Also, what we all know, because all of these cyber events over the past handful of years have really accelerated, the cost of not doing it is significantly more, and more people will lose their jobs than being open and candid about what happened and trying to remediate it. You can look at a bunch of them over the course of the years and see how institutional shareholders and boards had changed because things were not disclosed, things were not shared, and they could have been, and it would've mitigated some of that.
Adam, I went in this reverse order so that you could pick up the stick on the last one because I know this came from one of our utilities because of the way that it was worded, and the question came across right after Puesh talked about DOE, you know, different than FERC. I have to imagine, even though you came out of the FBI and you moved into the private sector in critical infrastructure, there were probably some folks back in 2018 that weren't really too keen on the complete open kimono about everything. What did you do, and how did you shape those conversations to try to help get around that or advance?

Adam Lee:
My charge when I got here ... and CISA, Brian Harrell in Eric's chair before, helped us think around some of these things ... but converging security, physical cyber and building a capacity for threat intelligence, knitting the two together, and then using that threat intelligence director position which I created in my organization to be the conduit with government and the trades, and to really be our funnel point for receiving as much information as we could, and then having analysts distill it down.
Then what they do is take all that threat information and produce intelligence products for our leaders at Dominion Energy and some of them for the entire workforce. It's really to inform our leaders about what the threat picture is for a whole variety of things, from physical threats, active shooters, all the way to Eastern European hacking groups and nation-state attacks and supply chain attacks. We try and really inform our leaders about these risk areas.
Then just relentless training, relentless sensitizing to build a security culture within our organization. I think three years in, we've achieved a great deal of success. Constant battle rhythm briefings to our board of directors and our audit committee. I think it really is a persistent effort at changing a culture because let's face it, regulated utilities are engineer cultures, and it's like the fire department. We're the power company. As long as the lights are working and rates are low, everybody likes us. You really need to change that culture because you're going to be asking for investments, you're going to asking for behavior changes, you're going to be asking for a user interface on the end points that is going to be maybe a little less streamlined, so whitelisting, nation blocking, a lot of the things that we have to do as a utility. I think we've made great progress, but that's really the challenge for a CSO or a CISO is to really work to change the culture because, frankly, your people are your greatest asset and your greatest liability, depending on your culture.

Jim Guinn:
Absolutely, and I like the fact that it's not just about cybersecurity and dealing with U.S. government entities that could possibly be regulators. It's about all threats, physical, kinetic, all of them, and having a continual education and dialogue with the leadership so that it's not just a one-off thing. It's talking about threats as it pertains to Dominion and what you provide.
Well, look. I know we are literally at exact time with one hour. I can tell you from my perspective personally, and from Accenture's perspective, and anybody that's listening on the phone, our

clients, our competitors, our colleagues, media, everybody that has participated in this, I cannot say thank you enough for being candid, open, and discussing things that there's a lot of buzz about. I'm not talking about the kinetic war that's going on in Eastern Europe. I'm talking about ETAC and what you guys are doing with JCDC, and then CISA's performance goals and standards, and really trying to wrap your head around it and share with at least everybody who's watching this what might be coming next. I personally thank you, we at Accenture thank you, and we hope to see you again very soon. Thank you all for your time and your comments.

Puesh Kumar:
Thank you.

Eric Goldstein:
Thanks so much.