Live captioning by AI-Media

Hello

ARIA JAVIDAN:
Hello, the webinar will begin in approximately 30 seconds. Hello, my name is already a job done on the project manager of the National Consortium of Telehealth Resource Centers. Welcome to the latest presentation in the NRDC RC's series, 'CISA Services: Federal Cybersecurity Resources for Telehealth', is hosted by the Northwest Regional Telehealth Resource Center.

These webinars are designed to provide demonstrations for support and guided development of your telehealth programs. Just to provide a bit of background on the consortium, located truck the country, there are 12 regional telehealth centers and one national, one focused on telehealth policy and the other on telehealth policy. Each service point for the effective use of telehealth and sporting access to telehealth services in rural and underserved communities.

A few tips before we get started, your audio has been muted. Please use the Q&A function of the Sioux platform to ask questions. Questions will be answered at the end of the presentation. Please only use the chat feature for communicating issues with technology or commit authentication access issues. Please refrain from asking questions or making comments.

Please note the close captioning is available at the bottom of your screen, today's webinar will be recorded and you will be able to get access to this and past webinars at our YouTube channel and at our website. With that, I will pass over to Nicki Perisho, Rogan Director of the Northwest Regional Telehealth Resource Center.

NICKI PERISHO:
Thank you, Ariela. Welcome, everyone, it is my honor to introduce our speakers in today's sea's a webinar. Travis Light serves as cybersecurity advisor for the Cybersecurity and Infrastructure Security Agency or CI essay, CISA looks to strengthen the resilience of the nation's infrastructure.

Cybersecurity infrastructure advisors work with infrastructure advisors for subsequent information, develop mitigation strategies, and respond to cyber incidents. They also provide cybersecurity resources.

Next up, I would like to introduce Bob Bastani. Bob is a senior cybersecurity advisor critical info structure at the administration for strategic preparedness and response, he also co-leads the government wide cybersecurity coordinating Council for the health sector and the joint healthcare and public sector.

Cybersecurity working in his role. Mister best Donnie works with the federal government, state, local, and entities and public owners and operators of infrastructure. He also worked with healthcare and public until the managers in order to improve the sectors cybersecurity risk posture. Without further ado, I will head over to Travis and Bob to take over the show.

TRAVIS LIGHT:
Thanks, Nikki, let me pull up my slides there. Are they displaying OK?

ARIA JAVIDAN:
Yep, looks good.

TRAVIS LIGHT:
Good afternoon, everybody, or good morning if you're on the West Coast. Just introducing today, CISA, some of the federal resources that are available. What we are doing in the federal government to help serve critical info structure providers which includes telehealth providers, too. More on that in a moment.

As Nikki said, Travis Light, I'm the security advisor for CISA, has a cadre of cyber advisors across the country and we are here to help you. I'm joined today by Bob Bastani with Health and Human Services, for strategic planning and resources. I will talk a little bit about how CASA
are working together.
A little bit of background, CISA, we will cover that at the beginning here, go over the current threat environment, introduce the joint cybersecurity toolkit, cover the Health and Human Services cyber performance goals and then finally close out with some additional resources leaving time for some questions at the end.

If you are unfamiliar with CIS a or haven't heard of us before, we are the newest federal agency. We are within the department of homeland security and we will actually turn six here on November 26, we're just shy of six years old as of today. We serve as a national coordinator for critical infrastructure resilience and response, meaning that we cover both cybersecurity and physical security as well.

We also have missions to protect chemical security for critical infrastructure owners and operators, and telecommute occasions. Really, we are here to protect all of critical infrastructure in a variety of different categories there. We are here to defend today and secure tomorrow via a wide range of services both on a technical layer, on strategic layers, and to work with a concept I will introduce in the moment, the cyber risk management agencies.

Some of our core capabilities, we are here in a nonregulatory capacity to help bolster cyber defense across the country, physical defense across the country, again, across those critical infrastructure owners and operators, you will hear me see -- say that many times. Many of the ways we do that is to build community, build partnerships, make sure the appropriate and sees and organizations within states and between states are actually communicating with each other.

In some ways, we are able to share information on current threat actors, on current indicators of compromise for the latest cyber threat activity, down to those individual organizations and also take lessons learned to feed the broader regional and national communities.

We also work in incident management and response, we are hopefully able to get ahead of that so you are not dealing with cyber incident but in the event that that happens, we are here to provide some amount of support. We are also here for risk assessment and analysis, more on that later, venture technical services that feed the network defense service that we provide, and emergency communications.

We work across all 50 states, closely with local and state and private sectors. We are divided into 10 regions, you will see this regional concept applies to several other federal agencies, I think FEMA might have been the first to divide the country like this and everyone else liked it and jumped on, I believe, Health and Human Services is split into regional offices like this as well.

You will also see, I will provide the slides at the end, you got the email contact to reach out to whoever you were closest region is so feel free to do that. I mentioned critical infrastructure sectors and sector rich management agencies, so I want to go over some background there.

2013, the federal government established these 16 sectors, you can see where healthcare and public health and obviously were telehealth fits into that concept. On the right, you will see the primary federal agency responsible for managing the risk and managing security in an agency.

For healthcare and public health, you probably already guessed that it is health and human services, the cyber risk management agency, this supports management and can authentication between the seams but we are not the lead for security and telehealth.

For that, I will turn over to Bob, who is with Health and Human Services for more information on how that looks from their perspective.

BOB BASTANI:

Thank you, good morning, good afternoon, everyone. It's really good to be with you today. A little bit about, so my colleague Travis talked about the HHS being a sector rich management agency for healthcare and public health.

Within HHS, the administration for strategic preparedness and response, a SPR for short, is the operating division that has that responsibility for risk management agencies activities. HHS, like many other federal agencies, is a very large and diverse organization with many operating divisions.

We have a lot of subject matter experts spread across the division and that aspect plays a strong role in project management and coordinator. That circle that you see is all the different organizations within HHS that touched different parts of healthcare and public health.

For example, FDA, this plays a big role in medical devices, especially of interest to this group and telehealth group. CMS does a lot of processing of building and so on. When there is an incident in healthcare and public health, it touches a lot of these different divisions and we do that coordination with the different groups.

Wanting to bring up here is that in our role as S RMA, we are purposely firewall on the divisions that have responsibilities or the parts of the divisions that have responsibilities, preparatory responsibilities. Things that are passed to us, we don't pastor them, therefore, there is that level of trust that we are trying to build separate from our regulatory agency. Our goal is aligned, it's pretty laid out by system, -- CISA, take a lot of our lead from CISA, and our goal is ultimately to strengthen the resiliency of healthcare and public health against cyber threats, be in a position to respond to cyber threats. And protecting patient information.

As mentioned, I work very closely with healthcare, coordinating Council, cyber security working group, and is basically a joint public partnership. It has a 400+ memory from all subsectors of healthcare and public health, from healthcare providers, hospitals, pharmaceuticals, med tech companies, health ID companies, and basically, we have a large number of task groups that will work on different aspects of cyber risks.
To adjust the cyber risks in this sector.

Also, within this is also an HHS 405D task groups, the HHS for a 5D program, which is another large partnership within public and private entities, it develops very detailed guidance on how to prepare the sector for cyber threats. To respond to cyber threats and also how to do a lot of training programs and so on.

TRAVIS LIGHT:

Thanks, Bob.

BOB BASTANI:
I'm turning this over to you now.

TRAVIS LIGHT:
I want to highlight, too, each of the 16 critical infrastructure sectors has a sector correlating counsel that is intended to be this collaborative effort between not only the federal government and state and local governments but especially that private sector.

In this case, from what I've seen, healthcare coordinator counsel is by far the most developed. They put a lot of good information, a lot of what we will present later, but a lot that was born out of this healthcare Council, specifically this cyber workgroup.

Just kind of browsing through the list of 400 members, I haven't seen many that are dedicated to telehealth, so that might be something if there's anybody on the call who is interested in, as far as I know, it is a volunteer, there is a way to join this group and inform some of their publications.

Speaking of their publications, it's a few years old now, I think it was first published in 2021, but there is a guide to securing telehealth and telemedicine that they published. A lot of what we will talk about that is cyber related, it applies both to telehealth as much as it would traditional brick and mortar type clinics and hospitals.

Just keep in mind, Health Sector Coordinating Council, there's links that I will provide later in the presentation, certainly something to check out. Moving on to some of the current threat environment. Threat actors, in a variety of different flavors, each with their own goals, with their own motivations, and their own levels of sophistication as well.

We've seen a rise in really just about all six of these, from activists who target wastewater systems following the October 7 tax last year. Cybercrime has been lucrative, it continues to be lucrative, haven't seen that tamping down lately. Insider threat, we will cover this on the next slide, but insider threat is not necessarily malicious but certainly can be, it goes hand-in-hand with espionage.

Cyber terrorist attacks and warfare, we seen a lot of real-world examples of that not only with the conflict in the Middle East lately, but between Russia and Ukraine. Going back to that Health Sector Coordinating Council, a lot of what the resources that they provided our built around these five flavors or categories of cyber threats. Including social engineering, that being traditional phishing scams, email compromise, we've seen a huge rise and that which is like phishing but a far more sophisticated version.

Organizations are able to compromise somebody's, specifically, any email account and they're able to send out what look like legitimate invoices they've made. Whether it's an invoice or request to change banking information or for payments, etc.

Social engineering is hard to defend although there are several ways to do it, it seems probably like the least sophisticated Avenue. Ransomware attacks, in short, a threat actor is able to put an effect on your system and they are able to threaten all of your files and data and programs to prevent you from accessing them.

They then try to sell you that encryption key back, they have Expo treated or stolen your data so they are demanding a second or additional fee for you to gain access to your data again, and prevent them from selling that on the current platform.

Third category, loss of -- loss or theft of equipment and data, goes hand-in-hand with ransomware attacks or denial of service, so that you out there providing telehealth services don't have access to the tools you need to function. Insider or accidental data loss there, we've seen a huge uptick in that as well and then attacks against network connected medical devices, all these new Internet of Things or the smart technologies, especially since they have some kind of connection to the internet, whether it's that they face the public internet themselves or they are accessible via a smart phone or a local network.

Each of these provide an avenue for an attacker to gain a foothold on your system, or they are able to compromise that medical device. I also want to highlight ransomware attacks, loss of data, each of these has been far more lucrative in compromising personal identifiable information. Personal health information goes for far more on the dark web then your Social Security number or your credit card information.

A lot of what leads to that increase where it's so much more valuable to compromise health information is that one, is something that doesn't change. If your credit card is compromised, it's too easy to call and get a new credit card. There are monitoring services in place if your socialist compromise. There is less that is able to protect against your health information. It's been far more lucrative. There's also concerns about how sensitive the information is in particular and also, the compromise, if you have that data on somebody, you have a whole new way of attacking them.

Just going out there that health information is lucrative, and I have some quotes that will highlight that in just a moment. I know everyone is excited about AI these days, it's important to remember that threat actors can use AI, too. They are using it to create more sophisticated and credible social engineering tactics, they are able to use AI to generate and build malware and find new vulnerabilities. In existing software and hardware. Folks are compromising your AI services or even poisoning the data so, in short, since this isn't a full presentation on AI, to deliver bad information so that when a patient is looking to or find information from an AI service or no if a procedure or medication is safe, the AI says, "Yes, those two can be combined no problem," When in reality that is not true but the data the AI is pulling from has been compromised.

Something to consider, the health sector correlating counsel has a great presentation on integrating AI and machine learning in healthcare as well. I have some case studies here, not to name and shame these effective organizations, but to drive the point home. Each of these is widely publicized, you can find far more information on it by googling.

I want to highlight Prospect medical holdings that was affected last year, specifically by ransomware and because their systems were compromised by ransomware, that ended up close to emergency rooms, they had to divert and onto his, of the 16 hospitals affected, at least three of them were still diverting and balances from the hospitals for 17 days following this ransomware attack.

You can see how even though the ransomware is just optimizing the IT systems, it has real-world impact. Thankfully, I haven't heard of any deaths attributed to this you can see the impact that something like ransomware can have in the physical world. They did have to revert to manual processes for the processing of records, and patient data was stolen and sold on the dark web as well.

You do see on the right of the HC three alerts, going back to Bob's slide on a SPR and some of the subdivisions of that, (unknown term) is one of them, I will talk about that in just a bit. The next case study, I imagine most everybody on the call is most familiar with the compromise of change healthcare, which is a software provider with in United health processes, I believe most of the claims of organizations in the country were hit by ransomware earlier this year.

Really, the effect of that on individual clinics, hospitals, etc., a lot of them were worried they wouldn't be able to keep the doors open. Providers are having to dip into their own pockets to try and make payroll. Again, just like with Prospect, folks are having to go back to processing prescriptions insurance claims by hand, potential ransom was paid was claimed to be $22 million. The actual economic impact of that was far greater than $22 million, and then they put out that there was a significant portion of US citizens data that was compromised, probably in the tens of millions.

Personally, my family each got one of the letters in the mail saying their data was compromised. I pulled that picture from (unknown name) communications just to show the supply chain attacks. It wasn't TRICARE or military hospitals or individual hospitals, but that supply chain attack really had so many downstream effects including on military readiness here. Sadly, within a few weeks of that initial attack, change healthcare got hit again.

While they were trying to recover and restore healthcare services, we restored some systems that might still be vulnerable to that frat actor, they got hit a second time by a different group just within weeks of the first. Certainly something to inform your cyber incident response program.

Pulling just a couple of quotes, one for my Deputy Director and as well as Deputy Erie -- Deputy Secretary of Health and Human Services. (Reads) (Reads) You can see especially from Prospect and the interruption of emergency services how a cyber attack can actually have those real-world consequences.

Really, the threat landscape in healthcare tends to be the top target lately. That's fantastic. Moving onto the cybersecurity toolkit and hey, federal government, what are you doing about this? Just some information here. We have published, it's really easy, you have a link on this slide, these slides are centered everybody, but this consolidates a lot of CISA and HHS resources, some of which we will cover in just a moment.

Some of our free technical services, how can touch with us, how to sign up for alerts and advisories, available both online and in-person training, and exercises and incident response guides. One of those you can see there is the Health Sector Coordinating Council, CMS, HHS 405D, conducted a resiliency landscape analysis, huge survey that they published this last year for health providers of all different levels, etc. I want to cover some of their findings there because really, that is informed a lot of what we are doing at the health center.

Key findings, growing threat of ransomware, we already covered that. Variable adoption of critical security features, you've probably heard of or familiar with multifactor authentication, they did find that something like 90% of the hospitals surveyed had some form of MSA but maybe not against the most critical systems or what they might identify as their crown jewels, the data systems that they really want to protect.

Vulnerability assessments, this is another one were a lot of organizations out there are doing vulnerability assessments, but maybe don't have the capacity or the resources, the manpower, to do something about the findings of those assessments.

Training and outreach is something that a lot of organizations and clinics are doing but maybe they are not tailoring that training to the appropriate folks, so really, as it would apply to telehealth, I'd be very interested in seeing some kind of applicable training rather than just the general awareness.

Also, hospital and home, unsurprising that this is on the rise and introduces all sorts of vulnerabilities, ulcerative new attack vectors, but really, that they haven't been targeting hospital and home so much yet. Email protection, a lot of what's built in to alert suspicious looking emails or filter those that have been up across nearly every organization, something like 98% of them.

Supply chain risk is pervasive, change healthcare is a perfect example. As I said, medical devices so far are generally not targeted. I expect that to change. A few more findings, inconsistency across health organizations as far as where the weaknesses are, which does make it harder for us to address those. Really, establishing a baseline for cyber practices, which we will get into in just a moment. So that everyone is at least meaning the minim -- minimum of protecting from opportunistic attacks.

Use of antiquated hardware, software, and systems, hopefully we see this lesson telehealth, but is always the question of if the hardware the people are using at home is up-to-date. The cell phones and operating systems of those phones they are using to access those services, are those up-to-date or are they flashing red lights because they are using an old version of iOS or android or something?

Insurance premiums continue to rise, that's a whole other discussion but really, the insurance companies for probably about five years ago, the default was to pay the ransom or pay a threat after whatever they were asking, and maybe even negotiating that cost down.

Insurance groups have not been excited about paying that, looking to either raise premium prices or they are looking to require customers to need a certain baseline per cybersecurity. We start talking about the cyber performance goals, keep in mind that it can lead to increased costs in insurance premiums.

Probably goes without saying, recruiting and retaining cyber talent as a challenge, but also adopting these baseline cybersecurity practices works. Across any of those practices, the organizations that were following them had much better results and far fewer incidents than those that weren't adopting those practices.

I want to introduce, I mentioned them a couple of times, cyber performance goals. Want to cover what those look like, I mentioned that healthcare and Health Sector Coordinating Council has been kind of leading the way as far as the sector correlating councils go. Another way they do that is with the cyber performance goals.

2022, CIS eight published the cross sector cyber performance goals. They are meant to be voluntary guidelines that are capturing almost cyber security 101. Please, if you are doing nothing else, do these midmonth things. The healthcare sector took that and ran with it and develop their own cyber performance goals tailored to healthcare organizations, there are 10 essential goals and there are 10 enhanced goals, if you're being into the essentials, focusing on those enhanced goals would be the next step.

Bob is here to tell you far more about the CPG's as they relate to healthcare than I am.

BOB BASTANI:
Thank you, Travis. Just to tell you that CPG use, CISA has also developed a number of performance goal guidelines for all the industries as a whole and the CPG's that we have customized has really been very much in synchronization with what CISA has developed.

They are tailored for healthcare and public health based on the vulnerabilities that we have seen in healthcare. So why should we have the CPG's? I think the idea of having these performance goals is that they are only voluntary right now. Voluntary recommendations for now, but with the question comes why have this? What drove this?

Travis set the stage, you are seeing an enormous amount of increases in cyber attacks in healthcare. We've seen some very big incidents this year, we saw some last year that really affected continuity of care. When we look at these incidents, because of these incidents, we see that some of them vulnerabilities that were compromise, that were exploited, were somewhat basic. They could have been avoided. Some really basic steps.

There's a lot of numbers in this and I won't go through this, you can see the percentage increases in breach and ransomware, that we've had to deal with. That survey that we did, the study that we did of healthcare that Travis went over, really identified a number of reasons, some of them are mentioned here, healthcare and public health rely on very small margins.

Cybersecurity is very much underfunded when it comes to investments. That's an even bigger issue in the smaller hospitals, the smaller remote entities when the choice has 2B between buying new IT equip and or a new extra rate -- X-ray machine. The funds are very limited. We also see that the threat landscape has been involved here.

Now, with the introduction of new tools, they are based tools boast on the offense of side and on the tooling side, we see that the landscape has really increased. Attacks are a lot more sophisticated and the landscape is much larger. The sector as a whole has complained that they are getting way too many guidance from different parts of the federal government.

(unknown term) has a lot of guidance, CISA has a lot of guidance, and they are already warning some centralization of this guidance. This really set the stage for developing these basic performance goals.

For the sector. That's how they came about, if you can move to the next one.

A little bit of an overview of what the CPG czar. They were developed in coordination with a lot of work between CISA and HHS and the private sector. To develop this guidance. This is not something we developed in a vacuum. They are pretty much (indiscernible) guidelines. There is a map to this framework and also to four or 5D guidance to achieving them.

The basic set of recommended controls that are just minimal controls that you would like the entities to put in place, these are really addressed to very prominent, known entities who have seen this, they are easy to do, and for the most part, easy to implement. There's a large return value for putting them together.

As I mentioned, a big part of the CBG's is to simplify the landscape of controls and demystify this framework, all the frameworks that are out there. Next? We have the essential goals and the enhanced goals, the essential goals are basically the floor, a set of floor safeguards. The essential goals are listed here.

We talk about mitigating known vulnerabilities and enhancing security, making sure you have multifactor authentication and making sure that you deploy encryption, both at rest and in transit, guidance on how to put controls and credential management, and big user and account management. We see this being exploited all the time where there is no separation between users and access levels. These CPG's are applicable both on the supplier side and on the vendor side.

In addition to that, we also have a set of enhanced goals, these are for more mature organizations, with essential goals in place, and they're looking to enhance their defenses. It targets the more sophisticated attacks, the more impactful tax these are things like making sure we have asset inventory, and third-party vulnerabilities. This third-party, I'm thinking within the telehealth environment, as you dealing with the landscape that involves many different providers, all the way from telecom providers and different thought providers and so on.

Each of these providers provide an opportunity for introducing vulnerabilities into the landscape and just being able to manage that vulnerability and to contracts sometimes and others to manage that landscape. Next? Again, I talked about how the goals are mapped to controls, CBG's, and the hiccup practices.

If you go to the side, you will see there are links here to the CBG's, you can see that clearly and I think that does acute services to demystifying and D confusing this landscape of controls.

I talked about the four or 5D -- 405D program, excellent resources for when it is hard to do something, that is building awareness campaign for the environment, how to do outreach, training material, there are a lot of posters that have been developed and so I strongly urge you to go to the 405D website and take a look at the valuable assets that have been developed there. They have been developed mostly by private sector partners.

Do I turn this over to you at this point, Travis?

TRAVIS LIGHT:
Yeah, I will take it back over and close it out in a few minutes. Bob mentioned the 405D program, that's another one within a SPR, that knowledge on demand bit. We have that joint kit linked to the 405D program, the knowledge on it, so it's written not for the technical folks among us but is written mainly not only for providers but for decision-makers, C-Suite execs, that sort of thing. Cybersecurity training and awareness is intended for a broad audience and you can see, for the knowledge on demand, it's aligned with those five threats that we covered earlier, if you start a social engineering, this is all free and available on the website. Feel free to check it out.

You got a whole course on each of those threats and there's far more to go into as well. More background on what CISA is and does, at least as it relates to the CPG's are those health industry cyber practices. I mentioned I'm a cybersecurity provider here in Montana. There's at least two of that -- us in each state now, there are additional ones of us in the larger cities, we are available here to answer questions, help you understand your current cyber posture, and we give gap analysis for things to improve either right now or on more strategic long-term goals.

Some of those, what I do on a daily basis is I visit, not only because I'm covering 16 different infrastructure sectors, not just clinics but I will go to a hospital to sit down for however long they like to, whether a two hour assessment or a full day assessment and talk through how they aligned those best practices. Are you thinking not just through technical controls but going back to the CPG's, things like if you are managing your supply chain or are you considering cybersecurity when contracting with vendors?

If you are outsourcing or using a managed service provider, what kind of controls do you have in place to log your activities and that sort of thing? Reach out to your local CSA and you can have a discussion with them or they are funded to come to you. Some of the technical pieces down there, I want to highlight the vulnerabilities scanning, Travis Light on that next. It is a take away today, sign up for a vulnerability scanning soon of the rest of what the worldwide internet knows about your system, and also we provide remote penetration testing services, and as long as you pay your taxes on April 15 every year, these are available at no cost.

You might be curious, if I have the federal government, and talk to me about my cyber posture, what happens with that information? The good news is that with CISA, since we are not regulatory, the assessment information, that vulnerability information is protected under that protected critical infrastructure program as well as a few other federal laws as well, so that information you are sharing with us is protected from release under FOIA requests, understate sunshine laws, protected from use in regular Tory purposes.

Obviously, if there is some kind of instances, you have to report that to HHS, we are talking specifically on vulnerability assessments, risk assessments, you talk to us and that will be fed into a government database or regulatory information. Back to that vulnerability scanning, it is limited, but if you have a static website that hasn't IP before, that has external scanning for free that lets you know what the rest of the internet already knows. It's on the internet, it's getting scanned, usually multiple times a day by multiple people. That's just a fact of life.

You might as well know what the rest of the internet knows about your system, it is a continuous scan meaning that it is no less frequently than once a week, I highly recommend, it's one of the easiest things to sign up for and gives you a nice report card like the one on the right. We also have resources for stopping ransomware, meant to be, protecting from ransomware, understanding the latest threat activity from ransomware actors and then an assessment to see where you stand and how well protected you would be from likely ransomware groups.

Going back to what Bob mentioned earlier, so many of the attacks we see, the overwhelming majority of attacks we see are opportunistic. Following those basic cyber practices, the cyber performance goals, stop what we see from there. Going back to the change healthcare one, that had to do with not having multifactor authentication on a particular server.

Identifying those crown jewels and those basic cyber practice really thwarts threat actors and those opportunistic attacks. I also want to highlight that we have cyber tabletop exercises, I have posted some here within the state that are focused on healthcare and are focused on local government or others, but we have the national cyber exercise team that can come to you, they will work with you to develop an exercise that's tailored for your organization, whether that's a coalition, maybe one of the regional telehealth resource centers wants to host a program for telehealth organizations within their area, that would be a great place to start.

You also have the premade tabletop exercises link there and then finally, protective security advisors. I'm a protective security advisor so I talk a lot about cybersecurity. CISA also has a whole cadre, of protective security advisors as well. If you have some kind of a brick-and-mortar location, if you have a data center and you are curious from a physical security standpoint, guns, gates, guards, cameras, doors, etc., reach out to them, they were full fleet of practices that's similar to us on the cyber side.

With that, aria, I will turn it back to you to moderate questions.

NICKI PERISHO:
Thank you, Travis and Bob. That was great, that's a lot of information and a lot of useful resources and links and information for our rural healthcare systems and low access hospitals. Let's see, aria is answering some questions in the chat, I don't think we have... Any specific questions. I will give everybody just a minute, I just want to express gratitude for these resources and that our federal government is sponsoring this because this is so necessary in this day and age and the education about how do authentication and other small steps that organizations can take to protect themselves in preventing cyber attacks moving forward.

TRAVIS LIGHT:
Absolutely, I will also add that we mentioned the cross sector cyber performance goals, they really only came to fruition, I think version 1.0 was published last year, landscape resiliency analysis was published last year. So much of this is new and developing and we are trying to take, so it's not only the federal government telling you what to do and what right looks like we are taking that feedback from the private sector and from local government to feed the broader community's best practices.

NICKI PERISHO:
Excellent. I want to show that these slides will be available and the recording will be available as well at the NCTRC website and the (unknown term) website. I want to thank you both for your contribution today and being available and I also want to highlight, as Travis had said, each state has two CIS a representatives. Please make sure to reach out and identify who they are. I see Bob has something to add.

BOB BASTANI:
Thank you. I just want to mention, since we talked about the extent of CISA, there's a task group within the joint cyber working group that is looking at cybersecurity of public health, specifically. There is a survey that had just gone out, it targets specifically the public health community. I just want to put a little plug about that, I will send you some information about where that survey is located, I would really like to get the state CISA's and the state CIOs to purchase paid in that -- participate in that survey.

The results of that survey will be used to request funding, for example, funding identified as a gap, we would go back and press funding. If there are legislative changes that need to be done, we can also take that survey, but it really depends on that survey and asset work really depends on the participation of the public health community.

I want to make sure that you get information about that and if you have that distribute it, we would be grateful.

NICKI PERISHO:
That would be great, Bob, we will put that in our newsletter, probably out in the January newsletter if that's OK.

BOB BASTANI:
The survey closes in December. If there's any way that you can figure it out, that would be good.

NICKI PERISHO:
Send it to me and will make it happen, we will send it out for the month of November is over. We did have a question, an attendee is wondering if there's any way to know if their organization is working with you now?

BOB BASTANI:
There is a list, we have a list and actually, if you go to the (indiscernible) we actually have a list of all the organizations that are engaged.

TRAVIS LIGHT:
The (unknown term) Council?

BOB BASTANI:
I assume that was the question.

TRAVIS LIGHT:
I'm not sure either, and typing out a response right now. It's a public list of who is part of that workgroup and also, if you are interested in knowing, "We already signed up for something like the vulnerability gains in service," I can look into that for you, too.

NICKI PERISHO:
That would be great, any other questions out there? Getting a lot of thank you for the detailed information, thank you for the presentation, getting a lot of that in the Q&A so I think people really appreciate these resources and this information and we are going to need more as we move into this digital space so good to plant the seed and let people know that you are out there, just like the TRC's to utilize at no cost to them. Hopefully we can make change.

Anything else, Bob or Travis, you want to add for I headed over to aria to close up shop?

BOB BASTANI:
I just want to stress my gratitude for this opportunity. Thank you.

TRAVIS LIGHT:
Yeah, I greatly appreciate, and I will add anecdotally here at the end, all my work in healthcare Center -- sector which is been an awful lot over the past few years, I am somewhat in the vulnerability scanning, someone reached out and I contacted them about it and it led to this working with Montana health Hospital Association, Montana primary care Association, Montana medical Association, etc.

You might not even think of it but these little communications, that community building, really can snowball and have a much broader effect on the broader healthcare community. Certainly get in touch with your local CISA cybersecurity advisors.

NICKI PERISHO:
Thank you, Travis.

ARIA JAVIDAN:
Thank you Travis and Bob for the pate today. Just a reminder that we don't host a webinar in December due to the holidays, our next webinar will be posted on Thursday, January 16, 2025. That will be hosted by the Mid-Atlantic Telehealth Resource Center, a registration information is available on the NCTRC events page.

Lastly, we do ask that you take a few minutes to fill out the survey at the end of the seminar, your feedback is valuable to us. Thank you to the Northwest Regional Telehealth Resource Center for hosting and to Travis and Bob for their presentations. Have a great day, everyone.

Live captioning by AI-Media