**November 9, 2021 Meeting - Seattle Community Technology Advisory Board**

Topics covered included: Cybersecurity at the City of Seattle; Cybersecurity Awareness and Hygiene

**This meeting was held:** November 9, 2021; 6:00-8:00 p.m., via Webex

**Attending:  (All via Webex)**

**Board Members:** Rene Peters, Camille Malonzo, Nicole Espy, Femi Adebayo, Leah Shin

**Public:** Dorene Cornwell, Eryk Waligora, Harte Daniels, Coleman Entringer, Tara Zaremba, Kristen Hoffman, Aisha Davis, Peter Walton, Bob Fletcher, Jesse Moore, Annie Shaw, Aurilee Gamboa, Cara Vallier, Alex Salazar, S, William Shuai Wang

**Staff:** Trayce Cantrell, David Keyes, Greg Smith, Tara Zaremba, Vinh Tang, Cass Magnuski

**27 In Attendance**

**Rene Peters:**   Everybody, welcome to the CTAB November edition. I would like to do a quick acknowledgement that we are in Seattle on the traditional land of the First People of Seattle, the Duwamish People past and present. We would like to honor them and offer our gratitude for the land, itself, and to the Duwamish Tribe. Harte Daniels, one of our members, pointed out to me earlier this week that November is National American Indian Heritage Month. I'm going to post a link here in the chat, but you can learn a lot about the interesting history, from Native Americans in the military to a ton of interesting links for events throughout the entire month of November on the site, so please feel more than free. And I would encourage you to take a look at some of those events. Thank you to Harte for raising that.  <https://www.nativeamericanheritagemonth.gov/>

I just generally hope that everybody is adjusting well to November and the newly oppressive darkness that we have been experiencing here since Monday and falling back on the clock. One of the things that I like to do throughout this year that I haven't done in a couple of months -- we've had some great presentations and this idea of tech tidbits or new and relevant news. And today I figured I'd talk a little or make a couple of points about Facebook, which I guess you may now call Meta instead. But, for those of you who don't have Facebook, they recently as of this week claimed to stop the use of facial recognition technology, specifically with tagging machinery and backbone. And so, ironically, that was the very topic of our last meeting when we had Councilmember Kohl-Welles in from King County, on facial recognition legislation that she had championed. What was interesting about Facebook's statement was basically, they needed to weigh the positive use of faces for facial recognition against growing societal concerns, especially as regulated. Legislators around the country have lagged in providing clear rules, and they are basically saying they'll be getting rid of their facial recognition setting. So, again, picture tagging primarily. And that will be shut down. But they'll still have some use cases of facial recognition primarily around individual personal identification issues. They will still use your face without identification, but only use it for unlocking your individual account, and getting rid of the option to have that facial recognition setting in tagging photos and things like that. They're also saying that around 38 percent of Facebook users, which I think amounts to about two billion people that have used that photo tagging and facial recognition, and they will be scrubbed or deleted. I would be curious to see the mechanics behind all of that and how they'll actually go about that data deletion, if that's what it will be. Another very interesting thing is that, going back to February of this year, Facebook had about a $650 million settlement from a class action lawsuit in Illinois where a number of individuals -- I think it might have been about 500 people -- claim that Facebook has stored biometric data with their photo tagging without any consent. And Illinois apparently has a little bit of a different facial recognition state legislation that a lot of other states that led Facebook to just settle with those individuals. I'll post a link where you can read up on that here in chat.  <https://www.theverge.com/2021/11/2/22759613/meta-facebook-face-recognition-automatic-tagging-feature-shutdown>

I work in augmented reality, so I have a bunch of thoughts on it, but I think it would be cool if some folks check out and watch some highlights of Mark's keynote. Whether you think it's pie in the sky or dystopian, I would love to hear back some of your opinions. Anyway, I'll close my rant because we have a really great agenda. We have some amazing guests today. First off, I'd like to approve the minutes from our October meeting where we had a fantastic update on facial recognition from King County Councilmember Kohl-Welles regarding legislation that she championed. That was our feature presentation. So, if board members could offer a motion to approve those minutes?

**Femi Adebayo:** I move to pass.

**Rene Peters:**   Thanks. Do we have a second for Femi?

**Leah Shin:**  I second.

**Rene Peters:**   All right. Can I have the 'ayes?' Are there any 'nays' or abstentions? All right. So, we'll go ahead and focus on the agenda for today. We have two great cybersecurity presentations. I want to thank the Privacy and Cybersecurity Committee and their members for their hard work in coordinating this. Can we have a motion from a board member to approve today's agenda?

**Femi Adebayo:** I move to pass.

**Rene Peters:**   All right. Can we have a second.

**Nicole Espy:**  I second.

**Rene Peters:**   Thank you. Can I have the 'ayes,' please? Any 'nays' or abstentions? Perfect. So, before we get started, I just wanted to run through who is here and do some quick introductions. Name, affiliation, and area of Seattle that you're calling in from today.

**INTRODUCTIONS**

**Rene Peters:**   That is everybody, unless somebody slipped into the queue after I started. If so, let me know. Again, I wanted to thank the cybersecurity community for two great presentations today. The first centers around Seattle cybersecurity. I wanted to thank Auralee and the rest of the committee for bringing in our speaker Greg Smith, and I would like to hand to either you, Auralee, or someone else on the cybersecurity committee to give an introduction to our speaker. Appreciate it, and I will hand off the mic.

**Nicole Espy:**   Camille is trying to speak.

**Camille Malonzo:**   I'll just give a quick introduction. First of all, thank you so much, Auralee, Tara, and the folks in the security program for joining us tonight. I don't want to take a lot of time, because we're really ready for a great presentation. Our first presentation is Greg Smith. He is the City of Seattle's chief information security officer, and director of security and infrastructure. He is responsible for the City's cybersecurity program as well as strategy and service delivery of foundational City technology. We're really excited to hear about cybersecurity more broadly as a program at the City of Seattle. So, without further ado, I think we're going to hand it over to Greg.

**CYBERSECURITY AT THE CITY OF SEATTLE**

**Greg Smith:**   Thanks, Camille. I'm really happy to be here. Thank you for having me. It's great to join everybody. I managed to avoid the tornadoes with power intact, so I'm good to go. I'm calling in from Edmonds tonight. It's a little bit north.

I'm the CISO of the City of Seattle. I've got a lot of technical domains in my purview. I'm responsible for both the cybersecurity program and a wide swath of service delivery aspects in the City. Over the past six months or so, we've begun to work towards weaving the cybersecurity mission in with the infrastructure mission. I'm going to share a little bit about that. But, also just generally, what are some of our challenges; what are some of the unique situations with driving the cybersecurity program in the public sector specifically in the City of Seattle.

Just a little bit more about me. I have been with the City for 24 years in various roles, 19 of them with Seattle City Light. Prior to the consolidation of about five years ago, I come from the infrastructure world. My career has been public sector. That's where my heart is, in the mission-driven work. So, it's exciting to be doing that in this new capacity. I've been in the CISO role for about six months, but I've been adjacent to it for most of my career.

Seattle IT provides information technology services to City departments in support of their missions. We have 37 departments, I believe. We have a lot of departments. So, we're kind of corporate IT for the City, and support them in their missions for the residents of Seattle. the cybersecurity program is really crucial to ensuring that we protect City data assets and keep our systems running and reliable and operationally sound because those are a big part of how we deliver services to the residents of the City of Seattle. Just by way of a preamble, there.

Agenda-wise, I'm going to talk about what is the general security landscape in the public sector and what are some of the wrinkles there. I talk to a lot of City CISOs and we kind of share the common challenges that our other peers don't face. So, I'll share a little bit about that. What are we thinking about when we think about cybersecurity? How are we approaching it? An important part of this is establishing relationships with other entities, not just other cities, but our regional partners, the County, other cities on either side of us. And then I'll do a quick wrap-up.

The general security landscape in the public sector -- we have a lot of diversity in our technical environment that Seattle IT is tasked to protect. It comes with the typical constraints of government. We have financial concerns. We are tax payer and rate payer funded. We are not here to make a profit; we are here to serve the residents in the City. Generally, in Seattle IT, we focus on lean and efficient technology delivery. We know that our financial situation may change with the general economic fortunes of the region. By extension, we are cognizant of being good stewards of tax- and rate payer funds in our approach to delivering a cybersecurity program and executing one. We have some of those typical governmental cybersecurity restraints, and we just have to build some agility around that in what we do. Politically, administrations change, the complexion of the City Council changes over time. Priorities shift and sometimes you have to restate your case. This is not unique to Seattle IT or cybersecurity programs. this is just kind of the nature of being in a government.

The diversity of our mission is in lines of business. It's all over the place. We have courts. We have public safety. We have utilities. We have transportation, human services, parks and rec, construction inspections, internal services, like every other business: HR, planning and administration. And then we have the myriad of smaller departments that are critical to other service delivery types in Seattle: animal shelters, immigration and refugee affairs, neighborhoods, education and early learning. It's all -- I could go on and on. Each of those missions is crucial to the overall mission of the City in delivering services. So, we have to keep all of that in mind. And we have a very diverse range of business customers to partner with. The next step from there is we have a wide range of types of employees in the City. Some are office workers that are fairly tech-savvy. But we also have a lot of field workers. We have a lot of seasonal workers. Some of them have a desk. Some of them do not. some of them have City-issued cell phones. Some of them do not. When we think about rolling out a simple technical control, we have a lot of different use cases to consider. And therefore, it can be quite complex to push things out to our user base.

And then, we also have public-facing departments. We have City staff interacting with the public on a daily basis, whether that's a physical access angle from City technology sitting in public spaces, like kiosks or shared work stations in service centers or community centers; things that are very close to public access where we have to think about physical security. So, there are just a lot of things to think about from the cybersecurity perspective. That's what makes it fun, exciting, and never dull.

Cybersecurity challenges: We do have, of course, an increasing level of sophistication in the cyber threats that we see out in the landscape. So, our challenge in the City  -- and I'm sure that the members of the board who are cybersecurity versed are well aware that the landscape is extremely dynamic from a threat perspective. Our challenge in the City is how do we keep up with the rapid pace of development of cyber attack techniques, different types of campaigns. How do we keep pushing up our maturity level to be well-positioned to stave that off? And that's not always just technology. That's a people issue. It's a process issue. Technology is sometimes the easy part. Of course, looking at the biggest threat factors for attacks starts with our end users at the most basic level; their vulnerability to social engineering via phishing attacks, or anything where they might click on the wrong thing. So, we have to think about our approach to that. As I said, that's where our diverse user base, their level of sophistication. Adoption of emerging cybersecurity technologies -- how can we be agile in our large, diverse institution? I just outlined the business units that we serve. We do try to standardize as much as we can in the hood, but as we go and partner with our various business customers, whether it's Seattle Public Utilities or SDOT, their priorities are very different as we move from department to department. And it may be different regarding their tolerance for change. Some of our departments are change-averse. They are large solid-state institutions. In many cases, that's fine and good and appropriate for their line of business, but we go in there and we have to ask them to be a little bit more nimble, as we keep up to where we need to be to have the right security function. Where staff are involved, there's a change fatigue that comes with adding this control and that control. So, there's organizational change management, a challenge at times. And, we are cognizant of that. We work through that, but it means that we have to be very intentional, and be thinking about that as we consider standing up a new cybersecurity initiative.

No surprise, here. Attracting and retaining cybersecurity talent is probably a nationwide and industry-wide problem. It's a competitive job market in Seattle, for starters for technological talent. When you get into the hottest technology area, cybersecurity, where they've been running a zero percent unemployment rate for a decade, you can see the challenge we have. Now, we like to look at that as an opportunity to identify individuals within our organization that have an interest and an aptitude. We're doing a lot of thinking about internships and different approaches to growing talent just out of school, reaching out to non-traditional avenues to find individuals. Because one of the things about cybersecurity is that it is very aptitude-oriented. There's a type of person who wants to be working in this and can be successful There's a lot of detail. Some of it is very detail-oriented. So, that's a challenge. I will say, too, that Microsoft recently made a statement about committing some massive investment into this part of the job market through training and recruitment. So, I think that there's broad awareness, and some very high-level efforts to address the talent gap and the availability of staffing in this area. And of course, the one thing I always like to say is that the bad actors, the malicious actors out there, while we are busy delivering service to the City, they're doing one thing: trying to figure out how to get in. That's one thing that's always a challenge. so, we always have to think about how we can be efficient and do better with the resources we have.

Why are we a target for cyber-criminals? There's often a perception that we don't have that much money to do a very good job with cyber-defense and building cybersecurity programs. We may have trouble justifying spending in the security space. I am happy to say that that isn't too much of a problem in the City right now. There's a lot of money to share here. And there's also a lot of cybersecurity funding being attached to some of the larger grant programs out there. In fact, the infrastructure bill that was just signed, Build Back Better, has a very large cybersecurity piece, so we're certainly paying attention to opportunities there. As we moved to remote work and the ARPA funding and some of the other funding sources that came out of that, the relief funds, there were opportunities to put in for some money to support cybersecurity initiatives, specifically around remote work and some of the things that that introduced. So, I would say that even though there has been limitation in the past, I'm in this role at the right time. There's a lot of great mind-share around cybersecurity, and I'm happy about that. Training? I think there's a perception that City folks don't always get good training. I think that that's not necessarily the case. When I think of training here, I think of how we are continually educating City staff to be vigilant and aware of threats that might be coming after them. The phishing emails are the most common. There's a very large percentage of attacks that begin with that simple vector. And then, time and resources. I think that we work in a resource-constrained environment, and then you have economic challenges that might hit your staffing levels or your resource levels. And I think it just sort of paints a picture of us being a soft target.

We also have a lot of different lines of business. We have a lot of reasons why people might want to come after a government, whether it's for political reasons -- I guess those are motivations down below there. First of all, money. If there's a ransomware opportunity, cyber-criminals are going to be looking at it. But beyond that, we may have data that is of interest, of particular types. As I said, we do have 37 different lines of business. That's going to appeal to somebody. Hacktivist reasons. We have some departments that may appeal on that front, whether it's public safety, or some of the other departments that we have. We have partnerships with peer public sector entities: King County, the State, for data exchange and things like that. We may not even be the target. We might be viewed as an avenue to another entity. So, that's something that we have to keep in mind, making sure that our connectivity to other entities like the State or the County are secure and monitored. Influencing elections is very much in the news, and we might not necessarily the target for that, but for public sector generally as their potential rationale. And then, what we do have are utilities. We have critical infrastructure in the City of Seattle. Seattle City Light and Seattle Public Utilities. So, for those who want to create havoc in that way, we might be viewed as a target.

So, that all kind of paints a picture of what we at Seattle IT are dealing with. Hopefully, that's helpful. The Mayor appoints the CTO and the Council confirms them. And then, I have been named by the CTO in my role, and I run the division that has both the security function and the infrastructure function where a lot of the security work is happening. So, my authority flows up to the CTO. Departmental support? We partner with other departments that don't flow up to the Mayor's Office. We have partnerships with law, legislative, and the courts. We share standards. We share certain forms of infrastructure. They receive services from us on the infrastructure side, and we support them on cybersecurity, as well. So, that's all very collaborative and positive. And then, I have very close relationships with Seattle City Light and Seattle Public Utilities on critical infrastructure security. That lives in collaboration land right there.

How do we get so many departments to come along on our security mission? One of the approaches that I'm taking is to really just focus on building a more comprehensive security governance approach inside the City, and that's to get business leaders thinking about cyber-risks in terms of risks to their businesses. It has been fairly traditional in the past to think of cybersecurity as just a technical function over there in Seattle IT. And my approach right now is to bring that to business leaders to get them thinking about important aspects that are risks to their business. I had a conversation with them today about the new emerging risks around vendor supply chain. That being we establish relationships with trusted third-party partners, and there's sort of an assumed level of the viability of that partner. But if they have cybersecurity gaps, and we are relying on them to deliver service for us, then by extension, we are putting ourselves at risk. And that might be simply that, hey, if the organization that prints our utility bills can no longer print utility bills, now we have a revenue problem. Of if this other corporation has the dataset for our payment cards, are they secure? Because they have critical data. They're not probably so much of a problem, because they have payment card regulatory issues. But those are examples of where we need to be raising those risks. It's not just technical, it's a business risk. So, think of it that way. And continually demonstrating the value, from a partnership perspective, of the security program, of what we're doing, being an advocate, understanding their business. And when they start to consider cybersecurity things, they've read something in the paper, to make sure I can go there and translate for them, be an advocate, be a translation liaison in all ways. There's an education component. And then, there's always a compromise and collaboration piece where, of course, as cybersecurity professionals, we want to get all of the things out there right now. But we know we can't. We have to partner with them to get this stuff out in a way that we are enabling them, because an environment that's so secure that you can't do anything isn't really supporting a business, not really driving business solutions. So, there's always that balance.

I touched on a lot of this already, but this is the slide I like to share when I'm talking about the program. People process technology is the common reason. I've added this governance layer because I think that that serves the purpose of getting a City-wide business leader view of how we approach this, how we fund it, how we resource it, how we sponsor it. We have a lot of great technologists that can talk about zero trust and identity security, and in our tooling approaches, and all of the great technology that we have in place to provide security. We can have technology, but if we don't build process to make sure that we're adhering to some of that stuff, we're going to fall down. They are the first line here. It's all of that and you can't ignore any of it.

I'm looking at the clock here, and I know you've got a full schedule.

**Rene Peters:**   No rush, Greg. Take your time.

**Greg Smith:**   Finally, it's a team sport. I communicate a lot with other CISOs. I communicate a lot with other CTOs in the region. We information share. My security team, when we get an email, when we get word of a spam email or a phish email, they look at it and they say, oh hey, this organization in North Carolina obviously has a compromised email account that's being used to send out spam and phishing attacks, we reach out to them. We tell them about that account. We always get a big old thank you, and we establish a relationship and a connection there. We like to do that. we receive that at times. And then of course, as I mentioned earlier, there's the network of public sector CISOs in the region. I'm part of a group of large city CISOs across the country, and we share our experiences and we learn from them, and we pass on tricks and techniques that have worked to push the security mission and similar organizations.

October was Cybersecurity Awareness Month, so I think it was 'do your part, be cybersmart' was the mantra. So, I just want to say, as a CISO, if you're asking me to provide one piece of advice for residents, it's use multi-factor authentication. All of you that have Gmail accounts, I'm sure that there are a lot of you that do, you can enable this by just going into your settings and you can set that up. That's become more and more important for all organizations because when anybody logs into Office 365 to get their email, if you don't have to do something to prove that you are you beside offer a password, then you're vulnerable to exploitation from credential theft, and that can get ugly pretty quickly.

How can CTAB help the City on cybersecurity. This is where I would say if you're interested in helping here, talk to your Councilmember and advocate for cybersecurity as a funding priority. Of course, I remind our business leaders that we can't really serve the residents of Seattle if we aren't adequately protecting our data about our City residents, whether that's utility accounts, whether that's something more personal, and if we are ransomewared and all of our stuff is locked up, and people can't access our systems to, say, request a permit or check their utility usage, or check our affordability portals. Things like that. We provide so much to the residents through our technology solutions. It's really fundamental and a lot of the value that we provide as government. I don't want to overstate that too much, but I'm a technology guy, so that's my take. The question I have for this group is if there's any way that the City of Seattle cybersecurity program can help you guys in your mission, please don't be shy about reaching out. We have a lot of membership here, and a lot of attendees from my division in particular and Seattle IT more broadly. I know there's a lot of interest and affinity for this group, and if we can support your mission, we are happy to contribute however we can.

With that, I'm happy to take some questions or comments or anything. And Harte, I did see your comment about Edmonds CC. They do have a very good cybersecurity program, and in fact we have an employee on my security team who joined Seattle IT as an intern out of that program, and is now a rock star on my team. So, that's a great suggestion. I appreciate it.

**Harte Daniels:**   Boeing has to do both business - they're one of the most tapped businesses in our area and they also do a lot of government and DOD, So, they are very intent on supporting education and the Seattle area. So, anything that any of the Boeing programs and any of the community colleges would be great.

**Greg Smith:**   Yes, absolutely.

**Rene Peters:**  Anybody have any questions? Answers? I have a quick one. I'm always curious about the intersection of cybersecurity and critical infrastructure. What are some of the key targets that you and your office and your team think about and defend against? What are the hottest conversations in that intersection?

**Greg Smith:**   Well, the hottest conversations are of course about utilities. It was earlier this year that a water utility in Florida was targeted to contaminate the water supply down there. It didn't get there, but it was kind of an eye-opener. And of course, there is a lot of concern about electrical infrastructure, as well. Electrical infrastructure is very heavily regulated. There are a lot of controls in place as it is. So, I think that's starting from a more conservative space from a security perspective anyway. They don't even like to have their sites connected by internet, for example. That's a risk factor. But at the same time, there's a lot of modernization happening in that space, too. So those groups are Seattle City Light partners, and are really having to chew on some of those balance points. I need to be careful about talking about some of the specifics here, but I know that this is certainly the top priority.

**Rene Peters:**  I think I saw somebody getting on the mic, so if you want to unmute yourself.

**Bob Fletcher:**   Just a quick question. I know you took over for Andrew. Are you in a permanent role as CISO, or can you shed light on that?

**Greg Smith:**   Unfortunately, Bob, I'm permanent. Sorry.

**Bob Fletcher:**   No, that's good! The last time I talked to you, you were filling in for Andrew, who moved on. So, you're permanent. That's great!

**Greg Smith:**   You know, I've been around for 24 years. You can't get rid of me that easily. I am permanent. I'm excited by the role. I'm actually very excited by the move to combine our security functions with our infrastructure functions. And honestly, that's happening more in the industry, from my conversations with other CISOs. I don't know that it fits for every organization, but we're liking what we're seeing, weaving that security mission out instead of instead of being on two sides of a wall is kind of the approach we're taking. And it's good to see you.

**Bob Fletcher:**   Yes. Thanks!

**Rene Peters:**  I know we're somewhat behind, so let's take one last question. Harte, did you want to ask your question?

**Harte Daniels:**  Given that my two questions in the chat were on the integration of cybersecurity, project management and your PMOs setting the governance on projects, as well as disaster response and recovery from the Office of Emergency Management, have you been able to work across departments to make cybersecurity or security and privacy integral from the very beginning. I know you have to touch base throughout, and just not leaving it towards the end? Your infrastructure architects' response, but to make it everyone's responsibility. Thank you.

**Greg Smith:**   It's a fantastic point. We do still have the problem of getting towards the end of a project, especially a multi-year project, since before we had this degree of emphasis on it. And it's getting close to 'go live,' and then you do some security scans before you go live, and you find vulnerabilities. You find problems, architectural issues. And then, you're kind of stuck in project delays, or swallowing hard and doing some follow-up remediation. We have process improvement that we're working on to get gates in there around security reviews and risk reviews and compliance reviews and privacy reviews. All of that is some process improvement in our PMO and education with our project managers. A work in progress, very much. On the DR and response and recovery, emergency management is in my purview and Tara Zaremba, who is here, clones that function in my division. And we have been working with departments on response to this. We actually had a table-top exercise about a ransomware scenario with public safety in September. And the idea there is to educate. What are your business continuity plans if your 911 application doesn't work? Or the computers in your offices don't work. Do you have a secondary approach? Of course, we have a recovery task in IT. But do the businesses know what they would do? There are multiple angles for that. But yes, it's the right thing to do as you say, Harte. Think of business continuity.

All right, I'll watch the chat a little bit longer to try to field any other questions.

**Rene Peters:**  We really appreciate that. Thank you so much for your perspective, and for bringing us up to speed on the work that you do every day. I think a lot of us, especially in the Cybersecurity and Privacy Committee look forward to continuing to work with you in building this relationship. Thank you very, very much.

We'll move on quickly to our next cybersecurity presentation. And I'd love to hand the floor off to Eryk Waligora, who was involved in bringing in our speaker, Alex. so, if you're there, feel free to come on and take it away.

**CYBERSECURITY AWARENESS AND HYGIENE**

**Eryk Waligora:**  Yes, sir. Thank you all very much. Thank you, Nicole Espy and Camille Malonzo from the Privacy and Cybersecurity Committee for helping make this possible. Our goal in this meeting is not only to bring on Greg Smith for that great presentation, but we also wanted to take this opportunity to speak to Seattle residents in a way that brings it more home to them personally. So, that's why we wanted to talk about basic cyber-hygiene, basic fundamentals. How is this affecting people in our daily lives? Not just through institutions, but through the impact that we see every day. So, we reached out to the University of Washington's Office of the CISO, and we are so glad to have found Alex Salazar from the office. And I won't take up any more time. I'll let him introduce himself. So, thank you, Alex!

**Alexander Salazar Jr.:**  Thanks for that introduction, and thanks, Eryk, and thanks again to everyone who has been working with me to prepare this presentation. I look forward to providing some insights for you all.

My name is Alexander Salazar Jr. As Eryk said, I work for the University of Washington Office of the CISO. I hope to give you some tips on cybersecurity hygiene as well as some awareness of cybersecurity threats. A little bit about me: I'm actually a recent resident of Seattle. I hale from Northgate. I went to Central Washington University, got my undergrad degree in IT and cybersecurity. I'm currently a UW grad student. I'm actually a newlywed and new resident of Seattle. I'm definitely enjoying the city life.

I work for the CISO, which is the chief information security officer. Our mission at the CISO office is for UW to share responsibility and safeguard personal and institutional data. And the different functions we use to do that is the daily security operations. Jesse Moore is a part of that. Cyber-intelligence, which is a team that I work with. As Greg Smith was saying, the end user is the key piece for cybersecurity. It's great that you all want to highlight that in this court. That's the only way that we're going to get ahead of this, through education and training and awareness.

So, we're going to talk a little about the industry approach to cybersecurity, why we should care about cybersecurity hygiene, some tips in these areas of phishing, credentials, and think before you click, and some consequences that we have seen in hygiene you get tricked and clicked on a phishing email or got a malicious file.  So, what is this industry approach? It's very school house in a sense, but we call it the CIA triad. It doesn't stand for the Central Intelligence Agency. It stands for Confidentiality, Integrity, and Availability and an information security asset. And I didn't know you worked for Seattle City Light. I actually picked that as a random sample to apply this methodology, was, 'hey, I'm trying to access Seattle City Light.' When I'm communicating with it or storing data there, our only authorized change is happening, somebody in the middle there, changing things. And the last thing is availability. Can I get to us. And you'll see these three methodologies as we go over some tips that I have laid out here.

Why cybersecurity hygiene? Interestingly enough, the Washington Attorney General just released the 2021 data breach report. I have the source in my notes here. I can put it in the chat later, but about 6.3 million Washingtonians were affected by data breach or cyber attack in the past year. And I found this specific really interesting. Only two of those reported were actually credit card breaches. The rest were information security attacks. So, you are actually a lot more vulnerable to fraud in surfing online. Twenty years ago, I had an incident where all of my money got drained from a credit card scam, but definitely the tables are turning. In an IBM security port there with some metrics, but the key piece there was individual costs that they analyzed ranged anywhere from $180 to get a lifelong subscription if you fell victim to a cyber-breach, or your entire life savings. And lastly, why care about cybersecurity hygiene? Especially in Seattle, you worry about physical and digital issues. So, if you live 20 feet from the main road, you're going to lock your door at night, and maybe even buy a little Ring camera to make sure your packages aren't getting scoped out, and you're kind of taking these physical security steps. But the same thing should also be occurring for your digital security. You have a lot of important emails, bank accounts, tax statements that you've kept over the years, maybe some personal really precious pictures. You want to protect that and we're going to talk about that.

Phishing. We've all experienced or heard of it; it's expanding all the time. What is it? According to this organization that we pay attention to is called the Cyber Infrastructure Security Agency. They have a really long explanation there, but I've kind of broken down the bottom part of what is really behind a phishing attack, because it can definitely transform to spear-phishing, whaling, SMS phishing, a whole myriad. They all really prey on trust, banking on your complacency, trying to raise up your emotions. An example we have here is a job offer letter that we got. It was hoping to bank on a position of trust, especially if you email a spoof and it looks like a professor or a student might actually fall victim to this type of attack because they see the source as in a position of trust. This is a really good example for Seattle City Light. You get an email saying you bill is overdue. This would be the same equivalent.

Next is complacency. Maybe it's Monday morning and you're going through your emails, or it's Monday night and you came home from work and you're trying to catch up on your personal emails. It's banking on, 'Okay, this looks legit. I'm just going to click there and find out. It's banking on you're just being complacent and you click the link and access that site.

And lastly, we're talking emotions. Like I said, there's a new factor to phishing with SMS. I'm pretty sure you all have gotten one. But the real bank that the threat actor is trying to get after is your emotions. So, they might pretend to be your boss. Like, hey this is so and so. I had to borrow somebody's phone, and I need you to do this real quick. They're banking on you as the victim to trust your emotions and not let your boss down. If you let your guard down and go through the steps, they'll outline the scam for you.

Next, we'll talk about protecting your credentials. And what are your credentials? Well, they're the key pieces that identify who you are. I put some outlines there. And the big thing is why. Why protect your credentials? Well, a lot of these things lead to your bank accounts, public utilities. And you all very well know this. But an interesting piece that I have found while researching for this presentation was that if your credentials are ever compromised, the security research group by the name of Avari found that it took less than 12 hours for hackers to try to manually access that account. Manually access means they're going in there and seeing what is involved with this compromised Gmail account and seeing where else they can log into. Also, with protecting your credentials is the security piece of having well-formulated passwords and user and security questions. A University of Maryland study -- it's a little older, 2009 but very interesting -- found that they had some machines on the web, and every 39 seconds, they were getting pinged by somebody trying to guess at the passwords on the device, or trying to see if a certain service was running on the device. Bad passwords are really no passwords at all. What I wanted to highlight here was kind of the use of scripted attacks, especially in this age of machine learning and artificial intelligence. What's helping the technology side to progress is also helping the hackers. So, let's take a figurative person who lives in Illinois, born in 1998, married to a woman named Lauren. Through scripted polling through social media or different ways, I've seen these Excel sheets where they can produce password lists of maybe up to 100 different types of passwords. Somebody might use 'chicago1998.' They use that script to attack and try to get into these different accounts. So, what can you do to protect? Like I said, it takes 12 hours, so don't use password (unintelligible) accounts. As a breach happens, that's the very first thing hackers do, they're going to see every service available with that username and email, especially if you use the same password for your Gmail, your Bank of America account. They're going to figure that out. Don't share your passwords. Use long and complex passwords if you can.

This next bullet honestly overrides all of them. Greg Smith said he really wants to push multi-factor identification. I would also push for that because I really think the age of passwords is going away, especially with supercomputing. You have to have that second set. Once a password is broken, it's pretty bad. And if you don't have that second step to help protect you, the bad actors can get in.

There's a practical step that we always push at the University of Washington. It's called 'password manager.' It kind of puts everything in one eggshell, but it's better than having that password list in notepad, or having that password list in your notes on your I-phone. This password manager is a superior place to store passwords. It also generates passwords for you. So, all you have to do is memorize one. There are definitely free ones out there. KeePass is an open source one. Or there are ones that have a cheap subscription. I encourage using the Google password manager on your phone. Something is better than nothing.

Lastly, in regards to protecting your credentials and you don't believe me, if you haven't heard of this site, check 'Have You Been Pnwed.'  <https://haveibeenpwned.com/> This will show you all of the breaches that are associated with a certain credential. My information is on there. So, you may be surprised. If you use Google phone, you actually get updates if any password that you have was found in a data breach. You might want to change it. You can actually see the data breach associated.

Watch where you click. In 2019, an email security company found that 99 percent of email attacks required human interaction. So, you might think, yeah, I think before I click. Phishing is the relevant attack vector. It really banks on you thinking before you click. Some mitigations you can have in mind when you're checking email or accessing a site is be skeptical of all of the links you receive in an email. Make sure you verify, especially if it's rewritten to look a certain way. Treat all of your attachments with caution, especially if they have a very heavy file or you're not necessarily sure who the sender is. Remember that you know this can be spoofed, especially what we call the alias portion. So, if you're at work, and open Outlook, and get an email that says Rene Peters, and I know it's supposed to say @seattle.gov, but you check and see that it actually says Rene Peters @gmail.com, and you're actually just hoping that the system pops up as an alias for Rene Peters, that spoofing has occurred and you can definitely see it all the time. If you see a login page, check the URL, but honestly go to the source. If you go to the login page for the Bank of America and it says you need a login for this, go through the route that you know is verifiable. They're getting really good with making fake web sites and spoofing them. I have an example here. When thinking before you click, and the model I have is trust but verify, there's this free service that's run by Security Trails. It's not technical. If you can copy and paste, you can use this tool. It's called URLscan.io, and it's basically a sandbox. And it lets the link explode and you see what happens before your eyes. It sees what the link directs you to, and it gives you a screenshot to show that if you use this link, this is the web site it takes you to. This works really well. I'll show you this next step. But again, that's urlscan.io. Use this. Let's say you had clicked on this link -- this is a fake link -- and you got to the Employment Security Department. This is an actual screen shot of an actual spoof of the Employment Security Department that we have seen. The actors really did it. And if you had clicked that link and didn't check the URL, you are going around this site putting in your information thinking that you're actually accessing the real site. So, how can we think before we click and check for spoof sites? We check the top level down. What I mean by top level is everything to the left of the red is what we call the sub-domain. To the right is the top-level domain. And as we walk through, I will show you how you check. So, if I am accessing the Employment Security Department, if I see wa.esd, I think, okay, that's legit. As I start walking a little more, I might think, okay this is weird. I see some numbers and think, okay this is getting a little fishy. I'm probably going to put this into urlscan.io because this doesn't really seem traditional. <https://ciso.uw.edu/education/phishing-examples/>

And the last piece, the top-level domain is xyz. I'm like, wait, hold on. I'm pretty sure that the Employment Security Department is not xyz. So, honestly, I'm not even going to bother with this web site. If you take one thing from this briefing, it's if you have anything with xyz, it's bad. In regard to spoof, I have some other kinds of checks that you can do. You can't always trust a lock sign. So, here I have a screen shot from Google Chrome. What this lock sign is not saying is this is the legit Employment Security Department. What that lock sign is saying is that someone has either certified the certificate to say they own this site, and this site is a site. It's really misleading. This very site itself could have had the lock sign because the actors registered for it. And also, with Go Daddy and Google Cloud providers, it also shares hosting sites that also have that lock sign. This type of site.

Next, we're going to talk a little bit about encryption. The method is keeping your data from prying eyes. So, this goes all the way back to Egyptian hieroglyphics. The big thing I want to take away from encryption is without encryption it's like you're yelling your bank account number outside in the street. Without encryption, you would be communicating on the internet in plain text. Here's an example. If you communicated through HTTP, which is plain text type or ASCII plain text type of site, you're communicating that this is my password. But if you're communicating with HTTPS, it is secure. It has site encryption, you're communicating encrypted. And hackers or anybody collecting all of that data that's going around on the internet, they won't be able to guess it. So, the big takeaway from this one is make sure you're talking through encrypted sites.

What are the consequences? What happens when we click on a bad email or click on a bad attachment? The most common thing is either a) it's fraudulent, or you get malware. There's an explanation there. Especially in today's rat landscape, with everybody working at home, this isn't just going to be a you problem. This might affect your organization. If you clicked on a malware, it might lead to a data breach that your organization has to report on and investigate. If you worked like Eryk for Century Link; there are some people from Verizon; and Microsoft over here, you might need to put proprietary information loss because the system you were on was able to export that stuff. And also, just fiscal loss. Even the machine itself for any kind of damage from the malware. Lastly, with malware, can you just delete it? No, not really. In our lab at UW, any time we had an infected device we wiped it. We hope you have some backups online somewhere to defeat a bad actor. But usually, you have to either wipe the device or burn it to the ground.

Next within the threat landscape -- we're talking about ransomware -- I'm sure you have heard this in the news with Colonial Pipeline and some other incidents. Ransomware is basically a hijack. They do this through encrypting a device, but holding the key hostage. It can occur in your personal lives, or the network segment, or the organization that you're with. In 2020, this cost about $209 million on average for a company to remediate. So, if a City of Seattle ransomware attack happens, or at UW, we're looking at a very average $209 million in costs. That actually comes from *Forbes*. I have the link down there. Why did ransomware become a big thing? Obviously, it's a lot of cybersecurity (unintelligible). There's kind of patch management or vulnerabilities that just go unpatched. What that leads to is this marketplace. So, the same way you go to Amazon and look at a catalog for shoes, these access brokers have dark web forums where they might say, "I've got this exchange server at UW. Anybody want to try to hack it? I've got this public utilities at the City of Seattle web server. Anybody want to hack it?' Then they go off to another person who sells ransomware as a service, and the hackers technically adapt themselves, and they say, "I see you're trying to hack. For 20 percent, we'll take a cut. If you're able to ransom this organization, we'll take a 20 percent cut, and you take the 80. And here's the code to execute a ransomware attack. With the threat landscape, we're also seeing extortion in the sense of if organizations are taking their time, the actors are going to start leaking out things. As in, if you don't believe we have your stuff we're going to leak 10,000 personal identifiable files to get you to start getting to your incident response and we hope that you pay the ransom. And lastly, like I said, remote work. Traditionally, we've been able to contain all of these vulnerabilities and open holes because we have firewalls within a physical building and we're able to contain all of this. With this call -- I'm pretty sure you're all calling from home -- our own devices are being monitored from behind the virtual firewall that is our work. And the actors know that. So, if they're able to get a phishing email to your personal Gmail, which they know at 9:00 a.m., you switch from personal work to work on that same device, that's just an easier vector than trying to go through your business firewall.

So, what can we do about it? The biggest take away is just to honestly report it. And it's a community approach. The same way AI and machine learning is being used in password guessing, getting all of this information, parsing it out, it's kind of the same as if you fell into a phishing attack or there was a malware attack. There's a lot of information sharing that goes on. So, even though you fell victim to an attack, that signature for that specific email or the tactic that was used for that specific attack is we in the information security realm, the term we put to it is indicator of compromise. So that is then shared with the community, which is told to watch out for this. But we can't do that if nobody is reporting what's happening to them. So, please, if you caught it, that's awesome. Report it. And definitely if it's impersonating your employer. So, I would say, definitely with the City of Seattle, report it to that organization.

So, that was a lot. I appreciate the time. At a minimum, what to take away from this brief is in phishing always check the sender email. Don't just trust the alias just because it says Alex Salazar. Click on that 'to and from' area up on the email and make sure that's the appropriate email. And be skeptical of links and attachments. Always trust but verify. Protect your credentials. Use multi-factor authentication where it's available. Don't reuse your passwords. Think before you click. Remember top level domain all the way to the right. If you're accessing anything that's dot xyz, .co, don't trust it. Always trust but verify. Use urlscan.io to help you with that. As Greg said, and many others say, it's a community approach. At UW, we're a team of about 15 protecting about 65,000. Greg might have the same size team protecting a city of millions. We can't do it all. We can't be over your shoulder checking your emails. It's really got to start with you, the end user, to help us out and tackle this. Lastly, just a little snip for us. If you're interested in more on the topics we just covered today, we have some information available at our web site that goes more in depth. <https://ciso.uw.edu/education/phishing-examples/>

With that, I'm open for questions.

**Nicole Espy:**   Thanks, Alex, for the great presentation. I wonder -- I know that this presentation was based on what individuals can do to protect themselves, but I wonder a little bit about UW. Are there particular divisions within the UW community that require more attention or work to protect. You have a medical center; you have a lot of vulnerable students. Where are most of your energies focused?

**Alexander Salazar Jr.:**  Great question, Nicole. UW Medicine has its own information security officer, and they're actually in the process of hiring their own CISO. But we work in conjunction as a team, just because within Personal Health Information (PHI), the mission set is different. There's a lot more security and lock down that needs to happen within medical compared to academic research. We want the world to know this. We want to progress this research community, this academic community. We also have peer contracts that happen with the defense department. We actually have some security managers at our business laboratory that are looking at what the military call the 'dirty net.' It's a big set, but we definitely parse it because it's kind of hard to stamp it out in one big sweep.

**Harte Daniels:**  We have seen an increase in protection of PHI since 2013-2015 when I got laughed at by the Providence CTO when I mentioned ransomware and he tried to state that there is no such thing. Have you seen vast improvements, or are they still a pretty soft target?

**Alexander Salazar Jr.:**  Harte, I'm sorry you had that experience. I hope it's better now. Their team, I know a couple over there, information security analysts. They are pretty on top of it. We are always sharing information on what we're seeing. I would say that your information is in good hands with them.

**Harte Daniels:**  They've been staying off the wall of shame of the Office of Civil OCR. Obama created a wall of shame for anybody who had more than 500 people breached. They posted what the breach was, why it was, how it was, etc., and whether it was by a business associate or not. Maybe you should and look to see the OCR wall of shame. <https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf>

**Annie Shaw:**   (unintelligible)

**Alexander Salazar Jr.:**  Within our security education, training, and awareness, we have a specific communication specialist. She's really there segmenting our communications. Like I said, there's not one stamp, so we parse out our reporting to system owners, system administrators. Here's the student community. Here's some stuff. There was a lot of stuff two or three weeks ago with Discord being used to host malware hosting sites. That isn't as appropriate for staff as it is for students. From these, I would say that communication is definitely becoming important, if it's not already within information security, being able to understand what type of information needs to get out to a group.

**Annie Shaw:**   Thank you.

**David Keyes:**   Just a last question. Thanks a lot, Alex. And thanks, Greg. Just related to that, we work with a lot of community organizations and folks who are trying to pass the knowledge along to their family members. Where would you say there is a place to focus on the community education at UW, or other places for that that you recommend?

**Alexander Salazar Jr.:**  The web link that I -- those risk advisers are definitely are a little UW focused but they would help. That would be the best place. Also, if you emailed, we definitely would love to connect you. Within CISO, we have a communications specialist. She's an information security analyst, but she also specializes in that. Also, as a CIO, there's also a communications specialist. If you're interested in that partnership, I can forward you her name. Actually, Annie, as you were talking about communities, I would say, as a Latino, from a Spanish-speaking household within the City of Seattle, I think definitely if I could do this in Spanish, I would love to, but definitely targeting some of these other communities of non-English speakers, I can think of my grandma who gets WhatsApp messages. It's definitely a fraud scheme as well.

**Rene Peters:**  Well, Alex, thank you so much for really breaking down some simple but very impactful things that we can all do for our cybersecurity hygiene. I'll definitely be using some of these links, because I've definitely gotten dinged by one of those work test phish emails that they send out. I'm just as vulnerable as anybody. This is a really great presentation, and I would definitely encourage everybody on the call to spread some of the links that you and those around you who you know might be particularly susceptible to some of these attacks. This was really a fantastic presentation. Thank you. And thanks to Jesse for being a great hype man and echo, putting all of these links in the chat.

<https://ciso.uw.edu/education/risk-advisories/>

<https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf>

<https://ciso.uw.edu/education/risk-advisories/>

<https://ciso.uw.edu/education/phishing-examples/>

<https://haveibeenpwned.com/>

**Jesse Moore:**   I'm just trying to support and help everyone get those links, so having that handy for you to click is great.

**Rene Peters:**  Yes. I know Cass Magnuski really appreciates that.

**Alexander Salazar Jr.:**  Thank you, Jesse, Rene, and the board. This was really exciting to be able to talk to the community, and I hope this isn't the last time for our partnership with UW. We're definitely interested. As Greg Smith was saying, this is a community approach not just for the silo at UW, but for community members of Seattle as well.

**Rene Peters:**  Absolutely. It will be great to see you guys back here soon. Excellent. I guess this is a good segue for Committee Updates. I just wanted to really thank Eryk, Camille, and everybody, Nicole, on the Privacy and Cybersecurity Committee that has pulled together what have been two really great and very complementary presentations for tonight. With that, we will go ahead and quickly get through Committee Updates. If Privacy and Cybersecurity wants to keep the ball rolling with yours, go right ahead.

**COMMITTEE UPDATES**

**PRIVACY AND CYBERSECURITY COMMITTEE**

**Nicole Espy:**   These were really great talks. We appreciate all of your time. We also thank the audience for so many questions. We'd love for you guys to join the Privacy and Cybersecurity Committee. It's the last Tuesday of every month. The links to the meetings are already posted on the CTAB web site, so it's easy to find us. Hopefully, we will be following up with an expert on some of these topics and continuing our work. That's it.

**Rene Peters:**  Thank you so much, Nicole. Digital Equity and Inclusion, do you have an update for this month, or any announcements?

**DIGITAL EQUITY AND INCLUSION**

**Harte Daniels:**  I didn't realize that Coleman was here. Go ahead.

**Coleman Entringer:**  I'm going to go through just a few things. We discussed the state of the budget season, and the Pedersen amendments proposed forward as far as digital equity funding goes. Regarding the Build Back Better movement, we haven't put together an official position as a committee around those amendments. But we did discuss budget season. And then we put into the works plotting for a potential telecom panel board for CTAB. Those were the big updates. Just a reminder that we meet on the fourth Tuesday of every month at 7:00 p.m. So, feel free to drop an email if you want to get on the list. We'd love to have you.

**Harte Daniels:**  Cara also gave a call to action to remind people about supporting or talking to your City representatives about supporting equity. And David gave an update on DELN, forming us that they have signed an agreement with Literacy Source to coordinate DELM in future. If David wants to add to that, that's fine. They are in the process of hiring somebody who (unintelligible) former position. King County will have some digital equity grants, about a million dollars. The State is ramping up with Digital Equity Forum. There is a federal national infrastructure act, which should have more money for DE. And finally, I think the National Digital Inclusion Alliance conference will be in Portland next year on February 18. Did I miss anything, David?

**David Keyes:**  No, that's great. I'll post a link for folks who want to participate in the Digital Equity Learning Network, meeting on November 18. We're having folks from the State Broadband Office and from King County, talking about their digital equity grants, as well. A good time for networking. And, our office has just posted for internship positions. I'll send that around and put the link in. <https://www.eventbrite.com/o/deln-36681987993> We were talking about the budget. Cara Vallier is still here, as well.

**Rene Peters:**  I was going to say during public comment, but you might as well just add some color commentary on the call to action. Take the floor.

**Cara Vallier:**   Good to see you all. Thanks so much for sticking around. An excellent presentation by Greg and Alex. Thanks for all of that information.

The latest information is that the balancing package has been released. It is posted now. Councilmember Mosqueda, who is chairing the budget process, has released her balancing package and I think the good news is that Internet for All did well overall. We do have fully funded SPL hotspots. We have the Digital Navigator program still in there, which is good. It is not fully funded at the level we had asked for in Councilmember Pedersen's amendment, but TMF came out fully funded, so that's exciting news. As well as the continuity that we asked for to have the budget book describe all of the investments in Internet for All. What I think is new for us is that the amount of money that was expected from the forecast was less than the Council was working with previously. Those expectations were diminished a bit. So, I think the call to action now is to thank the Councilmembers for considering Internet for All, to thank the Councilmember budget chair for including all of the Internet for All amendments in her package and to emphasize how important Internet for All still is. We thank anyone in advance who would like to participate and call in tomorrow at 5:30 p.m. I can put that link in the chat as well, if that would be helpful. But mostly, it's positive news. We wanted it all, but everyone did have to take a bit of a haircut. It's a long story, but I think the take away is that they didn't have as much this year as they last year because of those estimates. But we feel thankful that Internet for All is still being carried forward in this budget.

**Rene Peters:**  Thanks. That's an awesome update. We're grateful for that news. We will work with what we got. Please definitely drop the link in the chat. From what I understand, the public meetings to call into are tomorrow at 5:30 and then also on the 18th in the morning, also. Thank you so much.

**Cara Vallier:**   Great. Terrific. Thank you.

**Rene Peters:**  All right, so we can just and open up for general public comment. If there are any updates or announcements? I'll open the floor.

**PUBLIC COMMENT**

**Jesse Moore:**   I have a question about Internet for All. I could probably go to that meeting. Could you speak a little about the partnership. I hear the budget concerns. I'm  curious about the partnerships that you have in mind. It seems like something we could do at the State of Washington.

**Cara Vallier:**   Certainly. We're looking at the amendments specifically; we're looking at hotspots to be checked out at the library, an additional 135. The second amendment was for the Technology Matching Fund, which CTAB has worked on for many years; community-based organizations. Digital Navigators is also a program. I think David Keyes could speak to that more, but that's being funded at $250,000. And then just keeping the Internet for All Initiative, which came out of the Internet for All Resolution that Councilmember Pedersen put forward last year. We didn't see that show up. In those terms, in this budget. So, we're hoping to have continuity in Internet for All for future budgets. I'm not sure if that answered your question, but I'm happy to give you more background on Internet for All.

**David Keyes:**   Jesse, maybe I could add a touch to that. I think there are sort of two avenues around the partnerships piece. One is where organizations, corporate sector, philanthropy individuals can help that route to City dollars to help these projects move forward. An example of that, for instance, with the Technology Matching Fund grants, Verizon helped fund one project this year. So, we were able to leverage some of our funds. And they made a contribution this year and last year to fund one project.  So, there's certainly a lot more opportunity, I think, on both the community grants for a variety of digital inclusion purposes, whether it be helping folks with devices, or signing up enrollment in low-income internet programs, putting up WiFi at community organizations, and supporting digital skills training. And the other piece of it is certainly the partnerships that we do through our community grants and the internet connections we have with the Access for All program, and organizations. We work a lot with, and rely on those trusted ambassadors out in the community to help in the frontlines on the work. We will have another round this coming year on the Tech Matching Fund. If the Digital Navigators money passes, likely that as well. So, there are opportunities both to help outreach and increase awareness about these resources, like with the Low Income Internet programs, and encourage organizations to also apply for the funding for projects.

**Harte Daniels:**   When is the community wireless effort that was in IFA in partnership with UW. I think you were talking about UW, Jesse. There is a group of researchers who are trying to turn theirs into a not for profit, but I don't know where it sits in the IFA with the budget. Either Cara or David could answer that. They are trying pilot projects in sections of the City, or were, but I don't know about where they are in  the IFA, and the back and forth that's been going on.

**Jesse Moore:**   Yes, thanks for that, Harte. Because I think the University of Washington has an interesting network of WiFi that goes across everywhere. They support the whole K-12 and K-20 network for the whole State of Washington. So, all of the colleges, all of the K-12s, they give them bandwidth. You would be surprised to go down to Seattle and see WiFi on, and you see University of Washington WiFi all over the place, because the University of Washington is all over the place. They're wired everywhere. It's crazy. So, I would see maybe advising or some partnership there to be pretty fruitful for this kind of Internet for All, just because they have that kind of depth and breadth. They are also part of the internet backbone for the Pacific Northwest, as well.

**David Keyes:**   Yes, they have some terrific infrastructure there, and the work we are doing help with background and some connections. The current university WiFi, the only university I'm aware of in the City that provides free WiFi to folks, unless you're a student with an account, or a faculty member or staff, is Seattle University. The University of Washington and others do not. But as Harte mentioned, the Community Cellular Project or CERS, which is not strictly a WiFi project, but the community lab there is doing some great work. And recently, turned on their first cell system at the Filipino Community Center down in Rainier Valley. They're going to work on a couple more. We funded them this year through the Solidarity Budget and had requested specific money for that project. And that's not in the budget. Cara can speak to that. We have been working with them and I know there are other applications to other funding sources that they're working on.

**Cara Vallier:**   And previously funded by TMF, I believe. It was independently funded to a large extent with a huge grant, which we were so happy to see. They would be eligible also for a TMF grant in the future, based on the type of work that they do. And so I do hope to see that go forward. But there wasn't anything specifically for that project in the hotspots, Digital Navigator, or TMF efforts that we proposed.

**David Keyes:**   Cara made one reference which was really exciting. We've been able to connect some of the sites we're using from the free internet connections that we negotiated for with Comcast and Wave, and more recently with Lumen Century Link, and so those connections, we've been trying to match that with the sites where community cell sites are going up to provide better bandwidth to those sites. So, that's really exciting.

**Rene Peters:**  Awesome discourse. They'll be great things to weave into our DEI work as a board, as well, and keeping updated with everybody who just chipped into that discourse. Glad to have folks like Jesse and Alex on the call to interact with folks like Cara and David. Thank you to all who have hung in there, as I have let this meeting go wildly off the rails. We were supposed to finish at 7:05. But, as you can see it is just so easy to get swept up in the spirit of community technology. One last note before we leave today. At the next meeting, our December meeting, which will be on the 14th, which is, coincidentally the latest possible second Tuesday we can have, that will be elections. We will have the chairship and the vice chairship opening up. And we will be nominating our leadership. We can do nominations at the meeting, but if you would like to nominate yourself or somebody else, send an email to us and add your email to the chat as well. [rjpjr@alum.mit.edu](mailto:rjpjr@alum.mit.edu) Email both of us if you would like to nominate yourself or somebody else, and do that before, ideally, December 1, just because we want to discourage surprise nominations in lieu of having a more understood field. If you're nominating someone else, the person who is nominating can just give some of their reasons in a few sentences. Each nominee during the meeting will be given time for a short speech, limited to about three minutes to outline their interests and their qualifications and their vision for CTAB in 2022. With that said, please put some thought to it, and if you're interested, let us know. That's the last announcement that I have for today.

**Harte Daniels:** I put my note in the chat on Understanding the Human Geographic Fabric of Neighborhoods webinar series. And I'd also like people to take time this Thursday to remember our veterans. This is National American Indian Heritage Month. To become familiar with everybody's history in our nation and the great contributions the First Nations People have made, both to our governance as well as the defense of our country. They did culturally volunteer more military service *per capita* than any other ethnic group. And they do it not for any economic reasons, but for cultural reasons, as they do see themselves as all of your protectors. So, please remember our veterans. This is the hundred year anniversary of the entombment of the unknown soldier. In 1921, they were going through the ending of a very bad war, and six million dead from a pandemic that we're going through right now. So, those two things. Remember the history, contributions of others, and remember our veterans this Thursday, please. <https://www.wwhgd.org/>

**Rene Peters:**  Thanks for sharing that, Harte, and I distributed the link to that web site at the top of the meeting. And there's some great resources that intersect both First Nations history and the military. So, thank you very much. Great note to end on. Everybody, enjoy the rest of your November. Again, contact me if you have self nominations or other nominations, and we will see you back here on December 14. Take care, everybody, and thank you again, Alex and Jesse.

**ADJOURNMENT**