Business

CEOs Pair Up for Gun Detection Technology

BY KARA C. RODRIGUEZ
krodriguez@loudounnow.com

Renss Greene/Loudoun Now

Telos CEO John Wood and Omnilert founder Ara Bagdasarian teamed up to launch a technology platform that detects the presence of guns and, they hope, prevents future mass shootings.

Telos CEO John Wood and Omnilert CEO Ara Bagdasarian developed a rapport and mutual respect for each other years ago as they worked on an initiative to boost Loudoun's nighttime economy. Now, the two have put their minds together to develop technology that could save lives.

Wood and Bagdasarian recently announced a partnership whereby the Telos Ghost visual obfuscation network is integrated into the Omnilert Gun Detect platform. They market it as the industry's first AI-powered visual gun detection solution.

Bagdasarian's Leesburg-based Omnilert was on the cutting edge of campus notification technology even before mass shootings became a tragically common headline. The company has since gone a step further, evolving "where AI meets the Internet of Things," he said. This means going beyond mass notifications to systems that allow doors to be locked with access control, or loudspeakers to be activated with notifications.

The marriage between the companies' technologies now takes it even a step further.

"We're protecting the IP address, Ara is protecting people's lives," Wood said. "On the one hand we're making sure adversaries can't hurt you from an internet point of view. Ara's technology makes sure someone can't hurt you [physically]. It's the coming together of physical and logical security."

The way the technology works is that Omnilert Gun Detect alerts administrators to the presence of a gun on a camera. The administrators can then make a quick determination whether to activate real-time emergency plans, like sending notifications, locking doors, or alerting authorities. If something is detected that is not a threat, a child playing with a water gun, for instance, the administrator can let the system know the object is harmless.

"It's not only detecting a firearm, it's what happens after that," Bagdasarian said. "You can initiate entire actions in a matter of seconds. In a school or corporate setting, you're giving people a head start to seek shelter. You're summoning first responders and law enforcement within seconds rather than waiting until a shot is fired."

Bagdasarian harkens back to the February 2018 shooting at Marjory Stoneman Douglas High School in Parkland, FL that claimed the lives of 14 students and three school staff members.

"The gunman exposed the gun in the stairwell and there was a camera and it was captured [on video]. Had things been different, can you imagine if the gun was detected when he pulled it out of his backpack?" he said.

Where Ashburn-based Telos' technology comes into play is via its ghost network.

"What we do as a company in general is we protect the cloud, the enterprise. We do cybersecurity for people. More and more what's happening is that people are realizing that computers are not computers anymore—computers are cars, HV/AC systems, cameras. All of those have IP addresses that are hackable. From our point of view, we want to protect the IP process of all these things, the Internet of Things. When I saw what Ara has, it's not a big leap to go from protecting your network and people's identities, to actually protecting people full stop. For me, it was sort of a natural extension to what we do," Wood said.

Wood and his team at Telos actually borrowed a technological breakthrough used in World War II to create its ghost network—signal hopping, where military members would change radio frequencies to avoid enemy detection. With Telos' ghost network, instead it is IP hopping. When someone signs in to the ghost network at Telos, the IP address may first appear as Ashburn, VA, but then could quickly change to somewhere in Europe, for example, and then another global location every few seconds.

"Unlike all of those other kinds of solutions that are out there that try to do missed attribution or obfuscation, the ghost doesn't leave a trail. The adversary can't hack back. The adversary cannot paint a target on a customer. Cameras can be enabled right away using Gun Detect to outwardly protect those customers as well. Embedding Ghost and embedding Gun Detect in other solutions, that enables us to scale to a much bigger level," he said.

Both Wood and Bagdasarian note the technology can be relevant to any number of types of campuses, from schools and universities, to medical and business campuses, to law enforcement and government facilities, and more. The two sadly note that mass shootings are no longer limited to workplaces or schools and news this week of a mass shooting at a Boulder, CO, grocery store makes that all the more apparent.

The duo both express optimism over the partnership and how it can help protect people and networks globally.

"It all started here in Loudoun," Wood said. "It is something that we're both very proud of."

"It's nice to do something locally and make a global impact," Bagdasarian added. ■

Announcements

NVCC, Equinix Launch Infrastructure Scholarship

With the data center industry projected to need 300,000 new hires by 2025, Equinix is teaming up with the Northern Virginia Community College Educational Foundation and the college's Financial Aid Office, to create the Equinix Digital Infrastructure Scholarship program.

"The data center industry is growing rapidly, and with that comes a high demand for skilled talent. We are excited to work with Northern Virginia Community College to provide an early career path to inspire the next generation of data center professionals on building the world's digital infrastructure at Equinix," said Chris Kimm, Equinix SVP of Americas IBX Operations.

The program provides the framework for students to enter the data center industry through the school's Engineering Technology Career Studies Certificate programs. Equinix will support five students with scholarships of $5,000 each.

"In the Northern Virginia region, we have seen great employment spikes in this sector, and it is gratifying to be able to offer students a paid and direct pathway into this important field," said Kelly Persons, executive director of the NOVA Foundation.

In addition to the financial benefit, eligible candidates will have the opportunity to register for mentorships and paid internships at Equinix. The application period is open for graduating high school seniors interested in entering the NOVA Engineering Technology program. The scholarship will be awarded in May for classes in the fall or next year.

The Equinix Digital Infrastructure Scholarship and many others are listed on NOVA's scholarship website at nvcc.academicworks.com.

Thomas Joins CapRelo as Senior VP

CapRelo has hired mobility executive Jennifer Thomas as senior vice president of business development.

Thomas reports to CapRelo Presi-

ANNOUNCEMENTS
continues on page **16**

LoudounNow

VOL. 6, NO. 31 We've got you covered. In the mail weekly. Online always at LoudounNow.com JULY 1, 2021

Independence Day celebrations started early in Loudoun, with Hillsboro putting on a concert and fireworks show Sunday. The first major Fourth of July celebration without COVID-19 pandemic restrictions brought out one of the biggest crowds the Old Stone School has ever seen for an afternoon of music, food trucks, local wine and beer, a reading of the Declaration of Independence, a performance of the National Anthem by Malcom Fuller, and a fireworks show.

—Renss Greene

The Digital Pandemic? Guarding Against Ransomware

BY KARA C. RODRIGUEZ
krodriguez@loudounnow.com

With the COVID-19 pandemic heading into the rearview mirror, security prognosticators are warning about a "pandemic" that could last considerably longer.

"This is a digital pandemic," said local security expert Morgan Wright, who currently serves as the chief security officer for Sentinel One. "It's spread beyond borders, it's global at this point and it's hurting everybody."

Ransomware attacks are nothing new. In fact, said Wright, they've been around about 15 years. But the phenomenon is on everyone's radar screen, at least on the East Coast, following the May Colonial Pipeline ransomware attack. In response, the oil refinery halted pipeline operations, creating a minor panic that quickly affected the East Coast gas supply.

"Colonial Pipeline was a watershed moment," Wright said. "This was criminal ransomware operating with the implicit approval of Russia that was able to attack and affect the critical infrastructure of the U.S. without crossing our borders. I do a lot of stuff for national and cable news. Some things are just a story here and now, and some things make the news cycle. This is one of the first times ransomware became part of the news cycle."

But a quick internet search shows that ransomware is much more prevalent than Colonial Pipeline or the Solar Winds' supply chain attacks of late 2020. Lately, everything from public school systems and universities to the New York City Subway and Martha's Vineyard Ferry, to unemployment offices, healthcare systems, even your run-of-the mill small business, have been the victim of a ransomware attack. Ransomware is quickly becoming its own industry, and more of a guaranteed get-rich-quick scheme that's as simple as reaching out to a site on the dark web. The industry is unfortunately fast-growing, doubling in 2020 following explosive growth in 2018 and 2019.

"In the last two-and-a-half years it went from kind of a marginal technique to being the number one problem, and it's costing people billions of dollars," said John Gilmore, the director of research for Abine, a data privacy company.

It's evolved from a simple consumer scam, where hackers convince members of the public to send them money via gift cards to pay fake outstanding fines, or purchase products that don't exist. Now, ransomware attacks can be highly complex.

"Unlike in the past, the people that wrote the ransomware code itself and the people doing the scam emails were all the same people. What happened in the last two years is that the industry has become specialized. The people that actually write the code are not the ones who execute the attacks," he said. "They can license the software to anyone that wants to use it, so you have this proliferation of potential attacks. It's a real franchise model. Criminal organizations are collecting money but don't have to attack anyone. It's a great way to make a

RANSOMWARE *continues on page* **38**

Ransomware

continued from page **1**

quick buck."

Another thing that has helped its growth is the move to more remote work since the onset of the COVID-19 pandemic, he added, and it's something to pay close attention to as the traditional workplace evolves.

"The fact that 80% of the public suddenly had to start working from home helped this spread. It was like a gift from heaven to all of these guys. Suddenly everybody was using private or web-based email with none of the protections of typical corporate email. Everyone was using cloud-based storage, sharing their password over Slack, and over chat, texting each other the Zoom password or VPN. That sort of thing suddenly allowed these guys to collect massive amounts of worker credentials. It became 100 times easier overnight," he said.

The rapid rise of ransomware and the more widespread use of bitcoin are inextricably linked, as the new form of currency helps to further anonymize its user.

"Ransomware is a problem because right now when ransomware is paid you often don't know who you're paying it to," said John Wood, CEO of Ashburn's Telos. "If you can't target or attribute where an attack is coming from it's very hard to figure out how to solve it."

There are several ways that ransomware attacks happen, the chance of which can be lessened if the private or public sector has its guard up. In the case of the Solar Winds attack, hackers got into the system due to a weak password.

"I would make the argument that for a software company, their source code server, which is arguably their most important asset, needs a really strong password," said Wood. "In the SolarWinds case it was solarwinds123. That's not a strong password."

Wood said user access control should be set at the highest level possible to avoid hackers accessing dormant accounts via malware. Multi-factor authentication is also a tool that should be used to guard against attacks.

Unpatched systems are also particularly vulnerable, Wright said, and that was Equifax's downfall for its 2017 data breach. Zero-day exploits that expose a security vulnerability can also make an organization an easy target for hackers. Traditional phishing, or spear phishing, is the method still favored by many nation states, he added.

By and large, hackers are looking for "low-hanging fruit" for easy access to disrupt systems and demand a ransom, Wood said. His advice is simple—practice good cyber hygiene by adopting the best cybersecurity practices throughout an organization.

Renss Greene/Loudoun Now

Jakub Jedrzejczak, Leesburg's director of information technology, has worked to keep the commonwealth's largest town guarded against ransomware threats by scheduling monthly training for the town's hundreds of employees.

Gilmore said he doesn't totally buy into the angle of communist countries working through digital pipelines to take down America's infrastructure. Instead, he believes the greater and more prevalent threat is hackers targeting small businesses.

"If you look at the data, 70% of all ransomware attacks have been happening to businesses with fewer than a thousand employees. Thirty percent are with less than a hundred employees. The vast bulk of what happens on a day-to-day basis is fairly lowball. The median payout is $70,000, but that's about double what it was a year ago. All we hear about in the media is big multi-million dollar, very damaging attacks on big corporate entities. The real story is it's a problem for small and medium businesses and it's growing very quickly," Gilmore said.

In addition to demanding a ransom payment that can have more sticker shock for a smaller organization than a larger institution, disrupting a business's systems could represent a far higher loss in income.

It's also a big problem for the public sector, he said. In the spring of 2018, a major ransomware attack on the City of Atlanta disrupted its payment software systems and compromised legal documents and police dashcam videos. Millions of dollars would be expended in the recovery effort. Countless other examples of state and local government systems being targeted have received mostly local media coverage over the years.

"People think of hackers targeting these organizations. That is not at all true. Organizations that are committing financial scams...they're opportunities. They throw out bots that scan for opportunities. Once they've infected a lot of organizations they look through and choose who is going to be the easiest, quickest payment. In most cases they do not want to hit a Colonial Pipeline, or big public organizations. They want it to be low profile," Gilmore explained.

The Commonwealth's largest town has not taken the prevalence of this type of news sitting down. Leesburg in recent years has invested heavily in an IT Strategic Plan, with a strong emphasis on robust cybersecurity measures. This investment is particularly remarkable because the county seat's funding for new staffing positions or new programs in its General Fund has been almost flat. But Leesburg looks to the all too frequent examples of other localities who allowed their cyber defenses to be weak, or out of date.

"One of the major things identified [in the strategic plan] was that we needed to invest in strong cybersecurity defenses, and we have set aside a significant amount of the budget to do that," said Clark Case, director of the town's Finance & Administrative Services Department. "A lot of that was building stronger infrastructure. That requires money, that requires updating systems and equipment as well, and investing in some services that make our cyber defenses stronger. There are a couple of staff positions that are designed to help us be better positioned to be better defended and more resilient."

It has been a costly, but necessary, investment, he added.

"We don't regard it as an enhancement; we regard it as essential base level spending that's being driven up by the cyber criminals. We can't afford not to. If you don't [invest in cybersecurity] you will be locked down, you will be unable to provide essential services. Our position has been to do a lot of planning and a lot of implementing of cybersecurity infrastructure. That's been our number one emphasis, but it's been expensive for the town," Case said.

Jakub Jedrzejczak came onboard as the town's director of information technology in the spring of 2019, and immediately placed a strong emphasis on cybersecurity, in concert with the strategic plan. He now runs monthly training for all of the town government's employees, across all departments.

"When I got this job two years ago, in the first month the training program was the number one foundational piece," he said. "I am personally a strong believer that in the IT office, we design everything around people, process and technology. You can't separate one and forget about one. You have to have people following the process using the right technology. That is really the foundation for cybersecurity."

Healthcare organizations are also a particularly vulnerable target, Gilmore said.

"By exploiting medical records, that's pretty much the best data for robocall scammers. They can sell medical data or they can use it themselves to do other sorts of mass attacks," he said.

Both of Loudoun's major hospital systems, Inova Health System and HCA's StoneSprings Hospital, largely declined to comment for this story. A statement provided by StoneSprings noted its investment and focus on the best security practices.

"StoneSprings Hospital Center has a number of robust security strategies, systems and protocols in place to help protect data. As you might imagine, not publicly discussing the details of our security measures is part of our overall protection strategy. Additionally, we follow federal, state and local requirements on reporting and notification," the statement read.

Wright said Loudoun's reputation as the global epicenter of Internet traffic makes the county a prime target for ransomware attacks. Hackers would love to take down a data center, he said, but acknowledged they tend to be armed with the highest and best cybersecurity systems and practices. While they may not have the budgets of a data center provider, both public and private sector organizations need to invest heavily to defend themselves against ransomware, he said. For those organizations that deal with public infrastructure, the investment needs to be the greatest.

"Companies need to spend proportionate to the threat they are facing," he said. "You pay someone in proportion to the job they do. You need to spend the same way according to the threat."

There needs to be greater collaboration among law enforcement, the intelligence community, the military, and the commercial world in combating ransomware attacks, Wood said.

"I'm seeing industries beginning to band together, even though they may compete at a high level. If they know this activity is occurring in [an] energy business, they've got to make sure all other energy businesses know this activity is happening. If they get hacked it's bad for the entire industry," he said. "It is causing alliances that in the past have not been quite there. I think these alliances are here to stay for some period of time."

The phenomenon is so widespread, Wright acknowledged, that taking out one cyber criminal organization will do little to topple the threat. The best offense is a great defense, security experts all agree.

"Ransomware is like cartels or criminal organizations. You might take out one, but it's like whack-a-mole. There's 10 more to take their place," he said. "We cannot arrest our way out of ransomware." ■

LoudounNow

VOL. 6, NO. 46 We've got you covered. In the mail weekly. Online always at LoudounNow.com OCTOBER 7, 2021

No Vax, No Job?

Employers and Employees Grapple with Vaccine Mandates

BY KARA C. RODRIGUEZ
krodriguez@loudounnow.com

As COVID-19 numbers began to decline locally, following a Delta variant that caused a spike in cases at the onset of the school year, many employers and employees are grappling with whether to institute, or abide by, a requirement to be fully vaccinated against the virus.

President Joe Biden announced in early September the largest-scale mandate to date—all federal employees and contractors must be fully vaccinated against COVID-19 by Nov. 22. The mandate will also extend to all private sector employers with more than 100 employees, with an option for weekly testing. The impacts of that mandate, with Loudoun a hotspot for federal workers and government contractors, has already begun its trickle-down effect.

It's coming at a time, Loudoun Chamber of Commerce President Tony Howard noted, when the job market is as competitive as ever, sparking an interesting tug and pull between employer and employee when termination in lieu of vaccination is the consequence.

"Employers are very reluctant to impose [a mandate] unless the government makes them do it because we're in such a war for talent nowadays," he said. "Some industry sectors really suffered [during the pandemic] and are still recovering;

VAX MANDATES *continues on page* **39**

Barts Recall Advances; Biberaj Disqualified from Case

BY HAYLEY BOUR
hbour@loudounnow.com

A Loudoun Circuit Court judge on Tuesday denied a motion to dismiss the voter petition to remove School Board member Beth Barts (Leesburg), and disqualified Commonwealth's Attorney Buta Biberaj from prosecuting the case.

Barts is facing a removal effort spearheaded by the group Fight for Schools. The group alleges that Barts' involvement in a private Facebook group violated open meeting laws and the School Board's Code of Conduct, among other charges.

During a four-hour hearing Oct. 5, Judge Jeanette Irby denied a motion to dismiss the pleadings on a technicality. Charlie King, the attorney for Barts, argued that the verbiage in the petitions did not make it apparent enough to signees that they were agreeing to grievances against Barts, under penalty of perjury. Irby said it was clear to petitioners that by signing, they were affirming the allegations.

Renss Greene/Loudoun Now

Fight for Schools Executive Director Ian Prior and some of the group's supporters celebrates victory in the first test of Barts removal petition in court.

She also denied a separate motion to dismiss the pleadings based on a claim that Fight for Schools lacked standing to intervene in the case. King argued that the only named parties in the case are the commonwealth and the defendant, and intervention they the activist group was not appropriate.

In ruling that Biberaj should be removed from the case, Irby said that her decision was based on a perception issue because the public might not trust Biberaj's impartiality.

"I have the utmost respect for Ms. Biberaj … however if she continued on this case there would never be acceptance on this case," Irby said.

The attorney for Citizens of Leesburg, the plaintiff in the case, David Warrington presented a tweet by Biberaj, in which

BARTS RECALL *continues on page* **11**

Vax mandates

continued from page **1**

others are doing quite well and are struggling to find talent. You don't want to impose something on employees that would risk any brain drain."

Howard, like others, noted that there are several factors in play for both imposing, and abiding by, such a mandate. Most who have imposed mandates allow exceptions for medical reasons or religious beliefs. Others offer the option of weekly testing and/or abiding by other COVID-19 safety protocols for those employees who choose to forego a vaccine.

The Chamber president himself recently imposed a vaccine requirement for his 11-person staff, who returned to the office in June following a 14.5-month closure during which the work completely remotely. He also announced in late August that the Chamber would require attendees at its in-person, indoor networking and educational events to be fully vaccinated, or show proof of a negative COVID test taken within 48 hours of the event.

Howard said he was expecting much more pushback from Chamber members and even his board of directors on the policy than he ultimately received. The policy led only to a "handful" of Chamber members leaving the organization.

"In the single digits," he said. A number, he said, that was "dwarfed by the number of folks who thanked me for adopting the policy."

Vaccine mandates locally have not always been so warmly received. Vocal resistance was heard during last week's Leesburg Town Council meeting, when three Leesburg Police officers spoke up at a meeting and said many officers would leave the town force if the council went through on a vaccine mandate it was discussing for town employees.

Should Leesburg go through on enforcing such a mandate—a council majority favored a 90-day timeline for complying with the mandate, with no option for weekly testing—the officers warned the town could lose a sizable portion of its sworn officers.

Officer William Butterfield said the vaccine mandate would cause the department to have an even harder time attracting and retaining good officers, at a time when police departments nationwide are having difficulties hiring employees. He noted what the town would be losing if he left town employ, pointing to all the money Leesburg has invested in him as a member of the police department's bike team and SWAT team, in addition to other certifications.

"I think we're all big boys, grown adults, that can make decisions for ourselves," he said.

Both Butterfield and Officer Josh Carter, who also spoke against the mandate during the Sept. 28 meeting, declined to be interviewed for this article.

Should the Town of Leesburg move forward with a vaccine mandate—with discussion expected to continue at the council's meetings next week—it would join Loudoun County government, which has imposed a vaccine mandate for its thousands of employees. Loudoun's constitutional officers also have the option to join.

Of the county's top 10 largest employers, at least seven have mandated COVID-19 vaccines for their employees or are subject to Biden's federal mandate. Included in that number is the county's largest healthcare provider, Inova Health System, which was the first hospital system in the commonwealth to mandate vaccines for its employees.

All of the healthcare system's employees, including its contractors and remote workers, had to have their first dose of the COVID-19 vaccine by Sept. 1 and their second dose by Oct. 1, according to hospital spokesperson Renee Brohard. Of the healthcare system's thousands of employees throughout the region, 89 chose not to comply with the requirement and were terminated, she said. That number represents 0.4% of the system's workforce. There was no option for employees to receive weekly testing in lieu of a vaccine.

Fellow Loudoun hospital system HCA StoneSprings has not mandated vaccines for its employees, although many of them have voluntarily opted to be vaccinated, said Suzanne Kelly, StoneSprings Hospital's director of marketing and communications.

"While at this time StoneSprings Hospital has not required its colleagues to be vaccinated for COVID-19, the majority of StoneSprings Hospital colleagues are fully vaccinated. StoneSprings Hospital helps ensure a safe environment by following guidance from the Centers for Disease Control and Prevention (CDC) as well as the Occupational Safety and Health Administration (OSHA). Inside our hospitals and other care settings, we continue to have universal protections in place requiring all staff in all areas to wear masks regardless of vaccination status. That includes requiring them to wear all recommended PPE, including N95 respirators, when caring for those with confirmed or suspected COVID-19 infection. In our non-care settings, we require unvaccinated staff to wear a mask," Kelly said in a prepared statement.

The county, for its part, has expanded its twice-a-month COVID-19 testing events to weekly, beginning Tuesday, Oct. 12.

The drive-through events are scheduled for Tuesdays from 10 a.m. to 1 p.m. at alternating locations across the county.

"I encourage anyone who thinks they may have been exposed to COVID-19 to get evaluated and tested promptly, either privately or through one of the county's testing events," Loudoun County Health Director Dr. David Goodfriend said. "You should get tested if you are exhibiting symptoms of COVID-19, such as fever or chills, cough, shortness of breath, fatigue and a new loss of taste or smell or if you have been potentially exposed to someone with COVID-19, regardless of their vaccination status."

Goodfriend advised that while waiting for COVID-19 test results, "you should stay home and away from others if you have symptoms of COVID-19, regardless of your vaccination status; or if you have had close contact with someone with COVID-19 and you are not fully vaccinated."

The testing events will move around to different locations each week, rotating among Claude Moore Park in Sterling, Philip A. Bolen Memorial Park near Leesburg and Franklin Park in Purcellville.

While, as of yet, local vaccine mandates have not led to widespread terminations or resignations, one local place of worship is providing a form letter for residents to document their religious objections to the vaccine. Cornerstone Chapel in Leesburg states on its website that it does not have an official stance on the COVID-19 vaccine but provides those with "personal and legitimate religious objections to a vaccine mandate" to use a PDF letter to provide to employers. The letter cites several Bible passages in making the case for a religious exemption.

"I am responsible to God for my body—how I treat it, how I use it, how I take care of it, and what I put into it. My body is considered a 'sacred temple' that is devoted to God for sacred purposes. I am to honor God with my body. It would be dishonoring to God for me to put something into my body for which I had a conscientious objection. Therefore, on religious grounds I believe I would be violating a sacred trust to honor God with my body if I were to allow the COVID vaccine to be injected into my body," the letter reads in part.

The letter also provides a section for an optional pastoral signature. Cornerstone Chapel Pastor Gary Hamrick did not respond to a request to be interviewed for this story.

To see the schedule of free testing events and other places to get tested, visit loudoun.gov/covid19testing. Visit vaccines.gov to find places to get vaccinated. ■

Energy strategy

continued from page **4**

a climate crisis based on energy emissions, and Loudoun County is through the roof right now."

While Loudoun's government has quietly been making its facilities greener for years, with measures such as energy-efficient buildings and lighting, County Chair Phyllis J. Randall (D-At Large) said the Loudoun County government should lead by example—and that it's hard to ask the business community to do things that the government hasn't invested in itself.

"When I said government by example, what I meant is, there are some things that we're asking the community to do but we're not doing yet ourselves, [electric vehicle] charging stations being a great example," Randall said.

And a big part of tackling the climate change problem even locally will be finding ways to fund the solutions.

"It costs money on the front end to do energy efficient things," Randall said. "It saves money on the back end, but it costs money from the front end, and how does that work, and what's the financing, how soon can that money be returned—and all those issues."

Supervisor Michael R. Turner (D-Ashburn) compared some current solutions to rearranging deck chairs on the Titanic.

"Not to put too fine a point on it, but we'll get what we're getting now," Turner said. "I think if this is going to be meaningful, we really need to step up the game in a major, exponential way, and let's not kid ourselves: it's going to cost us money." And he said emissions from transportation and the built environment will be "the key to the game."

But supervisors also all agreed that they will need much more information to make any policy decisions, such as which of those decisions would have the most impact.

"I think that it can't be only carrots, to be frank," Briskman said. "I think that we are going to need something in our zoning ordinance rewrite that addresses these issues."

For next steps, county staff members will conduct more research on the feasibility and cost of different strategies and begin work to draft a new energy plan. They are expected to bring that work back to the Board of Supervisors for further discussion in mid-2022. ■