Regulators deal a blow to Nev. rooftop solar industry

By Daniel Rothberg, Las Vegas Sun

With no discussion, state regulators this week voted unanimously to slash the value of credits rooftop solar customers earn for generating excess energy.

The three-member Public Utilities Commission adopted a proposed order that would reduce by 75 percent the amount NV Energy pays customers for excess power their solar panels produce and change the flat service rate for customers with solar panels. The changes in so-called net metering policies would phase in over four years, starting Jan. 1.Regulators deal a blow to rooftop solar industry

The PUC's position in the order is that higher bills are being paid by nonsolar users to provide "hidden subsidies" for those with solar panels. The PUC said solar users in Southern Nevada have been getting an annual subsidy of about $623. The subsidy for solar users in Northern Nevada is about $471.

Read the whole story

EPA wants toxic Nevada mine on Superfund list

By Scott Sonner, AP

Fifteen years after U.S. regulators started assessing damage and health risks at an abandoned Nevada copper mine, the

Environmental Protection Agency is moving to add the contaminated site to its Superfund National Priority List, according to documents obtained by the Associated Press.

Rural neighbors of the World War II-era mine that has leaked toxic chemicals for decades won a $19.5 million settlement in 2013 from companies they accused of covering up the contamination – some of it radioactive – near Yerington about 65 miles southeast of Reno.

The EPA sent a letter to Gov. Brian Sandoval this week announcing the agency's intention to place the mine on the list of the nation's most polluted sites to "mitigate exposures that are a substantial threat to the public health or welfare or the environment."

Nevada has opposed past EPA proposals to list the site based on fears about the impact on property values, as well as any precedent that could be set by federal intervention in the mining-friendly state that is the world's sixth-biggest producer of gold.

But earlier this year, the Nevada Division of Environmental Protection estimated it would cost $30.4 million to address only what EPA considers the most immediate health and safety concerns, and the state has been unsuccessful in obtaining financial assistance from those responsible for the damage.

Under the Superfund listing scenario, the EPA would cover 90 percent of the costs.

"Without an identifiable private source of funding, the only mechanism to make federal funding available is to add the site to the NPL," said Jared Blumenfeld, the EPA's regional administrator in San Francisco, using the acronym for the Superfund's National Priority List.

"If we do not receive a written response from the state by Jan. 29, we will assume that Nevada is in agreement with EPA

and will proceed with proposing the site for addition to the NPL," he wrote in the Dec. 22 letter obtained by AP.

Aides to Sandoval had no immediate comment.

The class-action lawsuit filed in 2011 accused Atlantic Richfield Co. and its parent company, BP America Inc., of "intentionally and negligently" concealing the extent of uranium, arsenic and other pollutants leaking into their drinking water wells from the mine covering 6 square miles of land owned partly by the U.S. Bureau of Land Management.

Atlantic Richfield acquired the property in 1977 from Anaconda Copper, which built the mine in 1941.

Previous owners left behind 90 million gallons of acidic solution that continues to threaten the groundwater, Blumenfeld said. That's equivalent to the amount of liquid it would take to cover about 80 football fields, 10-feet deep.

In 2008, a U.S. Labor Department review panel upheld a whistleblower claim by ex-mine cleanup supervisor Earle Dixon who said the Bureau of Land Management illegally fired him for speaking out about the risks in defiance of local politicians who tried to muzzle him.

Peggy Pauly, a Yerington minister's wife, helped organize efforts to demand additional cleanup and filed the lawsuit joined by about 700 past and present neighbors.

"She's the real hero in all of this," said Steven German, a New York-based attorney who represented the residents.

"This is an important next step in getting this massive old mine cleaned up," he told AP Wednesday. "It is going to cost a fortune."

Anaconda produced 1.7 billion pounds of copper from 1952 to 1978 at the mine in the Mason Valley, an irrigated agricultural oasis in the otherwise largely barren high

desert. The EPA determined the uranium was produced as a byproduct of processing the copper and that the radioactive waste was initially dumped into dirt-bottomed ponds that – unlike modern lined ponds – leaked into the groundwater.

EPA studies showed 79 percent of the wells tested north of mine had dangerous levels of uranium or arsenic or both that made the water unsafe to drink, including one a half-mile away with levels more than 10 times the legal drinking water standard.

At the mine itself, wells tested as high as 100 times the standard. Although the health effects of specific levels are not well understood, the EPA says long-term exposure to high levels of uranium in drinking water may cause cancer and damage kidneys.

Ritz-Carlton elevates s'mores to a higher level



Homemade marshmallows raise s’mores at the Ritz-Carlton Lake Tahoe to gourmet status. Photo Copyright 2015 Carolyn E. Wright

By Kathryn Reed

TRUCKEE – Charred. That’s how the chef likes her marshmallows.

Daniella Rinaldi prepares about 2,000 of these gooey squares each week at the Ritz-Carlton Lake Tahoe. Then guests turn them into s’mores.

Rinaldi likes when hers catch fire. That’s what happens when the stick stays static. To get an even golden hue it requires constant turning. Then the inside is totally melted.



Pastry Chef Daniella Rinaldi says marshmallow trays must rest for 12 hours before they can be cut. Photo Copyright 2015 Carolyn E. Wright

These are no ordinary marshmallows. Egg whites, sugar, corn syrup, water and gelatin never tasted so good. To this taste tester it seemed like the difference was more than the flavorings. What that extra might be the pastry chef was keeping a secret.

Over the massive gas fire pits on the back patio of the resort hotel guests are invited each day at 4:30 to partake in a free s'mores extravaganza. (If others show up, they won't be turned away.) Often there is a line before the first marshmallow is speared and set on fire. Each day a flavored marshmallow and

regular one are available.



The fire pit beckons people to come make a s’mores each afternoon at the Ritz. Photo Copyright 2015 Carolyn E. Wright

One outing was not enough for Lei Mikawa and Isreal Nahsohn of Napa. They saw the platter of s’mores ingredients at check-in and made a beeline to the fire pit. The fun of roasting the marshmallow brought them back another afternoon.

They are typical of the usual crowd – adults seem to have more fun; it’s nostalgic for them.

Eleven chairs surround the fire – ideal for hanging out, getting warm or partaking in the fun. While the logs are fake and fire is produced by gas and not wood, the marshmallow doesn’t know the difference.



All the fixings for gourmet s'mores. Photo Copyright 2015 Carolyn E. Wright

The flavors change with the season and the ingredients available. In summer Rinaldi's inspiration comes from the resort's garden – fresh herbs like mint and tarragon are used. At Halloween she created Frankenstein flavor and pumpkin spice.

For *Lake Tahoe News* she shared bubble gum – which was exactly like eating a piece of bubble gum. The blue marshmallow is a hit with kids – adults are a bit more discerning. It brought back memories of when bubble gum ice cream was a favorite.

The vanilla bean lacks that distinct vanilla flavor, and instead tastes more like a regular marshmallow.

The ginger snap is like taking a spoonful of molasses – outstanding if you like that flavor.

The chocolate mint was bursting with flavor. The only problem is the marshmallow is brown so it was more difficult to know exactly when it was done roasting.



The finished product. Photo Copyright 2015 Carolyn E. Wright

Ritz employees – one who is called a marshmologist – are at the ready to help turn the marshmallow into a s'mores. Pieces of Hershey's chocolate are on graham crackers waiting for the hot gooeyness to complete it.

S'mores stands for some more. Credit is given to the Girl Scouts for creating the marshmallow, chocolate, graham cracker treat; with kudos to Loretta Scott Crew for coming up with the combo in the 1920s. They are so popular that there is now a National S'Mores Day – Aug. 10.

Snowpack exceeds average for first time in years



Kirkwood received so much snow earlier this week that when the roads were closed employees spent the night at the resort. Photo/Provided

By Bettina Boxall, Frank Shyong and Joseph Serna, Los Angeles Times

A series of powerful snowstorms in the Sierra Nevada has resulted in a small milestone in drought-stricken California: The snowpack is now higher than average for this time of year.

The storms, which are likely to continue into Friday, have fattened the mountain snowpack to levels California hasn't seen for two years, said Steve Nemeth, water supply forecaster for the state Department of Water Resources.

The announcement was welcome news to a state that has struggled with extremely dry conditions for more than four years. However, experts were quick to point out thatCalifornia's drought is far from over.

Statewide, the snowpack is 111 percent of average for the date. In the northern Sierra, it is 116 percent of the norm; in the central Sierra, 121 percent of average and in the southern Sierra, 85 percent of the norm.

Read the whole story

Sinatra’s old Tahoe casino to reopen in May

By Dale Kasler, Sacramento Bee

Frank Sinatra’s fans celebrated his 100th birthday earlier this month, but there was something missing from the festivities: the Cal Neva Resort & Casino, the Lake Tahoe hotel once owned by the legendary entertainer.

The Cal Neva, closed for renovations since September 2013, was scheduled to reopen on the late singer’s 100th birthday, Dec. 12.

But construction has taken longer than expected, and now the venerable north shore property is set to reopen next May 26 with an international hotel operator in charge.

Read the whole story

Field needs to be built to keep SnowGlobe

By Kathryn Reed

The rush this fall to have the documents signed to create the Community Play Consortium had a lot to do with money. Money in regards to the three-day SnowGlobe music festival that starts Tuesday, money from Lake Tahoe Community College's facility's bond, money to be spent on **future fields** and the potential income they will generate.

When talks of creating the consortium started early this year it was uncovered that the deeds for the properties from more than a decade ago were never recorded properly. That has all been rectified.

The parcels include the old Caltrans right-of-way that the California Tahoe Conservancy obtained after the transportation department decided not to build a freeway there, South Lake Tahoe land, LTCC property and a floating acre Lake Tahoe Unified School District has contributed on which a baseball field will be it. It's all in the area of the current community play field in South Lake Tahoe. The old Caltrans parcel is now the city's. Half of the playfield is on it, the other half of the playfield is owned by the college.

The city and LTCC transferred easements to the consortium, not land ownership. Therefore the consortium controls the use of that field and the future fields that are planned to be adjacent to the current one.

The college and city make up the consortium. **LTUSD chose** not to be a part of it.



This will be the last year SnowGlobe uses LTCC's synthetic turf field. Photo Copyright 2014 Carolyn E. Wright

"SnowGlobe was always part of the conversation because the college, city and school district wanted to make sure whoever owns the land that they were properly insured," City Manager Nancy Kerry told *Lake Tahoe News.*

Alcohol sales at SnowGlobe have been one of the issues for the parties to deal with.

"It was not a major factor, but it was a factor," LTUSD Superintendent Jim Tarwater told *Lake Tahoe News* as to why the district is not in the consortium. "I am not a real supporter of SnowGlobe, but will do whatever the community supports."

The district, as is the norm for most K-12 institutions, has a zero tolerance policy for drugs and alcohol on its grounds.

The college has policies in place as well regarding alcohol, but they are more flexible. To get around alcohol being sold

on campus the beer booths have always been on city property – on the asphalt on the mountain side of the set up. The consumption, well, that is allowed everywhere.

“If the field is under the control of the consortium, under the easements our laws don’t apply. That is part of the reason why we were working so hard when we realized the easements were not in effect so SnowGlobe could take place this year,” Kindred Murillo, LTCC president, told *Lake Tahoe News.*

Chad Donnelly, SnowGlobe founder and promoter, did not return *LTN*’s call asking how big of a deal alcohol sales are for the three day event that runs Dec. 29-31.

“We don’t have restrictions about selling alcohol. What the city can’t do is make money off alcohol sales,” Kerry said. “The nonprofits that work with SnowGlobe get a percentage of the alcohol sales.”

This will be SnowGlobe’s final year on the field where Lake Tahoe Community College’s soccer team plays. That is because the college intends to replace that field next year at a cost that is likely to exceed $1.6 million.

The money in part will come from the college, and part from the city via Measure S/R dollars.

“We are looking at a pretty high quality synthetic field. We are looking at some of new techniques that do not off gas,” Murillo said. “That is under investigation, to put in the latest and best and most safe field. That field is so hard and off gassing. We believe it really needs to be replaced as soon as possible.”

Talks are under way with Tahoe Regional Planning Agency to begin work before the May 1 opening of construction season so the field would be ready for the soccer teams in August.

In order to invest bond money into the new field, the college

has to have “reasonable use of that property for the life of the investment,” Murillo said. This means the college’s athletic department and all other programs get first priority on that field.

The city next year is looking to build a field next to it that will be sod. It would be a secondary field and where SnowGlobe could go in the coming years. The city and Donnelly have a three-year contract, with this being year two.

Donnelly was asked what he thought about having to come up with a new configuration, but he chose not to answer that question.

The college is likely to provide parking lots for future SnowGlobes. As to whether anything else would be used is up for negotiation.

“Once we build the new field it will be a better location (for SnowGlobe),” Kerry said. “It will be natural. You can’t damage it like synthetic.” She envisions the possibility of vendors and foot traffic going on the new synthetic field.

That will be up to the consortium – not the college. And right now it’s just the college and city in the consortium.

Reno airport files complaint against U.S. Customs

By Jane Kane, Reno Gazette-Journal

Officials with the Reno-Tahoe International Airport are decrying the treatment of a 15-year-old girl by U.S. Customs and Border Protection agents at the airport when she

flew to Reno from Guadalajara, Mexico in November and was allegedly detained, questioned for five hours and unable to contact family.

On Monday, Reno-Tahoe Airport Authority board chairman Andy Wirth and Marily Mora, the president and CEO of the airport, said they filed a formal complaint on Dec. 16 against the federal agency. Both Wirth and Mora said they have been hearing from the local Hispanic community since this summer about alleged mistreatment by federal border protection agents at the airport, which added the direct flight to Mexico about a year ago.

“She was coming to visit her family for the holidays and was treated in a way that should not be tolerated in our airport, our community or in our country,” Wirth said of the 15-year-old girl, whose identity is being withheld by the airport because she is a minor. “The treatment she received was appalling on every level and deeply disconcerting.”

Frank Falcon, a spokesman for Customs and Border Protection in San Francisco, said he had not heard of the situation in Reno until a reporter called him on Monday.

Airport officials noted that they have been receiving complaints of the customs process in Reno since late summer this year.

Read the whole story

Low water level allows pipe removal at Tahoe



Boy Scouts take the initiative to remove a pipe from shores of Lake Tahoe. Photos/Devin Middlebrook

Publisher's note: *This was first published in Tahoe In Depth and is reprinted with permission.*

By Devin Middlebrook

The low water level at Lake Tahoe is the starkest reminder of the current drought, with piers and marinas reaching out over sand and rocks that are normally hidden from view.

But sand and rocks are not the only objects being exposed by the drought.

Near Tahoe City, a long-abandoned, cast-iron pipe sat just below the surface for decades, having only the occasional run-in with a boat propeller or kayaker. Installed in the early

1900s, the pipe originally delivered drinking water to Tahoe Tavern from Watson Lake to the north. With the receding lake level, the pipe, now strewn along the shoreline, was visible to all that visited the area.

That is where Eagle Scout candidate Cyrus Miller, 16, and the rest of Boy Scout Troop 228 from Danville decided to step in. With a large section of the pipe now exposed, the troop wanted to take advantage of the situation.

“This drought made it a unique and once-in-a-lifetime opportunity,” Miller said. “We wanted to complete a project that made a big impact.”



The beach with the exposed pipe.

With this goal in mind, Miller and his troop developed a plan to remove the pipe and return the area to a more natural state. Working closely with local agencies – Tahoe Regional Planning Agency, California Fish and Wildlife Service, California Division of State Lands, Placer County Museums, property owners, NV Energy, Tahoe Tavern, and Tavern Shores – the troop created a comprehensive plan for safely removing the pipe.

Using a few power tools and a lot of determination, the seven scouts cut the lengthy pipe into manageable sections. They then removed these smaller sections from the lakebed.

The sections were hauled away and recycled with a little help from Hansen Management & Maintenance Company of Tahoe City. The scouts then cleaned the project area, making it as though the pipe was never there.



The beach with the pipe removed.

Over the two-day project, the scout troop removed 700 feet of pipe from the lakebed.

At the end of day two, Miller looked over the project area and said, “It is amazing how much of an impact our troop’s hard work made.”

Several pieces of the pipe were donated to the Placer County Museum; where they will live on to tell the story of Lake Tahoe and its rich history.

Devin Middlebrook is an environmental education specialist with the Tahoe Regional Planning Agency.

Sierra’s cat on the prowl to perfect riders’ experience – especially in terrain parks



Sierra has a four-year lease on its snowcats so the fleet doesn’t get too old. Photos/Kathryn Reed

By Susan Wood

TWIN BRIDGES – It’s not your grandfather’s Bombardier.

That’s the impression of Sierra-at-Tahoe’s new addition to its terrain park grooming fleet – the Prinoth Tier 4 Bison X. The workhorse of a machine runs smoothly like a Cadillac, but acts like it has the conscience of a Tesla electric car when it comes to protecting the environment, an underlying goal the ski resort 12 miles west of Meyers has focused on for years.

Benny McGinnis, Sierra's terrain park manager, has welcomed the new member of the family of 12 grooming machines – some of which like this Bison are geared for the terrain parks. The $200,000 machine comes equipped with more torque, more features and more fuel efficiency – while throwing out fewer emissions. As numbers go, it emits 90 percent less in noxious fine particles compared to past generations, according to McGinnis' fact sheet.

The output is right in line with Lake Tahoe's environmental movement.

And if wondering why else this machine is important, one need only look at what in recent winters had not been falling from the sky in Tahoe to understand. California is coming off four years of unprecedented drought. If not for reliable and capable grooming machines and their operators, the ski seasons would not have lasted as long as they did. They can save a season. Think of it this way, in drought, there's only so much snow that can go around.



Benny McGinnis is a veteran snowcat driver at Sierra specializing in terrain park

work.

“In the wake of the drought, efficiency is key. That means efficiency in on-mountain operations – the way we move and preserve snow and also efficiency in environmental practices. This cat gives us the chance to accomplish all of those while continuing to create progressive terrain parks,” spokeswoman Thea Hardy told *Lake Tahoe News.*

Progressive terrain parks are breeding grounds for Olympians.

In 2014 Sierra was celebrating the cultivation of three Olympic gold medalists – Maddie Bowman, Jamie Anderson and Hannah Teter. There’s a reason they ski and board here.

“The terrain park has definitely influenced Jamie Anderson in becoming the huge athlete she is today,” said McGinnis, a 14-year veteran terrain park builder who operates heavy machinery for the U.S. Forest Service in the summer months. In winter though, it’s all about Sierra – and all its users.



Drivers sit in the middle of

the cab with a slew of controls at their fingertips.

The Prinoth machine has a smaller cab than older models while maintaining the track size. That helps it maneuver more easily – especially at the “take offs” and “landings” associated with terrain parks.

“I like that this job gives me the opportunity to create something and to let a normal person come up and feel like an Olympic athlete. Tourists want to come up and get out of their lifestyle – to speed up or to slow down, and be an athlete,” McGinnis told *Lake Tahoe News.*

The Prinoth groomer, clad on the outside with a camouflage design, has more than 30 possibilities to manipulate the tiller and blade through a joystick attached to a panel that resembles an airplane. The blade can even pick up terrain park features.

This machine also provides more visibility with heated wipers and larger windows as well as more comfort for the operator with a Bluetooth sound system and heated seats. McGinnis admitted operators might get work fatigue just like a plane pilot or even someone who operates a computer for eight hours. His crew of six machine operators works two shifts encompassing between eight to 10 hours, the latter if the ski area gets dumped on. The job requires 80 hours of training.

Some are set in their ways and like to stick to the older machinery. But the handful of terrain park builders like the challenge of the new toy. All like to create a culture that embodies play.

“These cats are expensive to run. If we’re not managing the business responsibly, then we as a culture we love can’t exist,” he added as if a poet.

Call them poets of the night, writing the fate of the mountain

slopes the next day.

——

Notes:

What else is new at Sierra-at-Tahoe this year?

· The Learn-to-Ride program is enhanced for all ages wanting to try their hands and feet on the Burton Backhill snowboard design.

· The addition of a safety program called Helmets are Cool has come on board.

· The WiFi has been beefed up in the base area, so guests will be able to connect with family members and friends more easily.

U.S. not prepared for power grid cyberattack

By Garance Burke and Jonathan Fahey, AP

Security researcher Brian Wallace was on the trail of hackers who had snatched a California university's housing files when he stumbled into a larger nightmare: Cyberattackers had opened a pathway into the networks running the United States power grid.

Digital clues pointed to Iranian hackers. And Wallace found that they had already taken passwords, as well as engineering drawings of dozens of power plants, at least one with the title "Mission Critical." The drawings were so detailed that

experts say skilled attackers could have used them, along with other tools and malicious code, to knock out electricity flowing to millions of homes.

Wallace was astonished. But this breach, the Associated Press has found, was not unique.

About a dozen times in the last decade, sophisticated foreign hackers have gained enough remote access to control the operations networks that keep the lights on, according to top experts who spoke only on condition of anonymity due to the sensitive nature of the subject matter.

The public almost never learns the details about these types of attacks — they're rarer but also more intricate and potentially dangerous than data theft. Information about the government's response to these hacks is often protected and sometimes classified; many are never even reported to the government.

These intrusions have not caused the kind of cascading blackouts that are feared by the intelligence community. But so many attackers have stowed away in the systems that run the U.S. electric grid that experts say they likely have the capability to strike at will.

And that's what worries Wallace and other cybersecurity experts most.

"If the geopolitical situation changes and Iran wants to target these facilities, if they have this kind of information it will make it a lot easier," said Robert M. Lee, a former U.S. Air Force cyberwarfare operations officer. "It will also help them stay quiet and stealthy inside."

In 2012 and 2013, in well-publicized attacks, Russian hackers successfully sent and received encrypted commands to U.S. public utilities and power generators; some private firms concluded this was an effort to position interlopers to act in

the event of a political crisis. And the Department of Homeland Security announced about a year ago that a separate hacking campaign, believed by some private firms to have Russian origins, had injected software with malware that allowed the attackers to spy on U.S. energy companies.

“You want to be stealth,” said Lillian Ablon, a cybersecurity expert at the RAND Corporation. “That’s the ultimate power, because when you need to do something you are already in place.”

The hackers have gained access to an aging, outdated power system. Many of the substations and equipment that move power across the U.S. are decrepit and were never built with network security in mind; hooking the plants up to the Internet over the last decade has given hackers new backdoors in. Distant wind farms, home solar panels, smart meters and other networked devices must be remotely monitored and controlled, which opens up the broader system to fresh points of attack.

Hundreds of contractors sell software and equipment to energy companies, and attackers have successfully used those outside companies as a way to get inside networks tied to the grid.

Attributing attacks is notoriously tricky. Neither U.S. officials nor cybersecurity experts would or could say if the Islamic Republic of Iran was involved in the attack Wallace discovered involving Calpine Corp., a power producer with 82 plants operating in 18 states and Canada.

Private firms have alleged other recent hacks of networks and machinery tied to the U.S. power grid were carried out by teams from within Russia and China, some with governmental support.

Even the Islamic State group is trying to hack American power companies, a top Homeland Security official told industry executives in October.

Homeland Security spokesman SY Lee said that his agency is coordinating efforts to strengthen grid cybersecurity nationwide and to raise awareness about evolving threats to the electric sector through industry trainings and risk assessments. As Deputy Secretary Alejandro Mayorkas acknowledged in an interview, however, “we are not where we need to be” on cybersecurity.

That’s partly because the grid is largely privately owned and has entire sections that fall outside federal regulation, which experts argue leaves the industry poorly defended against a growing universe of hackers seeking to access its networks.

As Deputy Energy Secretary Elizabeth Sherwood Randall said in a speech earlier this year, “If we don’t protect the energy sector, we are putting every other sector of the economy in peril.”

The attack involving Calpine is particularly disturbing because the cyberspies grabbed so much, according to interviews and previously unreported documents.

Cybersecurity experts say the breach began at least as far back as August 2013, and could still be going on today.

Calpine spokesman Brett Kerr said the company’s information was stolen from a contractor that does business with Calpine. He said the stolen diagrams and passwords were old – some diagrams dated to 2002 – and presented no threat, though some outside experts disagree.

Kerr would not say whether the configuration of the power plants’ operations networks – also valuable information – remained the same as when the intrusion occurred, or whether it was possible the attackers still had a foothold.

According to the AP investigation, the hackers got:

- User names and passwords that could be used to connect remotely to Calpine's networks, which were being maintained by a data security company. Even if some of the information was outdated, experts say skilled hackers could have found a way to update the passwords and slip past firewalls to get into the operations network. Eventually, they say, the intruders could shut down generating stations, foul communications networks and possibly cause a blackout near the plants.
- Detailed engineering drawings of networks and power stations from New York to California – 71 in all – showing the precise location of devices that communicate with gas turbines, boilers and other crucial equipment attackers would need to hack specific plants.
- Additional diagrams showing how those local plants transmit information back to the company's virtual cloud, knowledge attackers could use to mask their activity. For example, one map shows how information flows from the Agnews power plant in San Jose near the San Francisco 49ers football stadium, to the company headquarters in Houston.

Wallace first came across the breach while tracking a new strain of noxious software that had been used to steal student housing files at the UC Santa Barbara.

"I saw a mention in our logs that the attackers stored their malware in some FTP servers online," said Wallace, who had recently joined the Irvine-based cybersecurity firm Cylance Inc., fresh out of college. "It wasn't even my job to look into it, but I just thought there had to be something more there."

Wallace started digging. Soon, he found the FTP servers, typically used to transfer large numbers of files back and forth across the Internet, and the hackers' ill-gotten data – a tranche of more than 19,000 stolen files from thousands of computers across the world, including key documents from

Calpine.

Before Wallace could dive into the files, his first priority was to track where the hackers would strike next – and try to stop them.

He started staying up nights, often jittery on Red Bull, to reverse-engineer malware. He waited to get pinged that the intruders were at it again.

Months later, Wallace got the alert: From Internet Protocol addresses in Tehran, the hackers had deployed TinyZbot, a Trojan horse-style of software that the attackers used to gain backdoor access to their targets, log their keystrokes and take screen shots of their information. The hacking group, he would find, included members in the Netherlands, Canada, and the United Kingdom.

The more he followed their trail, the more nervous Wallace got. According to Cylance, the intruders had launched digital offensives that netted information about Pakistan International Airlines, the Mexican oil giant Pemex, the Israel Institute of Technology and Navy Marine Corps Intranet, a legacy network of the U.S. military. None of the four responded to AP's request for comment.

Then he discovered evidence of the attackers' most terrifying heist – a folder containing dozens of engineers' diagrams of the Calpine power plants.

According to multiple sources, the drawings contained user names and passwords that an intruder would need to break through a firewall separating Calpine's communications and operations networks, then move around in the network where the turbines are controlled. The schematics also displayed the locations of devices inside the plants' process control networks that receive information from power-generating equipment. With those details, experts say skilled hackers could have penetrated the operations network and eventually

shut down generating stations, possibly causing a blackout.

Cylance researchers said the intruders stored their stolen goods on seven unencrypted FTP servers requiring no authentication to access details about Calpine's plants. Jumbled in the folders was code that could be used to spread malware to other companies without being traced back to the attackers' computers, as well as handcrafted software designed to mask that the Internet Protocol addresses they were using were in Iran.

Circumstantial evidence such as snippets of Persian comments in the code helped investigators conclude that Iran was the source of the attacks.

Calpine didn't know its information had been compromised until it was informed by Cylance, Kerr said.

Iranian U.N. Mission spokesman Hamid Babaei did not return calls or address questions emailed by AP.

Cylance notified the FBI, which warned the U.S. energy sector in an unclassified bulletin last December that a group using Iran-based IP addresses had targeted the industry.

Whether there was any connection between the Iranian government and the individual hackers who Wallace traced – with the usernames parviz, Alireza, Kaj, Salman Ghazikhani and Bahman Mohebbi – is unclear.

Cyberattacks designed to steal information are steadily growing in scope and frequency; there have been high-profile hacks of Target, eBay and federal targets such as the U.S. Office of Personnel Management. But assaults on the power grid and other critical infrastructure aim to go a step further.

Trained, well-funded adversaries can gain control of physical assets – power plants, substations and transmission equipment.

With extensive control, they could knock out the electricity vital to daily life and the economy, and endanger the flow of power to mass transportation, military installations and home refrigerators.

In summer 2014, a hacker of unknown origin, using masking software called Tor, took over the controls of a large utility's wind farm, according to a former industry compliance official who reviewed a report that was scrubbed of the utility's name. The hacker then changed an important setting, called the automatic voltage regulator, from "automatic" to "manual," he said.

That seemingly simple change to any power plant can damage the generator and destabilize parts of the nearby grid if the plant's output is high enough.

Last year, Homeland Security released several maps that showed a virtual hit list of critical infrastructure, including two substations in the San Francisco Bay area, water and gas pipelines and a refinery. And according to a previously reported study by the Federal Energy Regulatory Commission, a coordinated attack on just nine critical power stations could cause a coast-to-coast blackout that could last months, far longer than the one that plunged the Northeast into darkness in 2003.

"The grid is a tough target, but a lucrative target," said Keith Alexander, the former director of the National Security Agency who now runs a cybersecurity firm. The number of sophisticated attacks is growing, he said. "There is a constant, steady upbeat. I see a rising tide."

No one claims that it would be easy to bring down the grid. To circumvent companies' security, adversaries must understand the networks well enough to write code that can communicate with tiny computers that control generators and other major equipment. Even then, it's difficult to cause a widespread

blackout because the grid is designed to keep electricity flowing when equipment or lines go down, an almost daily occurrence that customers never see.

Because it would take such expertise to plunge a city or region into darkness, some say threats to the grid are overstated – in particular, by those who get paid to help companies protect their networks. Still, even those who said the risks of cyber threats can be exaggerated agree it is possible for cyberattackers to cause a large-scale blackout.

Traditional central power stations and transmission systems include equipment that is decades old and physically unable to handle electronic threats. Some run on machines that use software that is so old that malware protections don't exist, such as Windows '95 and FORTRAN, a programming language developed in the 1950s.

At the Tennessee Valley Authority, a corporation owned by the federal government that powers 9 million households in the southeastern U.S., a former operations security expert said in recent years he saw passwords for some key operating systems stored on sticky notes.

"Some of the control systems boot off of floppy disks," said Patrick Miller, who has evaluated hydroelectric dam cybersecurity for the U.S. Bureau of Reclamation and Army Corps of Engineers. "Some dams have modeling systems that run on something that looks like a washing machine hooked up to tape spools. It looks like the early NASA stuff that went to the moon."

The rush to tie smart meters, home programmable thermostats and other smart appliances to the grid also is causing fresh vulnerabilities.

About 45 percent of homes in the U.S. are hooked up to a smart meter, which measures electricity usage and shares information with the grid. The grid uses that information to adjust output

or limit power deliveries to customers during peak hours.

Those meters are relatively simple by design, mostly to keep their cost low, but their security is flimsy. Some can be hacked by plugging in an adapter that costs $30 on eBay, researchers say.

FERC recently raised concerns about another area that is not covered by federal cybersecurity rules: contractors that sell energy companies software and equipment. As is evident from the Calpine incident, attackers have used outside companies to pull off hacks against energy companies.

“We’ve got these vulnerable systems out there that are old and never had security built into them, and now we’re exposing them to a wider audience,” said Justin Lowe, a utility cybersecurity expert at PA Consulting Group.

“That wider audience is getting much more hostile.”

The full extent of the attacks on the grid is not public knowledge. A Freedom of Information Act request by the AP for information regarding any FBI investigations of such hacks was not fulfilled. The Department of Justice said that agency kept no record of how often any such cases had been prosecuted.

The North American Electric Reliability Corporation, which oversees the reliability of the electrical sector, collects information about cyber incidents involving utilities and other users, owners, and operators of the bulk power system — but it is scrubbed of identifying information and details are confidential and exempt from disclosure under FOIA.

Authorities say they take the threat seriously. In response to a FOIA request, Homeland Security said it had helped more than 100 energy and chemical companies improve their cyber defenses, and held both classified and unclassified briefings in June 2013 and late 2014 on threats to companies associated with power grid operations.

A small DHS team compiles statistics about hacks and vulnerabilities on control systems powering the grid and other public infrastructure, and responds to some attacks. But former federal employees who spoke on the condition of anonymity because the information was sensitive said government red tape kept the team from thoroughly responding to the smaller municipal and rural utilities that most needed their help, and that the statistics overstated the agency's grasp of the problem.

The companies themselves say they are vigilant – though they caution no fortifications are foolproof.

Early this year, an operations supervisor in Virginia for a subsidiary of American Electric Power – the nation's largest power grid operator, with operations in 38 states – opened a personal email on a company laptop and unwittingly downloaded a piece of malware called CryptoLocker.

Known as "ransomware," CryptoLocker is a relatively common type of malware that reaches to outside servers, usually overseas, and downloads encryption instructions that scramble a computer's contents, making them inaccessible to anyone without a specific "key." The malware then moves through a computer – and computer network – and encrypts all the files it can, keeping users from accessing anything.

In exchange for a fee, the hackers provide the victim a key that allows the files to be unlocked.

Members of AEP's cyber-security team – housed in the company's Columbus, Ohio, headquarters behind an unmarked door that unlocks with a fingerprint scanner – saw the strange network behavior as soon as it started.

"When you see this (code) attempting to hit thousands of systems outside of the AEP network, that's a 'holy crap' moment," said Sean Parcel, AEP's lead cyberinvestigator.

Had CryptoLocker wormed its way into AEP’s system, the business and operations networks could have locked up, experts say.

But Parcel said AEP’s cyberteam already had blocked the foreign addresses that the malware needed to reach to start encrypting files, part of a policy of systematically blocking hundreds of Internet Protocol addresses each week to keep employees from inadvertently downloading malicious code.

AEP said the team remotely isolated and erased the supervisor’s computer before its systems were affected.

Like most big utilities, AEP’s power plants, substations and other vital equipment are managed by a network that is separated from the company’s business software with layers of authentication, and is not accessible via the Internet. Creating that separation, and making sure that separation is maintained, is among the most important things utilities can do to protect the grid’s physical assets.

But cybersecurity experts say the protective gaps between computer systems that manage utilities’ business operations and machines that manage their grids are not always as wide or as unbridgeable as utilities say they are. And even the utilities’ own experts, who maintain it would be extraordinarily difficult for a hacker to knock out power to customers, admit there is always a way in.

“If the motivation is high enough on the attacker side, and they have funding to accomplish their mission,” Parcel said, “they will find a way.”