



Department of Homeland Security

Daily Open Source Infrastructure Report for 24 December 2008

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)
<http://www.dhs.gov/>

- According to the Los Angeles Times, federal inspectors said Monday that they will ratchet up scrutiny of the San Onofre nuclear plant in California after discovering that a battery meant to power safety systems had been inoperative for four years. (See item [4](#))
- The Washington Post reports that a massive underground pipe rupture on Tuesday in Montgomery County, Maryland, flooded a road with 4 feet of water, trapping motorists and blocking a major commuter artery. (See item [17](#))

DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: [Energy](#); [Chemical](#); [Nuclear Reactors, Materials and Waste](#); [Defense Industrial Base](#); [Dams](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#); [Information Technology](#); [Communications](#); [Commercial Facilities](#)

Sustenance and Health: [Agriculture and Food](#); [Water](#); [Public Health and Healthcare](#)

Federal and State: [Government Facilities](#); [Emergency Services](#); [National Monuments and Icons](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: **Physical:** ELEVATED, **Cyber:** ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *December 22, Insurance Journal* – (Oklahoma) **Damage from industrial fire at Oklahoma port estimated at \$500k.** Tulsa, Oklahoma, fire officials say initial damage estimates after a raging industrial fire at a petroleum recycling facility at the Tulsa Port of Catoosa may be close to a half-million dollars. A fire captain says they managed to limit the environmental impact at the port after the December 19 blaze. He says specialized absorbing buoys were placed in the river to contain any petroleum products from spreading outside the port. More than three dozen firefighters responded to the Safety-Kleen Systems fire to battle the petroleum fire, which also was fueled by a ruptured natural gas line. After the gas was shut off, he says firefighters were able to get the remaining flames under control fairly quickly.

Source: <http://www.insurancejournal.com/news/southcentral/2008/12/22/96528.htm>

2. *December 22, Abilene Reporter-News* – (Texas) **Big Spring refinery owner fined in February fire.** The Occupational Safety and Health Administration recently fined Alon USA \$52,275 for violations in connection with the February 18 fire at the company's Big Spring refinery. The blast, centered at the propylene splitter, injured five people, including one passer-by. An incident investigation by Alon indicated liquid propylene was released through a rupture in one of the pumps located at the propylene splitter unit and reached an ignition source, according to a statement from the refinery manager. He said the pump was installed in 1978. The rupture in the pump was caused by a poor weld on the bottom of the pump case, officials said in a statement. The refinery manager said in the statement that the refinery is in the process of implementing recommendations to inspect other pumps in the refinery as a result of the incident. Source: <http://www.reporternews.com/news/2008/dec/22/big-spring-refinery-owner-fined-in-february-fire/>

[\[Return to top\]](#)

Chemical Industry Sector

3. *December 22, WOWK 13 Belle* – (West Virginia) **Chemical leak poses no immediate hazard, says Dupont.** The director of emergency services for Kanawha County says phosphoric acid leaked in the water treatment area of the Dupont plant in Belle on Monday. Officers with the Department of Environmental Protection (DEP) and DuPont are investigating the leak. Dupont confirms approximately 4,800 gallons of 35 percent phosphoric acid spilled when a tank leaked. A large portion of the spill was contained in the storage tank dike; however, some product leaked into the ground and the nearby Kanawha River. There are no immediate environmental concerns to people who work at the plant or live nearby, but the DEP will continue to monitor the situation. Source: <http://wowktv.com/story.cfm?func=viewstory&storyid=48836>

[\[Return to top\]](#)

Nuclear Reactors, Materials, and Waste Sector

4. *December 23, Los Angeles Times* – (California) **San Onofre nuclear plant under tighter federal scrutiny.** Federal inspectors said Monday they will ratchet up scrutiny of the San Onofre nuclear power plant after discovering that a battery meant to power safety systems had been inoperative for four years. Plant personnel discovered in March that bolts connecting an emergency battery to a circuit breaker were loose, a problem the U.S. Nuclear Regulatory Commission attributed to poor maintenance. The commission said that the twin-reactor plant near San Clemente, run by Rosemead-based Southern California Edison, remains safe, and that other backup batteries are functioning. But the commission expressed concern that the battery problem had gone unnoticed from 2004 to 2008. Apart from the battery, the commission discovered seven additional safety flaws that it described as minor in themselves — including poor documentation and inconsistent follow-up on potential problems — but that taken

together formed a troubling picture. As a result, the commission issued a “white finding,” characterized as a low- to moderate-level safety concern, and said it will step up inspections at San Onofre until it sees improvements. In a news release, Edison said it accepted the commission’s findings and promised to ramp up “the rigor needed in problem identification and resolution.”

Source: <http://www.latimes.com/news/printedition/california/la-me-nuclear23-2008dec23,0,4905009.story>

5. *December 22, KPTV 12 Portland* – (Oregon) **Truck carrying radioactive load crashes.** A semitrailer that was carrying a low-level radiation load jackknifed and crashed on Interstate 84 Monday afternoon in La Grande, Oregon. No one was hurt when the commercial semitrailer lost control, jackknifed, went off the road, and collided with a rock wall, Oregon State Police said. Oregon troopers, Oregon Department of Transportation workers, and the La Grande Fire Department’s regional hazmat team responded to the scene, police said. The hazmat team found that there had been no breach of the container with the unidentified load.

Source: <http://www.kptv.com/news/18340417/detail.html#->

[\[Return to top\]](#)

Defense Industrial Base Sector

6. *December 23, WIRED* – (National) **New missile kills air defenses dead.** Soon after radar-guided anti-aircraft missiles became a threat, planners realized that the simplest way to stop them was to take out the radar. The problem with this type of missile is that it relies on the enemy radar being turned on: enemy operators can turn off the radar so it has nothing to home in on. All that changes when a High Speed Antiradiation missile (HARM) is fitted with a Global Positioning System (GPS) module that allows it to accurately pinpoint the location of the radar emitter. The addition means that even if the radar turns off, the missile can still hit it precisely. Raytheon’s upgrade is called HDAM, for HARM Destruction of Enemy Air Defenses Attack Module. It is being built for the Air Force. And it incorporates both GPS and an inertial measurement unit with a fiber-optic gyro. Raytheon will not say exactly how accurate it is, but unlike other anti-radiation missiles which rely on a shrapnel warhead, HDAM has achieved “metal on metal” hits on radar targets, both emitting and non-emitting. And they can target more than radar. The GPS guidance also means that the upgraded missiles can be programmed to hit a precision target from sixty miles away, making HARM the only high-speed air-to-surface weapon in the inventory. This gives it obvious utility against fleeting, time-critical targets.

Source: <http://blog.wired.com/defense/2008/12/new-missile-kil.html>

7. *December 23, Navy Times* – (National) **U.S. Navy orders 8 new subs.** As expected, the U.S. Navy announced on December 22 a contract to buy eight new Virginia-class submarines. The new group of subs is referred to collectively as Block III. Previous Virginia-class submarines were authorized in two groups of five subs each. Eighteen submarines of the class are in service, under construction, on order, or authorized, with a total of 30 planned. The Block III submarines will be the first of the class to be fitted

with the Virginia Payload Tubes (VPT), a development of the modified former ballistic missile launch tubes in the Ohio-class converted cruise missile subs. Two VPTs in the bow of each of the new submarines will replace 12 vertical launch tubes used for Tomahawk cruise missiles in previous submarines and can hold six cruise missiles. The new subs also will feature the Large Aperture Bow (LAB) Array of sound-detection gear. Experts said the LAB Array provides improved passive listening capability over traditional spheres using transducers. The Navy claims the LAB Array and VPTs, along with more than two dozen other modifications, shaved \$40 million per submarine. The general manager of the Newport News shipyard said that the agreement “brings stability to the submarine program, to our work force and to the shipbuilding supplier industrial base for the next decade.”

Source: http://www.navytimes.com/news/2008/12/military_subcontract_122308/

[\[Return to top\]](#)

Banking and Finance Sector

8. *December 22, Times-Picayune* – (Louisiana) **Telephone scam cons 450 in Jefferson Parish of credit card information.** More than 450 residents have received telephone calls from credit card scammers who used phony automated messages to con victims out of account information over the weekend, a spokesman for the Jefferson Parish Sheriff’s Office said. And it seems the scam has gone national, with reports of similar mass messages left on the telephones of residents in Atlanta, Georgia; Richmond, Virginia; and Dallas, Texas according to a spokesman for the Jefferson Parish Sheriff’s Office. The sheriff issued a formal warning about the scam Sunday. As of Monday morning, investigators had found only 14 people who actually gave up personal information. The calls apparently began as early as Thursday night. The scammers would dial up home telephones and even wireless phones and play a recorded message from a person purporting to be from the Jefferson Parish Sheriff’s Office, the Jefferson Parish Federal Credit Union, or a security firm, according to authorities and victims.

Source:

http://www.nola.com/news/index.ssf/2008/12/telephone_scam_cons_450_in_jef.html

9. *December 22, San Jose Mercury News* – (California) **Key Fry’s executive arrested in alleged \$65 million fraud scheme.** A one-time computer salesman who rose through the ranks to help build Fry’s Electronics into a robust national retailer is facing allegations that he defrauded the San Jose-based company out of \$65 million. The 42-year-old, who has been Fry’s vice president of merchandising and operations, appeared in federal court Monday, where prosecutors filed a complaint that alleges he was involved in a “secret kickback scheme to defraud Fry’s Electronics of millions of dollars.” Fry’s executives did not know about the illegal kickbacks, the federal complaint states. The alleged scheme occurred from 2005 until mid-October when a Fry’s high-level employee walked into the defendant’s office and saw confidential spreadsheets, letters, and extraordinarily high commission amounts on the defendant’s desk. The defendant is expected to be formally charged in U.S. District Court on January 15, on counts of money-laundering and wire fraud.

Source:

http://www.insidebayarea.com/oaklandtribune/localnews/ci_11290239?source=rss

10. *December 22, Associated Press* – (Massachusetts) **Subway fare hackers to partner with transit agency.** A trio of Massachusetts Institute of Technology students who found a way to hack into the Boston subway system’s payment cards have agreed to partner with transit officials there to make the system more secure. The Electronic Frontier Foundation announced the agreement Monday, two months after the Massachusetts Bay Transportation Authority (MBTA) dropped a lawsuit against the students. The students have argued all along they were trying to help the MBTA by giving it advance notice of their planned talk last summer and keeping specific details of their hack secret. But the MBTA worried of widespread fare fraud if students discussed how they were able to add hundreds of dollars in value to MBTA’s two primary payment cards.

Source:

http://tech.yahoo.com/news/ap/20081222/ap_on_hi_te/techbit_subway_hack

[\[Return to top\]](#)

Transportation Sector

11. *December 23, Associated Press* – (Colorado) **Investigators: Doomed jet made odd noise.** Investigators trying to determine why a Continental Airlines plane veered off a runway and skidded into a ravine heard an odd bumping and rattling noise on the flight’s recorders shortly before it tried to take off. The noise was detected 41 seconds after the jet started speeding down a runway at Denver International Airport on Saturday. Four seconds later, one of the crew members called for the takeoff to be aborted, said a spokesman for the National Transportation Safety Board. Experts planned to begin a more in-depth analysis of the contents of the flight recorders in Washington, D.C., on Tuesday while investigators return to the plane’s wreckage in a snowy field at the airport. Investigators have found no problems with the plane’s engines, tires, or brakes, but they are not yet ruling anything out.

Source: <http://www.msnbc.msn.com/id/28330517/>

12. *December 22, Dallas Morning News* – (New York) **DOT wants to limit LaGuardia operations.** The Transportation Secretary proposed Monday that airlines voluntarily limit takeoffs and landings at New York LaGuardia Airport to an average of 71 an hour, down from the current 75. “Too many flyers know that LaGuardia’s delays are the worst of the worst, and we want to use every tool at our disposal to help passengers stuck with this grueling congestion,” the Secretary said in a statement. A federal judge has temporarily prevented the Department of Transportation’s attempt to reduce the number of operations at LaGuardia, New York Kennedy, and Newark by taking slots away from existing holders. The DOT’s plan was to kill some of the slots and redistribute other slots to new entrants into those airports. But the Secretary argued that something needs to be done until the legal dispute is settled, since LaGuardia regularly ranks last among 32 large airports in on-time arrivals. In October, only 75 percent of LaGuardia’s flights arrived on time, worst among 32 airports tracked.

Source: <http://aviationblog.dallasnews.com/archives/2008/12/dot-wants-to-limit->

[laguardia-o.html](#)

[\[Return to top\]](#)

Postal and Shipping Sector

13. *December 22, Army.mil* – (Texas) **NG team responds to suspicious package.** Camp Mabry, Texas, was added to the growing list of National Guard installations Wednesday to receive a suspicious package through the mail. Under the oversight of the Federal Bureau of Investigation and the Austin Police Department Bomb Squad, the 6th Civil Support Team responded to a request to remove and analyze two suspicious packages received by the Armed Forces Reserve Center. Since December 12, more than 50 packages with anti-war compact discs have been discovered at National Guard facilities around the country, said a spokesman for the National Guard. The Mobile Analytical Lab System was used to analyze the packages. Three other Texas National Guard installations received similar packages. One was delivered to the 149th Fighter Wing at Lackland Air Force Base in San Antonio, another found at the 136th Airlift Wing in Fort Worth, and a third at the 147th Reconnaissance Wing in Houston. These packages were analyzed in similar fashion and determined to be nonhazardous, officials said.

Source: <http://www.military.com/news/article/army-news/ng-team-responds-to-suspicious-package.html?col=1186032369115>

[\[Return to top\]](#)

Agriculture and Food Sector

14. *December 23, Xinhua News* – (International) **Fresh outbreak of bird flu detected in Bangladesh.** A fresh outbreak of bird flu has been detected in Bangladesh. Authorities have so far culled nearly 10,000 chickens in five districts, a senior government official said. The director of Bangladesh's Fisheries and Live Stock Department told Xinhua on Tuesday, "We have detected avian influenza, known as H5N1, in four commercial farms and a household in five districts so far this month." "Some 9,950 birds of the farms and the household and nearby areas of the country's western Natore, central Gazipur, eastern Narsingdi, and northern Gaibandha and Kurigram districts were culled this month," he said. He said his department has yet to confirm the sources of fresh attacks of the disease, "but it may be due to germs of bird flu remained as we faced a huge outbreak last winter."

Source: http://news.xinhuanet.com/english/2008-12/23/content_10549045.htm

15. *December 23, USAgNet* – (Minnesota; Wisconsin) **Alfalfa sprouts recalled after tests turn up contamination.** A Wisconsin-based sprout grower has notified their customers to remove their alfalfa sprouts and certain sprout mixes from store shelves after routine food safety tests by the Wisconsin Department of Agriculture turned up positive for Salmonella, a bacteria that can cause food-borne illness. Sunrise Farms, Inc. of Neenah is recalling their packaged Alfalfa Sprouts, Spicy Sprouts, Crunchy Sprouts, and Onion Sprouts. These sprouts and sprout mixes are sold in four-ounce packages at grocery

stores and retailers throughout Wisconsin and Minnesota. The other sprout mixes produced by Sunrise Farms are not part of the recall. At this time, there have been no reports of illness. The company is working closely and cooperatively with the department's Food Safety Division to determine how these sprouts became contaminated.

Source: <http://www.usagnet.com/story-national.php?Id=2973&yr=2008>

16. *December 22, Packer* – (California) **California gears up for latest fruit fly fight.** The well-oiled fruit fly eradication machine of the California Department of Food and Agriculture is in operation again after a Mexican fruit fly infestation was discovered near the Los Angeles suburb of Azusa. A female Mexican fruit fly was trapped December 8. Expanded trapping was initiated and three more flies have been found, said the director of public affairs for the state agency. As part of the campaign to eradicate the infestation, a 70 square-mile quarantine area has been established, he said. The prevalence of Mediterranean fruit flies in the 1990s led the Department of Food and Agriculture to introduce the sterile program as an exclusionary measure. The preventative release program has minimized the number of fruit fly introductions, he said. At least 6.5 million sterile Mexican fruit flies are scheduled for release weekly over the core of the quarantine zone beginning December 22. The quarantine requires that residents in the quarantine area not move homegrown fruits and vegetables from their property. Landscape nurseries may not move host plants out of the area. The closest commercial crops to the quarantine area are the citrus groves and a few avocado orchards in San Bernardino County, about 40 miles east of Azusa.

Source: <http://www.thepacker.com/icms/dtaa2/content/wrapper.asp?alink=2008-153954-613.asp&stype=topnews&fb>

[\[Return to top\]](#)

Water Sector

17. *December 23, Washington Post* – (Maryland) **Motorists rescued after massive water main break.** In Montgomery County, Maryland, a massive underground pipe rupture flooded River Road with 4 feet of rapidly swirling water Tuesday morning, trapping motorists and blocking a major commuter artery. The break caused “widespread water outages” in school buildings across lower Montgomery County, officials said, affecting the heating system in some cases as well. More than 100 customers were without water, a spokesman for the Washington Suburban Sanitary Commission said. He said the rupture did not affect the safety of the county water supply. The 66-inch water pipe burst shortly before 8 a.m., sending a 4-foot wall of water onto River Road in Bethesda and trapping 15 people in about a dozen vehicles. The spokesman said the depth and speed of the current made it too dangerous for workers to reach the site where the 44-year-old pipe had ruptured and turn off the valve. Instead, workers had cut the supply from the Potomac Filtration Plant to reduce the amount of water flowing through the pipe, which is a direct line from the plant. They had located two valves up the line from the break and were trying to close them in order to stop the water entirely, he said. The flow had subsided substantially by 11:30 a.m. There was no initial information on why the large pipe might have ruptured, but age and extreme weather are often factors in

such breaks.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2008/12/23/AR2008122300847.html?hpid=topnews>

[\[Return to top\]](#)

Public Health and Healthcare Sector

18. *December 23, Associated Press* – (California) **SoCal hospital employee accused of ID theft.** Officials at Cedars-Sinai Medical Center in Los Angeles say more than 1,000 patients have had personal information taken by a former employee, who is alleged to have used the identities to steal from insurance companies. In a letter written to affected patients last week, the hospital's chief financial officer warned that their information had been found during a search of the home of the suspect, who had been an employee of the billing department.

Source: <http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2008/12/23/state/n023725S89.DTL&type=science>

19. *December 22, Center for Infectious Disease Research and Policy* – (National) **FDA approves shortened anthrax-vaccine course.** The U.S. Food and Drug Administration (FDA) recently approved a new version of BioThrax — the nation's only licensed anthrax vaccine — that requires fewer doses and changes the injection route. Emergent BioSolutions, maker of BioThrax, said in a press release that the FDA's approval of the company's supplemental biologics license application for its anthrax vaccine adsorbed allows a new schedule for the vaccine: five intramuscular doses compared with the previous regimen of six subcutaneous doses. The vaccine is required for U.S. military members who are deployed to the Middle East.

Source: <http://www.cidrap.umn.edu/cidrap/content/bt/anthrax/news/dec2208anthrax-jw.html>

[\[Return to top\]](#)

Government Facilities Sector

Nothing to report

[\[Return to top\]](#)

Emergency Services Sector

20. *December 22, Newspaper Tree El Paso* – (International) **A review of border haz-mat awareness.** U.S. and Mexican officials are well aware of the potential for catastrophic accidents and/or massive environmental contamination along their common border. Consequently, preventing and preparing for such events has slowly but steadily emerged as a focus of joint cross-border environmental initiatives since the signing of the 1983 La Paz environmental agreement between Mexico and the United States. By 2008, 15 local sister city agreements, with the support of Washington and Mexico City,

were signed to provide mutual assistance in the event of hazardous materials emergencies. According to the director of the Environmental Protection Agency office in El Paso, the voluntary agreements call for “table-top” exercises, or simulated disasters, in which emergency responders on both sides of the border contact each other by phone in a predetermined chain of notification, as well as actual emergency drills involving first responders from both sides of the border. On the emergency response front, unequal levels of training, funding, and technological access are key considerations, the Good Neighbor Environmental Board chair asserted. “In order to properly protect U.S. citizens, we need to make sure that Mexican communities have excellent training and equipment to deal with emergencies like chemical spills,” he said.

Source: <http://www.newspapertree.com/news/3234-a-review-of-border-haz-mat-awareness>

21. *December 22, Hanover Evening Sun* – (Pennsylvania) **Responders say new 911 radios flawed.** The York County, Pennsylvania, 911 center is booting up a new dispatching system after problems with first responder radios. Those problems — such as lost or garbled transmissions — have some county fire chiefs frustrated. Radios have had to be re-programmed several times, chiefs say. According to the Hanover Fire commissioner, the Hanover Fire Department’s portable radios have been sent back twice for re-programming and now a representative from M/A-Com will be coming to Hanover to program the radios a third time. The department has also not yet received mobile radio units. The installation, which includes setting up software, erecting tower equipment, and replacing portable radios, concludes with a “cut-over,” during which agencies switch from the old analog system to the new digital system. The radio issues have pushed back the cut-over date more than once.

Source: http://www.eveningsun.com/ci_11288166

[\[Return to top\]](#)

Information Technology

22. *December 22, IDG News Service* – (International) **Microsoft warns of SQL attack.** Just days after patching a critical flaw in its Internet Explorer browser, Microsoft is now warning users of a serious bug in its SQL Server database software. Microsoft issued a security advisory late Monday, saying that the bug could be exploited to run unauthorized software on systems running versions of Microsoft SQL Server 2000 and SQL Server 2005. Attack code that exploits the bug has been published, but Microsoft said that it has not yet seen this code used in online attacks. Database servers could be attacked using this flaw if the criminals somehow found a way to log onto the system, and Web applications that suffered from relatively common SQL injection bugs could be used as stepping stones to attack the back-end database, Microsoft said. Desktop users running the Microsoft SQL Server 2000 Desktop Engine or SQL Server 2005 Express could be at risk in some circumstances, Microsoft said. The bug lies in a stored procedure called “sp_replwritetovarbin,” which is used by Microsoft’s software when it replicates database transactions. It was publicly disclosed on December 9 by SEC Consult Vulnerability Lab, which said it had notified Microsoft of the issue in April.

Source:

http://www.pcworld.com/businesscenter/article/155940/microsoft_warns_of_sql_attack.html

23. *December 22, Network World* – (International) **Small laptops pose big threat.**

Ultraportable laptops come with built-in compromises. Security weaknesses are directly attributable to the machines' diminished technology. "This is a threat that IT managers are just beginning to recognize," says a security analyst at Lazarus Technologies Inc. Minimized hardware resources force ultraportables to cope with weakened system software. Most models ship with a stripped-down Linux operating system or, in some cases, Microsoft Corp.'s previous-generation operating system, Windows XP. Newer and more capable operating systems, which also tend to have the latest internal security safeguards, demand processing and storage power that ultraportables typically lack, the analyst notes. Ultraportables' reduced resources also limit their ability to run add-on security software, such as data encryption and anti-malware tools. With processing power, internal memory, and storage space all at a premium, it can be difficult — sometimes impossible — to squeeze security software onto an ultraportable. "As a result, the machines are often sent out into the world with little or no protection," he says. Other key security features are often absent on ultraportables. "Many, if not most, [ultraportables] are sold without Trusted Platform Modules because they are targeted at the consumer market," says an analyst at Enderle Group in San Jose. "This means they either don't have encryption solutions or the solutions aren't that robust." Enderle also notes that most ultraportables are not designed to be managed centrally and therefore cannot have their solid-state drives remotely wiped clean of data in the event of loss or theft.

Source: <http://www.networkworld.com/news/2008/122208-small-laptops-pose-big.html?page=1>

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: <http://www.us-cert.gov>.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

Communications Sector

24. *December 22, Digital Trends* – (International) **Repairs underway on Mediterranean cables.** Operations are underway to repair three undersea telecommunications cables that were damaged in the Mediterranean Sea over the weekend, disrupting telephone and Internet service in parts of the Middle East and south Asia. However, this time the cause of the cable cuts is suspected to be a ship's anchor, rather than a deliberate act of terrorism or sabotage. The damage to the FLAG, SEA-ME-WE4, and SEA-ME-WE3 cables occurred late Friday; by Sunday a remotely-operated submarine robot was being used to locate and assess the damage to the cables. It is possible a ship anchor could

have dragged the cables some distance from their proper locations. Once the damage areas have been located and identified, the remote robot will bring the cables up to a repair ship which will repair the damage and then re-lay the cables on the ocean floor. Source: <http://news.digitaltrends.com/news-article/18720/repairs-underway-on-mediterranean-cables>

[\[Return to top\]](#)

Commercial Facilities Sector

Nothing to report

[\[Return to top\]](#)

National Monuments & Icons Sector

25. *December 22, LawFuel* – (Arizona) **Final National Forest marijuana cultivator sentenced to 144 months in federal prison.** A Phoenix man was sentenced by a U.S. District court to 144 months in federal prison on December 15. The man pleaded guilty to conspiracy to cultivate marijuana on national forest lands. He is the final defendant to be sentenced of 11 defendants associated with one or more of the many 2007 marijuana garden investigations who were arrested and prosecuted by the U.S. Attorney's Office in the District of Arizona. Over the course of the 2007 marijuana growing season, the Gila County Narcotics Task Force, Gila County Sheriff's Office, U.S. Forest Service, and the Drug Enforcement Administration located, investigated, and eradicated several marijuana cultivation sites, referred to as "gardens," on National Forest Lands in Arizona. The man was found to be a supervisor of at least two of the gardens in the Tonto National Forest which were eradicated in 2007. Source: <http://lawfuel.com/show-release.asp?ID=20309>

[\[Return to top\]](#)

Dams Sector

26. *December 22, St. Louis Business Journal* – (Missouri) **Army Corps of Engineers sues Ameren over Taum Sauk collapse.** The U.S. Army Corps of Engineers has sued AmerenUE, alleging that the Taum Sauk reservoir breach dumped sediment and debris into the Clearwater Lake Reservoir. As a result of the breach at AmerenUE's Taum Sauk hydroelectric plant, the storage capacity of the Clearwater Lake Reservoir "has been significantly reduced" and the Clearwater Dam is "undergoing a major rehabilitation project and is rated with the lowest safety rating," according to the lawsuit, filed December 12 in federal court in the eastern district of Missouri. Source: <http://www.bizjournals.com/stlouis/stories/2008/12/22/daily10.html>

[\[Return to top\]](#)

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions: Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421

Subscribe to the Distribution List: Visit the [DHS Daily Open Source Infrastructure Report](#) and follow instructions to [Get e-mail updates when this information changes](#).

Removal from Distribution List: Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.