



Homeland  
Security

# Daily Open Source Infrastructure Report

## 23 May 2012

### Top Stories

- More than 500 fires sparked at a chemical plant in Port Allen, Louisiana, May 21 forcing the evacuation of about 250 people and closing roads for miles. – *WAFB 9 Baton Rouge* (See item [8](#))
- The U.S. Securities and Exchange Commission charged two individuals who provided the biggest influx of investor funds into a more than \$157 million Ponzi scheme run out of Florida. – *U.S. Securities and Exchange Commission* (See item [13](#))
- The U.S. government filed three lawsuits against large banks seeking about \$92 million in restitution for losses on soured mortgage debt purchased by two small Illinois banks that failed in 2009. – *Reuters* (See item [15](#))
- About 30 or so people were forced to abandon their cars and walk out of a tunnel near the Capitol in Washington, D.C. after a big, empty bus being used by the military exploded. – *WUSA 9 Washington, D.C.* (See item [22](#))
- Malware writers used Crossrider, a cross-browser extension development framework, to build a click-fraud worm that spreads on Facebook, Kaspersky Lab researchers said. – *IDG News Service* (See item [42](#))
- A researcher devised a method that attackers could use to clone a software token that about 40 million people use to access confidential data belonging to government agencies, military contractors, and corporations. – *Ars Technica* (See item [43](#))
- Computer scientists identified a vulnerability in the network of AT&T and at least 47 other cellular carriers that allows attackers to surreptitiously hijack the Internet connections of smartphone users and inject malicious content into the traffic passing between them and trusted Web sites. – *Ars Technica* (See item [44](#))
- Fires in rugged, mountainous areas of Arizona, New Mexico, and Colorado, forced the evacuation of several small towns and torched more than 65 square miles of forest, brush, and grass. – *Reuters* (See item [53](#))

---

## Fast Jump Menu

### PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

### SUSTENANCE and HEALTH

- [Agriculture and Food](#)
- [Water](#)
- [Public Health and Healthcare](#)

### SERVICE INDUSTRIES

- [Banking and Finance](#)
- [Transportation](#)
- [Postal and Shipping](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

### FEDERAL and STATE

- [Government Facilities](#)
  - [Emergency Services](#)
  - [National Monuments and Icons](#)
- 

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: LOW, Cyber: LOW**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) - <http://www.esisac.com>]

1. *May 22, United Press International* – (Michigan; International) **NTSB releases Michigan oil spill documents.** The U.S. government said it released thousands of documents and dozens of pictures related to a pipeline spill of tar sands oil in southern Michigan in 2010, United Press International reported May 22. The National Transportation Safety Board (NTSB) said it released 58 photographs and 5,000 pages of documents related to the rupture of Line 6B of the Lakehead pipeline system in Marshall, Michigan, as part of its investigation. The NTSB said Enbridge Energy Partners, the pipeline operator, was notified of the leak on Line 6B July 26, 2010. “The pipeline had ruptured 17 hours earlier and spilled about a million gallons of crude oil into the immediate area resulting in extensive environmental damage to Talmadge Creek and the Kalamazoo River,” the NTSB said in a statement. The NTSB said the rupture on the pipeline measured about 6 feet by 4.5 inches at its widest location. The week of May 14, Enbridge issued a proposal to the Michigan Public Service Commission to replace more than 200 miles of Line 6B, part of the oil pipeline system transporting so-called tar sands oil from Canada.  
Source: [http://www.upi.com/Business\\_News/Energy-Resources/2012/05/22/NTSB-releases-Mich-oil-spill-documents/UPI-35431337692370/](http://www.upi.com/Business_News/Energy-Resources/2012/05/22/NTSB-releases-Mich-oil-spill-documents/UPI-35431337692370/)
2. *May 21, Associated Press* – (Wyoming) **Coal mine blast near Gillette results in 2 notices of violation from Wyoming, federal citation.** Wyoming officials issued two notices of violation to Cloud Peak Energy Inc. following a blast at the Cordero Rojo coal mine near Gillette that registered on seismographs on the scale of a small earthquake, the Associated Press reported May 21. State officials said the May 1 blast was so large because explosives adjacent to the blast area were also accidentally set off upon detonation, causing more than the legal limit of explosives to go off. The State

suspended the blaster in charge of the explosion and the blaster's assistant for at least 60 days. Cloud Peak Energy must submit plans to the state outlining how it will prevent a similar explosion. Federal mine regulators also issued a citation, but no penalty was immediately assessed.

Source:

<http://www.therepublic.com/view/story/87755a14594b4c0c83552fa0b8c04dab/WY--Mine-Blast/>

3. *May 21, Coldwater Daily Reporter* – (Illinois) **Equipment failure may lead to months of delays at power plant.** An equipment failure may lead to months of delays at the Prairie State power plant in Marissa, Illinois, partially owned by Coldwater Board of Public Utilities (CBPU) and under construction supervision of American Municipal Power, the Coldwater Daily Reporter reported May 21. The CBPU director said mechanical delays caused the start up to be pushed to the end of 2012 for the first of two 800 megawatt coal fired generators. “The extent of damage and root cause analysis is under way,” the firm reported, although the failure of a fan is suspected. Because it is not known why the fan failed, this delay could push the completion of the plant into late 2012. According to the filing, this would be about 1 year later than the first unit was supposed to come online December 2011. Because it was uncertain why the fan failed, the second unit was also shut down until analysis is completed. The fan is a key element for reducing air emission, which is designed to make the coal plant one of the least polluting in operation.

Source: <http://www.thedailyreporter.com/news/business/x1898608151/Equipment-failure-may-lead-to-months-of-delays-at-power-plant>

4. *May 21, KCSG 14 St. George* – (Utah; National) **Utah utility customers targeted by scams offering bill credits.** The Utah Department of Commerce and Rocky Mountain Power warned Utah utility customers to be aware of scammers posing as Rocky Mountain Power customer service agents or attorneys, KCSG 14 St. George reported May 21. During the con, elderly consumers are told that under a grant authorized by the U.S. President, they can receive a utility bill credit or have their bills paid directly. The potential victims are told they must provide their Social Security number, credit card, or check routing number first. The scam has been reported across the country and in Utah in recent months. Some scammers are handing out flyers in person, while others are using social media, texting, or contacting consumers by phone. Some customers who received such calls were told their electricity will be disconnected if they do not provide their credit card information.

Source: [http://www.kcsg.com/view/full\\_story/18671626/article-Utah-Utility-Customers-Targeted-By-Scams-Offering-Bill-Credits?instance=home\\_first\\_stories](http://www.kcsg.com/view/full_story/18671626/article-Utah-Utility-Customers-Targeted-By-Scams-Offering-Bill-Credits?instance=home_first_stories)

5. *May 21, CNN* – (Arkansas) **Arkansas blast fatally burns 3 beyond recognition.** A three-man oil crew was killed in an explosion in El Dorado, Arkansas, while dismantling an abandoned containment vessel filled with residual oil vapors, the Arkansas Emergency Management said May 21. The crew was working for the Long Brothers Oil Co. at the abandoned site when the blast occurred, an Arkansas EMS spokesman said. The El Dorado Fire Department initially responded to the explosion and controlled the fire, he said. Flames from the blast ignited a separate fire in a

wooded area near the abandoned oil site. The Arkansas Forestry Department was dispatched to contain the fire, which still burned 2.5 hours after the initial explosion. Source: <http://www.cnn.com/2012/05/21/us/arkansas-fatal-blast/index.html>

6. *May 20, Wichita Eagle* – (Kansas) **Thieves steal copper from Westar Energy.** Thieves broke into a Westar Energy warehouse in Wichita, Kansas, and took thousands of dollars worth of copper. The theft was discovered May 19 when Westar employees noticed someone cut a chain-link fence surrounding the property in several locations, according to a spokesman for the Wichita Police Department. Once inside the warehouse, the thieves used a skid loader to steal the copper. The loader was later found outside the property in an abandoned field. Source: <http://www.kansas.com/2012/05/20/2342206/thieves-steal-copper-from-westar.html>

For another story, see item [33](#)

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

## **Chemical Industry Sector**

7. *May 22, KREX 5 Grand Junction* – (Colorado) **Tanker carrying fracking chemicals rolls over on Highway 139.** A tanker truck carrying thousands of gallons of fracking chemicals rolled over on Highway 139 at mile marker 32 near Loma, Colorado, May 21. A Colorado State Patrol trooper said the driver of the tanker truck was headed south on Highway 139 toward Grand Junction when he lost control, causing the truck to flip onto its right side. Officials with the Lower Valley Fire District (LVFD) said about 50 gallons leaked into a nearby stream before they dammed the area to prevent it from being contaminated any further. The LVFD and Grand Junction HAZMAT crews drained the remainder of the liquid from the truck and towed it away. The Environmental Protection Agency was slated to evaluate the site May 22. Source: <http://www.krextv.com/news/around-the-region/Tanker-Carrying-Fracking-Chemicals-Rolls-Over-on-Highway-139-152433015.html>
8. *May 22, WAFB 9 Baton Rouge* – (Louisiana) **Plant fire out, crews begin to inspecting and removing cylinders.** Most of the 500 or more fires that sparked May 21 at a chemical plant in Port Allen, Louisiana, were out. The fires forced the evacuation of about 250 people and closed roads for miles. Workers returned to the scene May 22 and assessed the condition of the cylinders containing acetylene, a highly flammable gas used mainly for welding, at the Air Liquide plant. They were forced to call off the assessment May 21 because of safety concerns. A Louisiana State Police captain said only three fires were still burning May 22. However, the plant remained closed. The captain said crews would first move all unaffected cylinders away from the site of the fire. Workers then would evaluate all of the cylinders that were burned to ensure their stability. Once a cylinder is deemed stable, it will be removed. The captain said there are about 1,000 total cylinders and hundreds were affected by the fire. U.S. 190, which closed down when the fire ignited May 21 remained closed in both directions at LA 983 May 22. Troopers said the highway was not expected to re-open until late May 22

at the earliest. People in homes and businesses evacuated within a 1-mile wide radius had not been allowed to return as of late the morning of May 22. The evacuation forced some to flee to one of the two community centers being used as shelters in Erwinville and Port Allen.

Source: <http://www.wafb.com/story/18579269/fire-out-crews-begin-to-inspect-cylinders-at-air-liquide-plant?clienttype=printable>

9. *May 22, Dover-New Philadelphia Times-Reporter* – (Ohio) **Dover Chemical: Safety assessments under way.** The president of Dover Chemical in Dover, Ohio, reported May 22 the building where the plant’s May 21 vapor release occurred would remain offline for several days while equipment and safety assessments are completed. “The chamber where the incident occurred continues to cool and remains isolated,” he said, noting it would be inspected and evaluated when safe entry is possible. All other operations were restarted after a thorough inspection of all safety systems, the president added. Dipropylene glycol — commonly known as automotive antifreeze — was a reactant in a reactor that overheated. Broken-down components of the chemical were released May 21 creating a a large vapor cloud, closing the plant, and putting local citizens and emergency personnel on alert for more than 4 hours. As a precautionary measure, local traffic was diverted and I-77 was closed between New Philadelphia and Dover.

Source: <http://www.timesreporter.com/news/x358790495/Dover-Chemical-Safety-assessments-under-way>

For more stories, see items [32](#) and [33](#)

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

## **Nuclear Reactors, Materials and Waste Sector**

10. *May 22, Nuclear Street* – (Louisiana) **River Bend experiences reactor scram.** River Bend Station near St. Francisville, Louisiana, experienced a reactor scram May 21 resulting from an RPS actuation, according to a Nuclear Regulatory Commission release. Following the scram, reactor water level briefly lowered below level 3. The reactor was stable, and pressure and temperature were being controlled by the feed water system and main steam bypass valves, respectfully. The cause of the scram was due to a turbine trip/low condenser vacuum. The low vacuum condition resulted from a loss of non-safety related 4160V switchgear that powers two of four circulating water pumps.

Source: <http://nuclearstreet.com/nuclear-power-plants/b/nuclear-plant-outages/archive/2012/05/22/river-bend-experiences-reactor-scram.aspx>

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

## **Critical Manufacturing Sector**

11. *May 21, U.S. Department of Labor* – (Pennsylvania) **OSHA cites Bear Ridge Machine and Fabrication for safety, health hazards at Frackville, Pa., shop.** The

Occupational Safety and Health Administration (OSHA) May 21 cited Bear Ridge Machine and Fabrication for 31 serious safety and health violations at their Frackville, Pennsylvania shop. The November inspection was initiated as part of the OSHA's Site-Specific Targeting Program for industries with high injury and illness rates. The serious violations involved electrical hazards and a failure to: implement a respiratory protection and hazard communication program; keep workplaces clean and sanitary; make exits clearly visible and marked; conduct a workplace hazard assessment; conduct fit testing and medical evaluations for respirator users; provide personal protective equipment for welders; provide machine guarding; provide fire extinguisher and hazard communication training; ensure proper cleansing of respirators; and remove defective power industrial trucks from service.

Source:

[http://www.osha.gov/pls/oshaweb/owadisp.show\\_document?p\\_table=NEWS\\_RELEASES&p\\_id=22425](http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=22425)

For another story, see item [32](#)

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

## **Defense Industrial Base Sector**

12. *May 22, Bloomberg* – (International) **China top source of counterfeit U.S. military electronics.** China's government has failed to curb manufacturing of counterfeit military electronic parts by Chinese companies that are the "dominant source" of fakes in the U.S. defense supply chain, a U.S. Senate investigation found. In January, the U.S. Air Force suspended a Shenzhen, China-based company from supplying parts to U.S. contractors after it sold about 84,000 suspect components, many of them installed on U.S. aircraft, according to an example cited in the U.S. Senate Armed Services Committee report released May 21. The panel's report outlines the results of a 14-month investigation disclosing dozens of examples of suspected counterfeit electronic parts. Saying U.S. companies and the military services did not crack down on abuses, the committee said the defense industry "routinely failed to report cases of suspect counterfeit parts, putting the integrity of the supply chain at risk." The report did not cite any examples of counterfeit parts causing damage such as lives lost or planes that crashed. The committee said it found "overwhelming and undeniable evidence to support" the conclusion that China has not taken steps to stop operations "that are carried out openly in that country."

Source: <http://www.bloomberg.com/news/2012-05-21/china-top-source-of-counterfeit-u-s-military-electronics.html>

For another story, see item [43](#)

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

## **Banking and Finance Sector**

13. *May 22, U.S. Securities and Exchange Commission* – (Florida) **SEC charges two feeders for one of south Florida’s largest-ever Ponzi schemes.** The U.S. Securities and Exchange Commission (SEC) May 22 charged two individuals who provided the biggest influx of investor funds into one of the largest-ever Ponzi schemes in south Florida. The SEC alleges the 2 men raised more than \$157 million from 173 investors in less than 2 years by issuing promissory notes from a company owned by one of the men, and interests in a private investment fund they operated. They used investor funds to purchase discounted legal settlements from a former Florida attorney through his law firm Rothstein, Rosenfeldt, and Adler PA. However, the settlements the attorney sold were not real and the supposed plaintiffs and defendants did not exist; the attorney simply used the funds in a Ponzi scheme. The scheme collapsed in October 2009, and its leader is currently serving a 50-year prison sentence. The SEC alleges the two men misrepresented to investors that they had procedural safeguards in place to protect investor money when in fact they often purchased settlements without first seeing any legal documents or doing anything to verify the settlement proceeds were actually in the firm’s bank accounts. Moreover, as the Ponzi scheme was collapsing, the pair sought new investor money while falsely touting the continued success of their strategy. The SEC’s complaint seeks disgorgement of ill gotten gains, financial penalties, and permanent injunctive relief against the men to enjoin them from future violations of federal securities law.

Source: <http://www.sec.gov/news/press/2012/2012-100.htm>

14. *May 22, Help Net Security* – (International) **Trojan stealing money in German online banking scam.** Trusteer came across a complex new criminal scheme involving the Tatanga trojan that conducts an elaborate Man in the Browser (MitB) attack to bypass SMS based transaction authorization to commit online banking fraud. The scam targets online banking customers of several German banks. When the victim logs on to the online banking application, Tatanga uses a MitB webinject that alleges the bank is performing a security check on their computer and ability to receive a Transaction Authorization Number (TAN) on their mobile device. In the background, Tatanga initiates a fraudulent money transfer to a mule account. It even checks the victim’s account balance and will transfer funds from the account with the highest balance if there is more than one to choose from. The victim is asked to enter the SMS-delivered TAN they receive from the bank into the fake Web form as a way to complete the security process. By entering the TAN in the injected HTML page, the victim is approving the fake transaction originated by Tatanga. Once the victim enters the TAN in the fake form and hits submit, the funds are transferred to the fraudster’s account. Meanwhile, Tatanga modifies the account balance reports in the online banking application to hide the fake transaction.

Source: [http://www.net-security.org/malware\\_news.php?id=2118&utm](http://www.net-security.org/malware_news.php?id=2118&utm)

15. *May 21, Reuters* – (National) **FDIC sues big banks over mortgage debt losses.** The U.S. government filed three lawsuits against large banks over losses on soured mortgage debt purchased by two small Illinois banks that failed in 2009, Reuters reported May 21. Acting as receiver for Citizens National Bank and Strategic Capital

Bank, the Federal Deposit Insurance Corp (FDIC) sued many banks including Bank of America Corp., Citigroup Inc., Deutsche Bank AG, and JPMorgan Chase & Co. Seeking a combined \$92 million, the lawsuits accuse the banks of misrepresenting the risks of residential mortgages they packaged into securities, causing losses for investors once the poor quality and defective underwriting became evident. Two FDIC lawsuits were filed in New York federal court and seek a combined \$77 million, while a third filed in Los Angeles seeks \$15 million. Bank of America and Citigroup were the only banks named as defendants in all three cases. Deutsche Bank and JPMorgan were defendants in two cases, and Ally Financial Inc., Credit Suisse Group AG, HSBC Holdings Plc., Royal Bank of Scotland Group Plc., and UBS AG in one. Citizens National and Strategic Capital, based in Macomb and Champaign, Illinois, respectively, had roughly \$1 billion of combined assets when they were closed May 22, 2009. Source: [http://articles.chicagotribune.com/2012-05-21/business/sns-rt-us-fdic-bank-lawsuitsbre84k1b4-20120521\\_1\\_renee-calabro-fdic-lawsuit-royal-bank](http://articles.chicagotribune.com/2012-05-21/business/sns-rt-us-fdic-bank-lawsuitsbre84k1b4-20120521_1_renee-calabro-fdic-lawsuit-royal-bank)

16. *May 21, Parker Chronicle* – (Colorado) **Parker man indicted for securities fraud.** A Parker, Colorado man faces more than 40 criminal charges on suspicion of orchestrating a scheme that authorities said bilked more than \$5 million from unsuspecting clients, the Parker Chronicle reported May 21. The Colorado Attorney General’s Office said the man offered high rates of return for those who invested in gas and well drilling operations. However, instead of putting the money into accounts that would grow, he is accused of using his two firms, Geodynamics Exploration Inc. and Geodynamics Inc., to redirect the money into his own accounts. He allegedly proceeded to drain the accounts by renting out a private Learjet and buying personal vehicles. The indictment said more than 60 investors fell for the fake operation. He faces 19 counts of theft and 22 counts of securities fraud. The Office of the Attorney General investigated the case and secured the indictment with the help of the Colorado Division of Securities and the U.S. Securities and Exchange Commission. Source: [http://www.ourcoloradonews.com/parker/news/parker-man-indicted-for-securities-fraud/article\\_4b6bd5c8-a37e-11e1-ab62-0019bb2963f4.html](http://www.ourcoloradonews.com/parker/news/parker-man-indicted-for-securities-fraud/article_4b6bd5c8-a37e-11e1-ab62-0019bb2963f4.html)
17. *May 21, Bloomberg* – (New York; International) **Nasdaq chief blames software for delayed Facebook debut.** Nasdaq OMX Group Inc. blamed “poor design” in the software it uses for driving auctions in initial public offerings (IPOs) after shares of Facebook Inc. were hit by delays and mishandled orders on its first day. Computer systems used to establish the opening price were overwhelmed by order cancellations and updates, Nasdaq’s chief executive officer (CEO) said May 20. Nasdaq’s systems fell into a “loop” that kept the operator from opening the shares on time. The U.S. Securities and Exchange Commission said it will review the trading. Nasdaq will use an “accommodation pool” that may total \$13 million to pay back investors who should have received executions in the opening auction, the CEO said. Media reports that brokers may lose \$100 million repaying investors whose orders were mishandled are credible, the chief executive of Knight Capital Group Inc. said May 21. Problems surfaced at 11:11 a.m May 18 after one of the stock’s underwriters completed its role in setting the price for the trade in Nasdaq’s opening auction. Trade requests received during the 5 milliseconds it took to operate the auction disturbed the process, leading to an imbalance of buys and sells and sending the program into a loop. Exchange officials

manually intervened to allow the auction to occur at 11:30 a.m. The IPO software “didn’t work” even after thousands of hours of testing for “a hundred scenarios” aimed at anticipating problems, the CEO said. Responding to the malfunction, Nasdaq altered its IPO procedures May 21. Orders totaling 30 million shares were submitted into the opening auction between 11:11 a.m. and 11:30 a.m., the CEO said. About half of them may involve “some level of dispute.”

Source: <http://www.bloomberg.com/news/2012-05-20/nasdaq-ceo-says-poor-design-in-ipo-software-delayed-facebook.html>

18. *May 18, Oklahoma City Oklahoman* – (Oklahoma) **Oklahoma City police seek help from Secret Service after finding fraudulent bank documents.** A drug arrest prompted the Oklahoma City Police to call for help from the U.S. Secret Service after a search of the suspects’ car uncovered hundreds of blank checks and equipment used to forged corporate checks. The two suspects were arrested on drug complaints, and police turned over the investigation into the financial documents to the Secret Service, according to a police report released May 17. Police were called May 13 to a hotel on a report of a suspicious group of people. They found two men in a car and questioned them. Police found hundreds of bank documents in the trunk of the car, including blank checks from individuals and businesses, as well as corporate documents that would be needed to print out a fake corporate check. Police called in the federal agency because of the volume of documentation, the report stated.

Source: <http://newsok.com/oklahoma-city-police-seek-help-from-secret-service-after-finding-fraudulent-bank-documents/article/3676408#ixzz1vEBDP2m1>

For more stories, see items [4](#), [39](#), and [44](#)

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

## **Transportation Sector**

19. *May 22, Missoula Missoulian* – (Montana) **Bus crashes on Highway 93 North; 4 injured.** A Rimrock Stages bus with about 17 passengers on board crashed into a pickup truck on Highway 93 North in Montana, injuring at least 4 people May 22. Passengers on the bus said a pickup truck started swerving, then pulled directly into the path of the bus, sending both vehicles off the highway at about mile marker 14. An Arlee police chief said all passengers on board the bus were sent to Missoula hospitals for observation, but only three appeared to have moderate to severe injuries. The pickup driver sustained the most serious injuries, he said.

Source: [http://missoulian.com/news/local/updated-bus-crashes-on-highway-north-injured/article\\_45e3dad2-a41f-11e1-9c74-001a4bcf887a.html](http://missoulian.com/news/local/updated-bus-crashes-on-highway-north-injured/article_45e3dad2-a41f-11e1-9c74-001a4bcf887a.html)

20. *May 22, CNN* – (Maine; International) **Passenger’s implant claim triggers flight diversion.** A passenger who claimed to have a device surgically implanted inside her triggered the security scare that led to the diversion to Maine of a jetliner that took off from France and was headed to North Carolina May 22, federal officials said. The passenger handed a note to the flight crew indicating she had had a device implanted in her body, but did not indicate the device was a threat or that she was threatening the

flight. Doctors aboard examined the woman and saw no sign of recent scars, and a senior federal law enforcement official said authorities determined no bomb was involved in the incident. US Airways Flight 787 landed in Bangor, Maine, after the incident. The Paris-to-Charlotte flight carried 179 passengers and a crew of 9, an airline spokeswoman said. The flight was diverted to Bangor “out of an abundance of caution,” the Transportation Security Administration said.

Source: [http://edition.cnn.com/2012/05/22/us/jetliner-security/index.html?hpt=hp\\_t1](http://edition.cnn.com/2012/05/22/us/jetliner-security/index.html?hpt=hp_t1)

21. *May 22, Truckinginfo.com* – (Tennessee) **I-75 one lane in each direction after massive landslide.** The Tennessee Department of Transportation reopened one lane for southbound travel on I-75 in Campbell County May 22. One lane remained open for northbound travelers as work continued to repair a massive landslide at Mile Marker 143. A 3-mile stretch of I-75 was down to one lane of traffic in each direction, from mile marker 141 to mile marker 144, May 22. Motorists were told to expect potential long delays and use extreme caution while traveling through the area. Wide loads were restricted from traveling through this area and were being detoured around the I-75 landslide.

Source: [http://www.truckinginfo.com/news/news-detail.asp?news\\_id=77026&news\\_category\\_id=19](http://www.truckinginfo.com/news/news-detail.asp?news_id=77026&news_category_id=19)

22. *May 21, WUSA 9 Washington, D.C.* – (Washington, D.C.) **Bus fire fills 3rd St Tunnel with smoke, drivers have to abandon cars.** A big, empty yellow school bus being used by the military exploded in flames May 21 in the 3rd Street Tunnel by the Capitol in Washington, D.C. The bus was hooked to a tow truck and started burning in the tunnel, with dozens of cars trapped in the tunnel with it. Three Capitol Police officers who inhaled a ton of smoke were all released from the hospital. The police ordered 30 or so people out of their cars and up the ramp. “We could not advance, smoke was into the car. The bus could explode any moment,” said a driver who was stuck. Police finally let the drivers back down to get their cars. After a few hours cleaning up the mess, the District of Columbia Department of Transportation finally re-opened the tunnel.

Source: <http://wusa9.com/news/article/205902/158/Bus-Fire-Fills-3rd-St-Tunnel-With-Smoke-Drivers-Have-To-Abandon-Cars>

23. *May 21, Associated Press* – (Minnesota) **Allegiant Air jet makes emergency landing in Duluth.** An airplane headed from Duluth, Minnesota, to Las Vegas had to turn around and make an emergency landing after running into engine trouble, the Associated Press reported May 21. An executive director of the Duluth Airport Authority said the Allegiant Air plane landed safely May 18 at Duluth International Airport. National Guard firefighters and other emergency responders were standing by. The Duluth News Tribune reported one engine failed about 50 miles into the trip and the crew shut it down, declared an emergency, and headed back to the airport. The plane had about 140 passengers and 5 crew members.

Source: <http://travel.usatoday.com/flights/story/2012-05-21/Allegiant-Air-jet-makes-emergency-landing-in-Duluth/55112496/1>

24. *May 19, Houma Courier* – (Louisiana) **Repair of pontoon bridge declared an emergency.** A Dulac bridge in Terrebonne Parish, Louisiana, was closed because of structural issues, Terrebonne Parish Houma Today reported May 19. Parish officials declared the project an emergency and said a return to service is necessary. An I-beam that supports the bridge unexpectedly collapsed and Terrebonne’s Roads and Bridges Division closed the bridge until further notice while engineers from Gulf South Engineering were called to assess the damage. Officials said the May 7 closure of the pontoon bridge could not have been more inconvenient with the 2012 hurricane season quickly approaching and with shrimping season under way. The bridge is used as one of the area’s emergency evacuation routes, and shrimpers who do not have access to the bridge have to drive along the bayou to the next bridge, about a 1-hour trip. The Terrebonne Parish council drafted a resolution to be voted on at the May 21 public services committee meeting to authorize the money for emergency repairs.  
Source: <http://www.houmatoday.com/article/20120519/ARTICLES/120519619>

For more stories, see items [1](#), [7](#), [8](#), [9](#), [50](#), [53](#), and [55](#)

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

## **Postal and Shipping Sector**

25. *May 21, Midland Daily News* – (Michigan) **Unknown white powder found on mailboxes.** An unknown white powder covering mailboxes caused police and fire crews to close roads in the area of North Lakeview Drive and Beamish Road in Jerome Township, Michigan, May 21. “We have the area cordoned off and we have a team coming to test it,” a Midland County Sheriff’s Office captain said. The Jerome Township Fire Department was called to the scene when a resident discovered the white powder on and inside of a mailbox, the Jerome Township fire chief said. “A resident went out to ... his mailbox [and] discovered the powder substance on and in his mailbox. And then as we got here we discovered there was a multitude of them (mailboxes with powder). So we have actually isolated the whole area off and will start testing them now,” the fire chief said. Agencies at the scene also included the Midland Saginaw Bay City HAZMAT team and Lincoln Township Fire Department.  
Source: [http://www.ourmidland.com/police\\_and\\_courts/article\\_f1d713d4-a34f-11e1-88d8-001a4bcf887a.html](http://www.ourmidland.com/police_and_courts/article_f1d713d4-a34f-11e1-88d8-001a4bcf887a.html)

For another story, see item [50](#)

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

## **Agriculture and Food Sector**

26. *May 22, Food Safety News* – (National) **USDA takes meat and poultry labeling to the web.** A new Web-based label approval system that will streamline the agency’s review process for meat, poultry, and egg product labels was introduced May 21 by USDA’s Food Safety and Inspection Service (FSIS). Called the Label Submission Approval System (LSAS), the new system will: make it possible for food

manufacturers to submit label applications electronically; flag application submission errors that could delay the approval process; and allow users to track the progress of their submission. The LSAS is supposed to reduce the time and costs incurred by the industry and the agency. Until the launch of LSAS, companies mailed or hand delivered paper applications to FSIS, and it reviewed and corrected them before returning them in hard copy. The agency receives 150 to 200 label submissions daily, and it can take more than 3 weeks for a label to be reviewed. The Web-based system will make approved or corrected labels immediately available to companies, saving time and mailing costs. The new system also will allow companies to store labels and make changes electronically, removing the need to print and re-submit modified labels for review to FSIS each time a change is made.

Source: <http://www.foodsafetynews.com/2012/05/usda-takes-meat-poultry-labeling-to-the-web/>

27. *May 22, Food Safety News* – (National) **Diamond Pet Foods recalls more dry dog food.** Diamond Pet Foods again recalled batches of dry dog food that may be contaminated with Salmonella, this time to include its Diamond Naturals Small Breed Adult Dog Lamb & Rice Formula dry dog food manufactured August 26, 2011, Food Safety News reported May 22. The earlier recalls involved various formulas manufactured after December 9, 2011 at Diamond’s production facility in Gaston, South Carolina. This recall involves food produced in Meta, Missouri. The most recent recalled product was distributed in Colorado, Illinois, Kentucky, Louisiana, Michigan, Minnesota, Missouri, Oklahoma, Pennsylvania, South Dakota, Tennessee, Texas, and Wisconsin. Further distribution through other pet food channels, including online retailers, may have occurred. For the earlier recalls, as of May 11, 15 people in 9 states and 1 person in Canada were reported sickened with an outbreak strain of Salmonella Infantis from contact with contaminated dog food or infected animals, said the Centers for Disease Control and Prevention. As of May 16, the Food and Drug Administration confirmed two dog illnesses related to the outbreak. The week of May 17, the Calgary Herald in Alberta reported two cats in a Montreal shelter died, and another was ill, after being fed Diamond products.

Source: <http://www.foodsafetynews.com/2012/05/diamond-pet-foods-recalls-more-dry-dog-food/>

28. *May 22, MSNBC* – (National) **Nearly 1,000 dogs now sick from jerky treats, FDA reports say.** Nearly 1,000 dogs reportedly were sickened by chicken jerky pet treats from China, according to a new tally of complaints from owners and veterinarians submitted to federal health officials, MSNBC reported May 22. The Food and Drug Administration (FDA) logged 900 reports of illnesses and deaths since November 2011, when it warned owners about continued problems with the products known variously as chicken jerky strips, treats, and nuggets, a spokeswoman said. The agency sent inspectors earlier in 2012 to Chinese plants that make the jerky treats, but no results of those reviews were yet available, an FDA spokeswoman said May 21.

Source: <http://vitals.msnbc.msn.com/news/2012/05/22/11798368-nearly-1000-dogs-now-sick-from-jerky-treats-fda-reports-say?lite>

29. *May 20, Food Safety News* – (National) **Salmonella Paratyphi B outbreak grows.** The Salmonella Paratyphi B case-count associated with contaminated starter culture used in raw tempeh products sold by Smiling Hara, an Asheville, North Carolina-based company, continued to grow the week of May 17, with the number of Salmonella Paratyphi B cases reaching 83, May 18. According to the Asheville Citizen-Times, 62 of the cases were counted among residents of Bruncombe County, North Carolina. Smiling Hara purchased the contaminated spore culture from Tempeh Online, a Maryland-based company that has since taken down its Web page and deleted all but one of its Twitter posts. The U.S. Food and Drug Administration was working with State health officials to determine whether or not Tempeh Online’s contaminated culture might have been used by any other producers. Smiling Hara recalled all of its tempeh made between January 11 and April 11 with best-by dates of July 11 through October 25.  
Source: <http://www.foodsafetynews.com/2012/05/salmonella-paratyphi-b-outbreak-grows/>
30. *May 20, Food Safety News* – (California) **Flours, legumes, spices recalled for allergens.** The U.S. Food and Drug Administration and Santos Agency, Inc. announced May 18 that Santos Agency was voluntarily recalling Santos Brands Products in California for undeclared peanuts and wheat. The Santos Brands Products were shipped to retail stores in California only, between May 2011 and May 2012. The recall was initiated after it was discovered the products were cross packaged on shared equipment with peanuts and wheat flour.  
Source: <http://www.foodsafetynews.com/2012/05/flours-legumes-spices-recalled-for-allergens/>
31. *May 18, Associated Press* – (California) **USDA lifts quarantines at 2 Calif. dairies after mad cow tests confirm no link to cattle feed.** Quarantines were lifted on two central California dairies associated with a case of mad cow disease after investigators found no link between the illness and food the diseased bovine might have consumed, federal officials said May 18. Tests performed by the World Organization for Animal Health also confirmed what U.S. labs had found: The cow had a random mutation of the illness that was unlikely to affect other cows in the herd. The tests were part of an investigation started in April when an examination of a carcass of a nearly 11-year-old cow taken to a Hanford rendering plant tested positive for mad cow disease, the nation’s fourth case and the third “atypical” strain to be discovered. The California cow had what is known as atypical L-type bovine spongiform that scientists know happens occasionally. As part of its investigation, the FDA and the California Department of Food and Agriculture examined feed records at the affected dairy and identified at least 10 suppliers. They said May 18 that all were in compliance with regulations.  
Source: [http://www.washingtonpost.com/national/health-science/usda-lifts-quarantines-at-2-calif-dairies-after-mad-cow-tests-confirm-no-link-to-cattle-feed/2012/05/18/gIQAr9R6YU\\_story.html](http://www.washingtonpost.com/national/health-science/usda-lifts-quarantines-at-2-calif-dairies-after-mad-cow-tests-confirm-no-link-to-cattle-feed/2012/05/18/gIQAr9R6YU_story.html)

For another story, see item [56](#)

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

## Water Sector

32. *May 21, Cleveland Plain Dealer* – (Ohio) **Northeast Ohio Regional Sewer District suspends sewer services to Kelly Plating for toxic discharges.** The regional sewer district issued an emergency suspension of sewer services May 19 against Kelly Plating Co. in Cleveland, which officials determined after investigation was dumping sewage that contained high levels of zinc on a regular basis. Zinc can be lethal to aquatic life and to micro-organisms in wastewater treatment plants, impacting all treatment at the plant. The sewer district requires companies that discharge zinc and other heavy metals to pre-treat them to remove toxicity before the discharge gets into the sewer system. Crews from the sewer district plugged the plant's sewer pipe May 21. The sewer district has taken this action about a dozen times since 1990. A criminal investigation has also been launched by the U.S. attorney's office, a spokesman said, because Kelly Plating has been dumping sludge into the sewers since March.

Source:

[http://www.cleveland.com/metro/index.ssf/2012/05/northeast\\_ohio\\_regional\\_sewer.html](http://www.cleveland.com/metro/index.ssf/2012/05/northeast_ohio_regional_sewer.html)

33. *May 19, Pittsburgh Tribune-Review* – (Pennsylvania) **Bromide level high in parts of Allegheny River.** Bromide levels have dropped in Pennsylvania's Allegheny River and its tributaries, but are continuing to increase downstream from four industrial wastewater-treatment plants, according to research from the Pittsburgh Water and Sewer Authority. Monthly samples in 2011 and two samples in 2012 showed bromide levels "aren't nearly as high" as they were in 2011, when State environmental regulators acted to cut rising bromide pollution in public water sources, the authority's water-quality director said May 19. The authority will have more conclusive data after a third sample later in 2012. The department in 2011 asked shale-gas drillers to stop sending wastewater to any plant that dumps treated water back into the river. Some drillers still take water to those plants, but treated water is shipped out to be used in drilling again, a spokesman of the industry group Marcellus Shale Coalition said. "So if bromide levels are still high ... there's clearly something else in play," he said. If shale-gas drilling water is not the source of the problem, it could be surface coal mining or shallow oil drilling, he said.

Source: <http://triblive.com/news/1824972-74/bromide-river-drilling-shale-states-allegheny-authority-department-gas-levels>

For another story, see item [7](#)

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

## Public Health and Healthcare Sector

Nothing to report

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

## Government Facilities Sector

34. *May 22, Associated Press; WVIT 30 New Britain* – (Connecticut) **Students expelled over Internet posts.** Two West Haven High School students accused of making threats on Twitter were charged and expelled from the Connecticut school, the Associated Press reported May 22. A police sergeant said teachers found the tweets in early May. The tweets, posted by a junior and a sophomore, did not appear to be linked to each other. The junior allegedly posted several messages about placing a bomb in a locker. The sophomore allegedly sent a tweet about shooting himself and other people. Police said the students' homes were searched and no weapons were found. Both students face felony charges.  
Source: <http://www.nbcconnecticut.com/news/local/Students-Expelled-over-Internet-Posts-152521765.html>
35. *May 22, Associated Press* – (Minnesota) **Osseo revises science experiments after accident.** The Osseo School District in Maple Grove, Minnesota, was making more permanent changes to its classroom science demonstrations after an experiment burned four students, the Associated Press reported May 22. An audit team of 12 science teachers recommended the methanol flash bottle demonstration that burned the students in December 2011 continue to be disallowed. It has not been done since the accident. The team's report called for a more stringent approval process for science experiments, provides a detailed list of accepted demonstrations, and requires science teachers to watch videos on experiment safety.  
Source: [http://www.wahpetondailynews.com/article\\_9373a658-a409-11e1-9341-001a4bcf887a.html](http://www.wahpetondailynews.com/article_9373a658-a409-11e1-9341-001a4bcf887a.html)
36. *May 21, Salt Lake Tribune* – (Utah) **Bomb threat temporarily halts construction at Bluffdale's NSA center.** FBI agents found no dangerous material after a bomb threat temporarily halted construction of a National Security Agency (NSA) data center at Utah's Camp Williams May 21. The U.S. Army Corps of Engineers evacuated the site after receiving the threat, said an FBI spokeswoman. Agents were investigating the origin of the threat, she said. The NSA broke ground on the \$1.2 billion cyber security center in January. Camp Williams is about 25 miles south of Salt Lake City.  
Source: <http://www.sltrib.com/sltrib/news/54156274-78/center-construction-bluffdale-bomb.html.csp>
37. *May 21, WKBN 27 Youngstown* – (Ohio) **Threatening note prompts extra security at Fitch.** Extra security was in place at Austintown Fitch High School in Austintown, Ohio, until the end of the school year after a threatening note was found on a desk the week of May 14. Police were checking students as they enter school, as well as cars coming on school property. The district put the protocol in place in light of the shooting that happened at Chardon High School in Chardon in February.  
Source: <http://www.wkbn.com/content/news/local/story/Threatening-Note-Prompts-Extra-Security-at-Fitch/13B2599oWU6ZbOODV2F-pg.csp>
38. *May 21, Reuters* – (National) **Computer hackers access U.S. Justice Department website: Spokeswoman.** One or more unauthorized users gained access to the inner

workings of a Web site run by the U.S. Justice Department, a department spokeswoman said May 21 after the hacker group Anonymous said they were behind the incident. The hackers accessed a server that operates the Bureau of Justice Statistics' Web site, the spokeswoman said. The department was looking into whether the unauthorized users broke criminal laws, she said. Online statements attributed to Anonymous said they were responsible for the security breach, and the files they obtained included e-mails. Source: <http://www.reuters.com/article/2012/05/21/net-us-usa-hackers-idUSBRE84K1B720120521>

For more stories, see items [12](#) and [43](#)

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

## **Emergency Services Sector**

See item [22](#)

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

## **Information Technology Sector**

39. *May 22, SC Magazine UK* – (International) **Social engineers breach billing service WHMCS.** Thousands of passwords and credit card details were exposed online after social engineers breached the billing platform WHMCS. Attackers obtained the data after masquerading as the platform's lead developer, and managed to con the company's hosting provider to release administrator credentials. The developer's details were then used to access WHMCS's database and steal hashed customer credit card numbers and passwords, usernames, and support tickets. Along with that data, they also made public a 1.7GB cache that included the WHMCS control panel and Web site information. Almost a day's worth of data was erased from the compromised servers, while links to the cache and other smaller files were hijacked. The lead developer said attackers from the group UGNazi provided correct answers to identity verification questions.

Source: <http://www.scmagazineuk.com/social-engineers-breach-billing-service-whmcs/article/242176/>

40. *May 22, Help Net Security* – (International) **Zeus Trojan variant comes with ransomware feature.** The recent popularity of ransomware as a tactic for tricking users into paying money resulted in an unexpected malware combination. F-Secure researchers recently spotted a new Zeus 2.x variant that includes a ransomware feature. Once this particular piece of malware is executed, it first opens Internet Explorer and directs it toward a specific URL — [lex.creativesandboxes.com/locker/lock\(dot\)php](http://lex.creativesandboxes.com/locker/lock(dot)php). Simultaneously, the users are blocked from doing anything on their computer. The site in question is offline, so it is difficult to be sure of what it contained, but a guess would be an extortion message. The command for "unlocking" the computer is present on the computer, in the registry, so it is possible to do so without paying the ransom.

Source: [http://www.net-security.org/malware\\_news.php?id=2120&utm](http://www.net-security.org/malware_news.php?id=2120&utm)

41. *May 22, Government Computer News* – (International) **After 6 weeks offline, ICANN reopens TLD application system.** The Internet Corporation for Assigned Names and Numbers (ICANN) reopened its Top Level Domain Application System for a 8-day window in which registered users can review and finalize applications. ICANN announced May 21 that the system, which was offline for nearly 6 weeks because of security problems, has reopened. It will remain open through midnight May 30. The deadline for registering to use the system was in March, and only users already registered will be able to complete applications. No new applications slots can be requested.  
Source: <http://gcn.com/articles/2012/05/22/icann-generic-top-level-domain-reopening.aspx>
42. *May 21, IDG News Service* – (International) **Cross-browser worm spreads via Facebook, security experts warn.** Malware writers used Crossrider, a cross-browser extension development framework, to build a click-fraud worm that spreads on Facebook, Kaspersky Lab researchers said May 21. Crossrider is a Javascript framework that implements a unified application programming interface (API) for building Firefox, Chrome, and Internet Explorer extensions. The API allows developers to write code that will run inside different browsers and, by extension, on different operating systems. The framework is still in beta testing and its creators plan on adding support for Safari soon. The new piece of malware is called LilyJade and is being sold on underground forums for \$1,000. Its creator claims the malware can infect browsers running on Linux or Mac systems, and since it does not have any executable files, no antivirus program is designed to detect it. The malware's purpose appears to be click fraud. It is capable of spoofing rogue advertisement modules on Yahoo, YouTube, Bing/MSN, AOL, Google, and Facebook, a Kapersky malware expert said. When users view or click on these ads, the malware's creators earn money through affiliate programs. To spread, the malware leverages control over infected browsers to piggyback on active Facebook sessions and send spam messages on behalf of authenticated Facebook users. The links included in LilyJade's Facebook spam direct users to compromised sites that load the Nuclear Pack exploit kit into a hidden iframe. Exploit kits like Nuclear Pack attempt to exploit vulnerabilities in outdated software — usually browser plug-ins like Java, Flash Player, or Adobe Reader — to infect computers with malware.  
Source:  
[http://www.computerworld.com/s/article/9227351/Cross\\_browser\\_worm\\_spreads\\_via\\_Facebook\\_security\\_experts\\_warn](http://www.computerworld.com/s/article/9227351/Cross_browser_worm_spreads_via_Facebook_security_experts_warn)
43. *May 21, Ars Technica* – (International) **RSA SecurID software token cloning: A new how-to.** A researcher devised a method that attackers with control over a victim's computer could use to clone the software token RSA's SecurID uses to generate one-time passwords. The technique, described May 17 by a senior security analyst at a firm called SensePost, has important implications for safekeeping of the tokens. By reverse engineering software used to manage the cryptographic software tokens on computers running Microsoft's Windows operating system, he found the secret "seed" was easy for people with control over the machines to deduce and copy. He provided step-by-step instructions for others to follow to demonstrate how easy it is to create clones that

mimic verbatim the output of a targeted SecurID token. An estimated 40 million people use these to access confidential data belonging to government agencies, military contractors, and corporations.

Source: <http://arstechnica.com/security/2012/05/rsa-securid-software-token-cloning-attack/>

44. *May 21, Ars Technica* – (International) **Smartphone hijacking vulnerability affects AT&T, 47 other carriers.** Computer scientists identified a vulnerability in the network of AT&T and at least 47 other cellular carriers that allows attackers to surreptitiously hijack the Internet connections of smartphone users and inject malicious content into the traffic passing between them and trusted Web sites. The attack, which does not require an adversary to have any man-in-the-middle capability over the network, can be used to lace unencrypted Facebook and Twitter pages with code that causes victims to take unintended actions, such as post messages or follow new users. It can also be used to direct people to fake banking sites, and to inject fraudulent messages into chat sessions in some Windows Live Messenger apps.

Source: <http://arstechnica.com/security/2012/05/smartphone-hijacking-on-att-47-other-carriers/>

45. *May 21, SecurityWeek* – (International) **Yahoo strengthens mail filters after attempted JavaScript attack.** Yahoo! strengthened its Web mail filters after researchers at Trend Micro detected a JavaScript attack the week of May 14 that was targeting its users. In the past, vulnerabilities within Web mail platforms were used to compromise accounts maintained by journalists and activists. May 18, Trend Micro said they detected several e-mails being used in targeted attacks that contained JavaScript in the “From” field. The code was attempting to launch a DOM-based cross-site scripting (XSS) attack, which would presumably yield access to the victim’s account to the attacker.

Source: <http://www.securityweek.com/yahoo-strengthens-mail-filters-after-attempted-javascript-attack>

46. *May 21, Threatpost* – (International) **Report: Diablo III users find accounts hacked, gold stolen and new ‘mystery’ friends.** Blizzard Entertainment’s update to the mega-popular Diablo game franchise hit a major snag the weekend of May 19, after users started peppering support boards and the company with reports of raided accounts, missing virtual “gold,” and mysterious new friends. Many report being the victims of account takeovers while they were online, suggesting hackers may be taking advantage of a vulnerability in Blizzard’s software or Battle.net gaming platform.

Source: [http://threatpost.com/en\\_us/blogs/report-diablo-iii-users-find-accounts-hacked-gold-stolen-and-new-mystery-friends-052112](http://threatpost.com/en_us/blogs/report-diablo-iii-users-find-accounts-hacked-gold-stolen-and-new-mystery-friends-052112)

47. *May 21, Government Computer News* – (National) **Critical industries don’t grasp IT risks, study shows.** A study by cybersecurity researchers at Carnegie Mellon University in Pittsburgh found that top corporate executives too often are disengaged from management of cyber risks to their organizations and that operators of critical infrastructure tend to lag behind the more highly regulated financial services industry in overseeing cybersecurity and privacy protection. The report, [“How Boards & Senior](#)

[Executives are Managing Cyber Risks,”](#) found that despite some improvements during the 4 years since the researchers’ first study, there still is a lack of understanding of the importance of IT risks in overall enterprise risk management.

Source: <http://gcn.com/articles/2012/05/21/carnegie-mellon-critical-infrastructure-risks.aspx>

For more stories, see items [14](#), [17](#), and [38](#)

### Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at [sos@us-cert.gov](mailto:sos@us-cert.gov) or visit their Web site: <http://www.us-cert.gov>

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

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

## Communications Sector

48. *May 22, Lake Powell Life* – (Utah) **Power outage Sunday affects KXAZ transmitter.** Listeners missed hearing KXAZ 93.3 FM Page, Arizona, May 20. A power outage by Garkane Power in southern Utah took the transmitter down until an emergency transmitter could get the Page FM radio station back on the air. As of May 22, full transmission power had been restored.  
Source:  
[http://www.lakepowelllife.com/index.php?option=com\\_content&view=article&id=3418:power-outage-sunday-affects-kxaz-transmitter&catid=186:latest-local-news&Itemid=18](http://www.lakepowelllife.com/index.php?option=com_content&view=article&id=3418:power-outage-sunday-affects-kxaz-transmitter&catid=186:latest-local-news&Itemid=18)

For more stories, see items [41](#), [42](#), [44](#), and [45](#)

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

## Commercial Facilities Sector

49. *May 22, Chicago Tribune* – (Illinois) **1 dead, 10 hurt in explosion at Arlington Heights business.** One person died and 10 others were injured in an explosion at a business in Arlington Heights, Illinois, releasing chemical fumes, May 22. Fire officials said the fumes posed no danger to nearby residents of the building. The force of the blast propelled rocks from the roof into a parking lot, damaging 20 cars. The explosion occurred at Arens Controls, a company that manufactures and tests electrical parts, according to the Arlington Heights fire chief. The explosion occurred in a machine in an area where parts are tested. The machine used a diluted form of potassium hydroxide, a chemical that can ignite combustible materials if mixed with water or other substances, the chief said. The violent explosion caused the roof to buckle, and resulted in twisted metal and devastation, he said. It also caused a small fire that was quickly extinguished, the chief added. Ten people — seven Arens employees and three

police officers — were sent to hospitals with injuries that did not appear life-threatening, officials said. About 50 Arens workers were evacuated, and the building was closed for the rest of the day.

Source: <http://www.chicagotribune.com/news/local/breaking/chi-arlington-hts-officials-investigate-possible-explosion-20120522,0,6468619.story>

50. *May 22, Sun-Times Media* – (Illinois) **Woman’s suspicious behavior leads to closure of Joliet streets.** A woman’s apparent displeasure with her cellular provider resulted in downtown streets being closed for nearly 4 hours May 21 in Joliet, Illinois. Buildings were also evacuated after witnesses saw her make suspicious gestures with a package before placing it in a delivery drop box. Firefighters examined the box and did not see any “leaking or other indications of immediate threat” but decided to activate the department’s hazardous materials team, which arrived to examine both the FedEx and UPS delivery boxes. The Cook County Bomb Squad was called out and used an X-ray machine to inspect the drop boxes, determining two packages would be examined because their contents contained electronics. The package that the woman deposited contained a phone she was returning to her cellular provider.

Source: <http://southtownstar.suntimes.com/news/12679387-418/suspicious-package-found-in-downtown-joliet.html>

51. *May 22, CNN* – (Oklahoma) **8 shot after Oklahoma City Thunder playoff win.** Eight people were shot May 21 near the Chesapeake Energy Arena as large crowds were leaving a National Basketball Association playoff game in Oklahoma City, police said. Of the victims, one was in critical condition and seven suffered non-life-threatening injuries. Additionally, a woman was injured when she was punched and kicked in the crowded streets, authorities said. Thousands of people were in the area following the end of the basketball game.

Source: [http://edition.cnn.com/2012/05/22/justice/oklahoma-shootings/index.html?hpt=hp\\_t2](http://edition.cnn.com/2012/05/22/justice/oklahoma-shootings/index.html?hpt=hp_t2)

52. *May 22, Worcester Telegram and Gazette* – (Massachusetts) **Chlorine gas released.** A chlorine gas scare in a building in a Southbridge, Massachusetts business complex triggered a HAZMAT response May 21. Workers from three companies in a Southbridge Business Center building were evacuated for several hours when an employee at Schott North America mistakenly mixed hydrochloric acid and sodium hypochlorite, which produced a small amount of chlorine gas. Workers in the building implemented an emergency response plan, evacuating about 100 people from Schott and other businesses in the building; they were allowed to return after about 4 hours.

Source: <http://www.telegram.com/article/20120522/NEWS/105229857/1003/NEWS03>

For more stories, see items [8](#), [43](#), and [53](#)

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

## National Monuments and Icons Sector

53. *May 21, Reuters* – (Arizona; Colorado; New Mexico) **Crews gain upper hand battling wildfires in southwest.** Fires in rugged, mountainous areas of Arizona, New Mexico, and Colorado forced the evacuation of several small towns and torched more than 65 square miles of forest, brush, and grass in the U.S. southwest, Reuters reported May 21. More than 1,100 firefighters in Arizona made progress against the Gladiator Fire, which charred about 22 square miles of ponderosa pine and brush some 40 miles north of Phoenix. Crews battling the 25-square-mile Sunflower Fire in Arizona succeeded in reinforcing control lines May 21, although authorities cautioned that dead trees burning sporadically in the remote, rugged Tonto National Forest could lead to long-term fire operations and smoke in nearby communities. In New Mexico, crews said two lightning-caused fires in the Gila Wilderness grew gradually overnight May 20. The Baldy Fire and Whitewater Fire have together consumed over 6 square miles of steep, rugged terrain in mixed conifer. In Colorado, crews had the 12-square mile Hewlett Fire burning in the Roosevelt National Forest almost completely contained, fire officials said May 21.

Source: <http://www.reuters.com/article/2012/05/21/us-usa-wildfires-idUSBRE84J00K20120521>

54. *May 21, Associated Press* – (Alaska) **Fire destroys one of Alaska's last roadhouses.** A historic roadhouse in Copper Center, Alaska, was destroyed in a fire May 20. The owner of the Copper Center Lodge, which was on the National Register of Historic Places, suspected bad wiring was to blame and said the lodge's oiled logs fueled the flames. The owner said a maintenance worker living on site alerted him to the flames. Firefighters from the Glenn-Rich Fire and Rescue, which serves the Copper Basin area, tried to battle the flames. "We just couldn't get enough water on it," the owner said.

Source: <http://www.adn.com/2012/05/21/2473721/fire-destroys-one-of-alaskas-last.html>

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

## Dams Sector

55. *May 22, WNEW 99.1 FM Washington, D.C.* – (Virginia) **Evacuations ordered near Lake Jackson dam in Manassas as flood concerns mount.** A level III emergency was declared in Prince William County, Virginia, May 22 forcing some residents to evacuate their homes due to concerns over the Lake Jackson dam in Manassas. The Prince William Fire and Rescue battalion chief said the dam was about 6 feet over its normal limit from recent rains. Officials said the dam was beginning to recede, but the heavy rains caused a number of sink holes in the county, closing three roads, and disrupting school bus service.

Source: <http://washington.cbslocal.com/2012/05/22/evacuations-ordered-near-lake-jackson-dam-in-prince-william-county-as-flood-concerns-mount/>

56. *May 22, Red Bluff Daily News* – (California) **Red Bluff Diversion Dam replacement nearly done.** The project manager for the Bureau of Reclamation said the Red Bluff Diversion Dam Fish Passage Improvement Project on the Sacramento River in California was scheduled to be complete in September, coming in under \$190 million. The original budget estimate was \$230 million. The joint project between the Bureau of Reclamation and the Canal Authority began more than 3 years ago after a federal judge's decision ordered the end of lowering the diversion dam gates and the end of Lake Red Bluff. The new pumping facility is meant to screen the water pumped into the canal, while allowing threatened and endangered salmon, steelhead, green sturgeon, and other fish species to pass through without disruption. Nine Florida-made pumps will be able to pump at 2,000 cubic-feet of water per second (cfs) and can be expanded up to 2,500 cfs. In all, 63 fish screens, 10-by-15 feet, span some 1,200 feet along the river's edge.

Source: [http://www.chicoer.com/news/ci\\_20678976/red-bluff-diversion-dam-replacement-nearly-done](http://www.chicoer.com/news/ci_20678976/red-bluff-diversion-dam-replacement-nearly-done)

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



**Department of Homeland Security (DHS)**  
**DHS Daily Open Source Infrastructure Report Contact Information**

**About the 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 Web site: <http://www.dhs.gov/IPDailyReport>

**Contact Information**

Content and Suggestions:	Send mail to <a href="mailto:cikr.productfeedback@hq.dhs.gov">cikr.productfeedback@hq.dhs.gov</a> or contact the DHS Daily Report Team at (703)387-2314
Subscribe to the Distribution List:	Visit the <a href="#">DHS Daily Open Source Infrastructure Report</a> and follow instructions to <a href="#">Get e-mail updates when this information changes</a> .
Removal from Distribution List:	Send mail to <a href="mailto:support@govdelivery.com">support@govdelivery.com</a> .

---

**Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto: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](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://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.