



Homeland  
Security

# Daily Open Source Infrastructure Report

## 16 May 2012

### Top Stories

- Vandals throwing big rocks and other debris onto Chicago-area expressways damaged more than a dozen vehicles in at least five separate incidents in recent days. – *Chicago Sun-Times* (See item [16](#))
- Sensitive personal data for more than 700,000 people who provide or receive home care for the elderly and disabled may have been compromised when payroll data disappeared in the mail, according to California officials. – *Los Angeles Times* (See item [30](#))
- U.S. military officials confirmed a wide-ranging investigation has uncovered a criminal conspiracy involving dozens of members of the Armed Forces. Officials recovered nearly \$2 million in guns and combat gear that soldiers and civilians stole and sold to gangs in the United States and foreign countries. – *Jacksonville Daily News* (See item [35](#))
- After stopping for several weeks, jamming of York County, Maine emergency radio transmissions started again. A May 12 incident of jamming delayed emergency response to a mobile home fire and resulted in extensive damage to four homes. – *Associated Press* (See item [36](#))
- Three of the most popular brands of closed-circuit surveillance cameras used by banks, hotels, hospitals, and other industries are sold with remote Internet access enabled by default and with weak password security, according to new research. – *Wired* (See item [40](#))
- Federal authorities joined the investigation after police in Palm Springs, California, found six crude pipe bombs near mobile home parks and other homes over a 5-day period. – *Associated Press* (See item [50](#))

---

## 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 15, WDSU 6 New Orleans* – (Louisiana) **Substation fire knocks out power to thousands.** A fire at an Entergy substation in New Orleans, Louisiana, knocked out power to thousands of people May 14. An Entergy spokesman said the outage affected about 14,000 customers in Terrytown, Algiers, and Algiers Point. Crews were called to the scene, but firefighters were kept outside the substation until the situation stabilized and it was safe to enter. Officials were working to route electricity from other substations to get the system back online. They expected to have most homes and businesses supplied with power by May 15.  
Source: <http://www.wdsu.com/news/local-news/new-orleans/Substation-fire-knocks-out-power-to-thousands/-/9853400/13394496/-/10a9nkgz/-/>
2. *May 14, XETV 6 San Diego* – (California) **Refinery problems continue to hurt California's gas supply.** Refinery problems continued to choke supplies of California's special blend of clean burning gas, sending gas prices at the pump skyrocketing, XETV 6 San Diego reported May 14. Phillips 66, Royal Dutch Shell, and Tesoro were performing work on units at three out of the five refineries in the Bay Area, Bloomberg News reported. Additionally, BP's Cherry Point refinery in Washington State also was down but could restart production the week of May 21. There are a limited number of refineries that produce California's regulated blend of gasoline, a petroleum analyst said. As a result, gas inventories on the West Coast were at their lowest levels in 20 years.  
Source: <http://www.sandiego6.com/news/local/Refinery-Problems-Continue--to-Hurt-Californias-Gas-Supply-151408945.html>

3. *May 14, Charleston State Journal* – (West Virginia; National) **Alpha establishes mine safety foundation.** Alpha Natural Resources officially announced the establishment of the Alpha Foundation for the Improvement of Mine Safety and Health May 14. The non-profit organization will seek to improve mine health and safety by funding academic and nonprofit research projects. Alpha contributed \$48 million to the foundation. It was created as part of Alpha Natural Resources' non-prosecution agreement with the U.S. Attorney's Office of Southern West Virginia from December 6. The agreement followed the Upper Big Branch explosion in Raleigh County where 29 coal miners died. The settlement totaled about \$209 million, of which \$80 million was to go to directly improve mine safety at all Alpha underground mines. The foundation is to operate independently of the U.S. attorney's office or Alpha Natural Resources.  
Source: <http://www.statejournal.com/story/18373163/alpha-establishes-mine-safety-foundation>

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

## **Chemical Industry Sector**

4. *May 15, KSLA 12 Shreveport* – (Arkansas) **Blown transformer causes gas and acid tanks to explode.** Ambulance, fire, and emergency responders in Union County responded to the El Dorado Chemical Company plant in El Dorado, Arkansas, for an explosion early May 15. According to a Union County sheriff's deputy, a transformer on site blew right next to a gas tank. That explosion caused another tank nearby to explode as well. The deputy confirmed the other tank was an acid tank.  
Source: <http://www.ksla.com/story/18421086/gas-tank>
5. *May 15, Hickory Daily Record* – (North Carolina) **Train destroys semi in North Carolina crash.** Officials spent more than 6 hours clearing up the wreckage in Long View, North Carolina, May 14, after a tractor-trailer hauling hazardous chemicals became stuck on train tracks and was hit by a train. A Long View police officer was driving early May 14 when he saw the semi-truck stuck on the tracks and two men outside doing something with dollies. He tried unsuccessfully to have Norfolk Southern stop the train. Although the train was going slowly, the truck was ripped in two. More than six agencies, including a HAZMAT team responded. The semi-trailer, owned by CRST Expedited out of Cedar Rapids, Iowa, was hauling disodium trioxosilicate, a white powder. The chemical is reactive with water, the Catawba County Fire Rescue manager said. "It would react with a cup of water, but it was diluted because of the large amounts of rain." Officials covered up the remaining load. There was no environmental impact, according to officials with the N.C. Department of Environment and Natural Resources.  
Source: <http://www.officer.com/news/10714226/train-destroys-semi-in-north-carolina-crash>
6. *May 14, New York Daily News* – (New York) **Owner of Chinatown mom-and-pop shop pleads guilty to selling illegal rat poison.** The owner of a mom and pop shop in the Chinatown section of Manhattan in New York City pleaded guilty May 14 to

selling illegal pesticides during an undercover probe that began after a woman mistook a rat poison called “The Cat Be Unemployed” for medicine and nearly died. The owner faces up to a year in prison. The banned substances were a cockroach killing product containing the unregistered pesticide fipronil and a rat killer containing the pesticide bromadiolone that could be sold only to a licensed professional and used in a non-urban area. The owner admitted to selling the banned products to an undercover official who visited his store on several occasions during the summer of 2011. The owner was 1 of 12 people arrested September 2011 in a joint federal and city investigation. Authorities said the pesticides appeared to come from China and were less expensive than legitimate products.

Source: <http://www.nydailynews.com/new-york/owner-chinatown-mom-and-pop-shop-pleads-guilty-selling-illegal-rat-poison-article-1.1078047?localLinksEnabled=false>

7. *May 14, KOIN 6 Portland* – (Oregon) **Hazmat team sent to tanker on I-5.** A tanker carrying liquefied oxygen south on Interstate 5 May 14 caused a HAZMAT situation near Wilsonville, Oregon, after it momentarily caught fire. “It is estimated that the flash fire, and subsequent explosion, caused approximately 700 gallons of liquid oxygen to be released into the atmosphere,” Tualatin Valley Fire & Rescue (TV&R) reported. The fire department’s hazardous materials team responded. The tanker pulled off to the shoulder at the Ellingsen on ramp, about 2 miles south of Interstate 205. The source of the fire was a failed main valve on the rear tank. The fire was contained to the rear unit and self-extinguished. “The danger of liquid oxygen is that it greatly magnifies any ignition source that it comes into contact with: open flame, electrical spark, etc.,” said a statement from TV&R. The agency said the tanker was towed the evening of May 14 to the company’s site, noting the small amount of liquid oxygen left in the tanker was off-loaded there.

Source: <http://www.koinlocal6.com/news/local/story/Hazmat-team-sent-to-tanker-on-I-5/Rwkuk3azw0yGuSjxcxgk8g.csp>

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

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

8. *May 15, Associated Press* – (Virginia) **Dominion to face extra oversight at Va. nuke plant.** Dominion Virginia Power will face additional federal oversight at its North Anna Nuclear Power Station near Mineral, Virginia, because of a safety violation related to its emergency diesel generators, the U.S. Nuclear Regulatory Commission (NRC) said May 14. Federal regulators said inspectors found that a gasket failure prevented one of the four diesel generators from performing its function following the August 2011 5.8-magnitude earthquake. The failed gasket was not caused by nor related to the earthquake. While it was replaced the same day, inspectors found the plant did not have adequate procedures for installing the gasket. Richmond-based Dominion discussed the issue with federal regulators in April. The NRC deemed it a “white” violation, or one that is of low to moderate safety significance.

Source: <http://www.wtop.com/120/2823543/Extra-oversight-at-Va-uke-plant>

9. *May 14, TCPalm.com* – (Florida) **Unplanned outages prompt increased federal oversight at St. Lucie Nuclear Plant.** The U.S. Nuclear Regulatory Commission (NRC) is increasing its oversight of Unit 1 at the St. Lucie, Florida, nuclear power plant because of several unplanned shutdowns at the facility, TCPalm.com reported May 14. Florida Power and Light Co. (FPL) owns and operates the plant. A spokesman said the outages in August and October 2011 were considered “complicated,” meaning the cause was not obvious or involved more than one system at the unit. The March outage is still under review. As part of the increased oversight, the commission will conduct an “intensive supplemental inspection” at Unit 1. The spokesman said the outages “were all separate issues” but added that FPL officials will be prepared to present all information to the NRC inspectors.  
Source: <http://www.tcpalm.com/news/2012/may/14/unplanned-outages-prompt-increased-federal-at-st/>
  
10. *May 11, U.S. Nuclear Regulatory Commission* – (National) **NRC prioritizes industry responses to request for post-Fukushima flood hazard evaluations.** The Nuclear Regulatory Commission (NRC) updated part of its March 12 request for information from all U.S. nuclear power plants, setting out a schedule for completing flooding hazard re-evaluations recommended by the NRC’s Near-Term Task Force, which examined lessons learned from the Fukushima Dai-ichi nuclear accident in Japan, said a May 11 NRC release. The prioritization schedule, outlined in a letter to every plant owner, gives plants 1, 2, or 3 years to complete the hazard evaluations. The evaluation results could lead to further assessment of potential flooding effects at the plants.  
Source: <http://www.nrc.gov/reading-rm/doc-collections/news/2012/12-055.pdf>

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

## **Critical Manufacturing Sector**

Nothing to report

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

## **Defense Industrial Base Sector**

See item [34](#)

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

## **Banking and Finance Sector**

11. *May 15, Softpedia* – (International) **P2P Zeus variant used to steal debit card details.** As revealed by security experts, Visa, MasterCard, Facebook, Gmail, Hotmail, and Yahoo all have a peer-to-peer (P2P) variant of the Zeus platform in common, Softpedia reported May 15. For each platform, cybercriminals have made a clever scenario, Trusteer reported. When targeting Facebook users, attackers use a Web inject to push an offer that urges users to link their Visa or MasterCard debit cards to their

social media account. By doing so, the victim allegedly earns cash every time he/she purchases Facebook credits. The attacks against Gmail, Hotmail, and Yahoo customers start with the advertisement of a new authentication service called 3D Secure, allegedly connected to the Verified by Visa and MasterCard SecureCode programs. The Hotmail scheme is somewhat similar with the potential victims being informed of the fact that “Windows Live Inc” is concerned about their security, offering a “100% secure, fast and easy” method of preventing fraud by linking the account to the debit card. In each scenario, the customer is presented with a number of textboxes in which he must enter his debit card number, expiration date, security code, and even the PIN.

Source: <http://news.softpedia.com/news/P2P-ZeuS-Variant-Used-to-Steal-Debit-Card-Details-269670.shtml>

12. *May 15, Help Net Security* – (International) **Sophisticated bogus PayPal emails lead to phishing.** PayPal users are being targeted with e-mails purportedly coming from the e-payment giant and asking for their help. The e-mail contains a link that will supposedly take users to PayPal’s log-in page but lands them on a spoofed one. Once users “log in,” they are asked to fill in personal and financial data, including name, birth date, phone number, home address; debit/credit card type, number, expiration date, and card verification number; Social Security number and two security questions and answers. Once submitted, this information is sent to the scammers who can use it to hijack the PayPal account and perform identity theft. Hoax-Slayer warns this scam is a bit more sophisticated than previous ones, as the text of the scam message is rather accurate, and the address of the fake Web site includes “paypal” along with a long string of numbers and letters. “The fake site includes all of the elements and navigation links familiar to PayPal users. However, clicking these links does not lead to another part of the site as expected but simply reloads the same scam form,” a researcher pointed out.

Source: <http://www.net-security.org/secworld.php?id=12930&utm>

13. *May 14, Reuters* – (National; International) **SEC charges China Natural Gas, chairman with fraud.** A China-based natural gas company and its chairman were charged with fraud by the U.S. Securities and Exchange Commission (SEC) for concealing loans designed to benefit the chairman’s family. In January 2010, the chairman and former chief executive (CEO) of China Natural Gas Inc. (CNG) arranged for two improper loans totaling \$14.3 million, and then lied about them to the company’s board, investors, and auditors, the SEC said May 14. According to the SEC, the former CEO concealed a \$9.9 million loan made through a sham borrower to a real estate firm owned by his son and nephew. It said he also concealed a \$4.4 million loan to Shaanxi Juntai Housing Purchase Co. The SEC said the CEO told CNG directors the loans involved senior Chinese government officers in charge of a liquid natural gas project, and “repeated this lie” to investors on a quarterly earnings conference call. It also said CNG did not properly report a \$19.6 million acquisition made in the fourth quarter of 2008. The lawsuit seeks civil fines and a ban on the CEO from acting as an officer and director of a public company. In September 2011, CNG announced the CEO’s resignation and said it would restate some financial results.

Source: [http://newsandinsight.thomsonreuters.com/Legal/News/2012/05\\_-\\_May/SEC\\_charges\\_China\\_Natural\\_Gas,\\_chairman\\_with\\_fraud/](http://newsandinsight.thomsonreuters.com/Legal/News/2012/05_-_May/SEC_charges_China_Natural_Gas,_chairman_with_fraud/)

14. *May 14, Washington, D.C. Examiner* – (Virginia) **Suspects wanted in 4 Virginia bank robberies.** Investigators believe the same culprits are behind four armed bank robberies in central Virginia, the Washington, D.C. Examiner reported May 14. The robberies happened in Sussex and Chesterfield counties in March and April. The FBI said in May that authorities determined the heists are linked based on statements from witnesses and a review of surveillance photographs from the robberies. One robber entered the bank in the first two heists; two suspects were seen in the other two robberies, according to the FBI. The suspects brandished handguns in all of the incidents, and a shot was fired during one robbery.  
Source: <http://washingtonexaminer.com/local/crime/2012/05/suspects-wanted-4-virginia-bank-robberies/610806>
  
15. *May 14, Housingwire* – (National) **Suspected mortgage fraud tops FinCen list.** Potential mortgage fraud reports recorded in 2010 and 2011 accounted for 37 percent of all suspicious mortgage-related activity filings in the past decade, the U.S. Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN) said in a new study. Between the years 2010 and 2011, suspicious activity reports (SARs) citing potential mortgage fraud shot up 31 percent, hitting 92,028 filings in 2011, compared to 70,472 in 2010. Suspected mortgage fraud is now the most popular subject for a SAR, outstripping suspected check fraud for the number one spot. FinCEN suggested the recent 2-year spike in fraud reports is directly tied to mortgage repurchase demands filed by financial firms that are now questioning the initial underwriting and other issues associated with the original mortgage.  
Source: <http://www.housingwire.com/news/suspicious-mortgage-activity-reports-hit-crescendo-2010-2011>

For another story, see item [40](#)

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

## **Transportation Sector**

16. *May 15, Chicago Sun-Times* – (Illinois) **Fifth rock-throwing incident in a week damages cars on expressways.** Vandals throwing debris onto Chicago-area expressways damaged more than a dozen vehicles in at least five separate incidents in recent days, including two May 14. A white Toyota utility vehicle windshield was broken during the first incident May 14 on the Eisenhower Expressway near Pulaski Road, a State Police District Chicago trooper said. Illinois Department of Transportation crews found the projectile was thrown from the top of the overpass. Two drivers were examined, but neither suffered serious injuries. Less than 4 hours later, witnesses saw kids throwing rocks at cars on I-57 from a bridge. May 13, five cars were damaged by rocks. Prosecutors charged two teens May 10 for allegedly throwing rocks at vehicles on the Chicago Skyway, May 9. They were charged with one count of felony vehicular endangerment and six counts of misdemeanor criminal damage to property, police said. Seven vehicles were hit with projectiles that damaged hoods and windshields, Calumet Area police said.

Source: <http://www.suntimes.com/news/metro/12529505-418/fifth-rock-throwing-incident-in-a-week-damages-cars-on-expressways.html>

17. *May 15, CNN* – (New Jersey) **Authorities: Security company supervisor at NJ airport used dead man’s identity.** A man who supervised more than 30 private security guards at Newark-Liberty International Airport in New Jersey was accused of being an illegal immigrant who took the identity of a man killed 20 years ago, the Port Authority of New York and New Jersey said May 14. The man began working as a private security guard in 1992 while allegedly using the identity of a man who was killed earlier that year, according to a Port Authority representative. He said the immigrant from Nigeria passed numerous background checks with the New Jersey State Police and Border Protection. An anonymous tip several weeks ago helped investigators build a case. The man was arrested and charged with identity theft. He worked at four private security companies over the last 20 years, most recently with FJC Security since 2003, and he had access to various secure areas of the airport including the runways; however, he was not a Transportation Security Administration employee.  
Source: <http://edition.cnn.com/2012/05/14/us/new-jersey-airport-arrest/index.html?iref=allsearch>
18. *May 15, St. Louis Post-Dispatch* – (Illinois) **Bus driver ticketed in I-55 crash that hurt sixth graders.** Police said they fault the school bus driver who smashed into the back of a tractor-trailer on Interstate 55 near Litchfield, Illinois, May 14. More than a dozen sixth graders who were riding the bus on a field trip were injured. The bus driver was issued a ticket for failure to reduce speed to avoid an accident. An Illinois State trooper said the accident reconstruction will take several weeks, as investigators compute the speed and inspect the bus and truck. The crash involved 33 students from Grantfork Upper Elementary School in the Highland School District, as well as 2 teachers, and 5 chaperones. The right front of the bus was demolished, but none of the injuries were considered life threatening. The Illinois State Police said 10 injured people were transported from the scene to nearby hospitals. One student was airlifted to a medical center and was reported to be in fair condition.  
Source: [http://www.stltoday.com/news/local/illinois/bus-driver-ticketed-in-i--crash-that-hurt-sixth/article\\_f1ab4dfc-9e91-11e1-9622-001a4bcf6878.html](http://www.stltoday.com/news/local/illinois/bus-driver-ticketed-in-i--crash-that-hurt-sixth/article_f1ab4dfc-9e91-11e1-9622-001a4bcf6878.html)
19. *May 15, WMAR 2 Baltimore* – (Maryland) **Tractor trailer carrying bleach overturned on I-70.** A tractor trailer carrying 44,000 pounds of bleach overturned on I-70 Westbound at Mile Marker 46 near Frederick, Maryland, May 14. The driver sharply steered the vehicle onto the right shoulder to avoid hitting another vehicle, causing the truck to overturn. None of the bleach spilled into the roadway, but when the trailer stopped, it was blocking all the westbound lanes of I-70. I-70 reopened to all traffic about 6 hours later.  
Source: <http://www.abc2news.com/dpp/news/state/tractor-trailer-overturned-on-i-70>

For more stories, see items [5](#), [7](#), [22](#), [25](#), and [50](#)

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

## Postal and Shipping Sector

20. *May 14, Taunton Daily Gazette* – (Massachusetts) **Hazmat crew removes suspicious parcel from Dighton Post Office.** A HAZMAT crew responded to the Dighton, Massachusetts Post Office and removed a suspicious piece of mail May 14. Postal workers called emergency responders after discovering a powdery substance on a piece of mail, according to the Dighton Fire Department. The Massachusetts Department of Fire Services sent two men wearing HAZMAT suits into the post office to remove the parcel. A postal truck was also cordoned off. The Dighton fire chief said the department was waiting for results from the State laboratory. In addition to the Department of Fire Services, an agent from the FBI and a postal inspector responded. The post office was closed for the day. While the questionable parcel was in the building, the postal truck that carried the mail was cordoned off by the HAZMAT crew, a Dighton selectman said. “The truck went off and delivered mail to about 50 or 60 houses,” he said. “The powder was all over the truck. When they brought it back to the post office, that’s when they called the HAZMAT.”

Source: <http://www.tauntongazette.com/topstories/x255395046/Hazmat-crew-removes-suspicious-parcel-from-Dighton-Post-Office>

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

## Agriculture and Food Sector

21. *May 15, Food Safety News* – (International) **FDA: Safety violations at India plant linked to tuna Salmonella outbreak.** As the case count continued to rise in the nationwide Salmonella outbreak linked to raw tuna, an inspection by U.S. health officials revealed unsanitary conditions at the India facility that produced the implicated tuna product, Food Safety News reported May 15. April 19, about a week after authorities announced a ground yellowfin tuna product imported by Moon Marine USA Corporation was the likely source of the Salmonella bacteria that sickened people, health inspectors began a 6-day review of the plant where the tuna was processed. The resulting report — issued by FDA’s Department of Health and Human Services (HHS) — detailed a series of 10 sanitation slip-ups. Of the offenses, four were violations of Hazard Analysis and Critical Control Points (HACCP) guidelines, which all foreign producers must comply with to export seafood to the United States. A HACCP plan identifies all points in the processing where contamination could occur, and outlines steps to prevent pathogens from entering food. HHS officials also reported the facility’s water and ice, which come into contact with fish during processing, were dirty. They also found product residue on the ceiling and on cutting knives and peeling paint above the processing line. The outbreak involving the company’s tuna scrape sickened at least 258 people.

Source: <http://www.foodsafetynews.com/2012/05/investigation-facility-linked-to-tuna-salmonella-outbreak-unsanitary/>

22. *May 15, Associated Press* – (New York) **Tons of yogurt spilled in highway wreck.** Crews were at the scene of a tractor-trailer crash outside Binghamton, New

York, that sent thousands of pounds of yogurt spilling alongside a highway May 14. WBNG 12 Binghamton reported a truck hauling 36,000 pounds of Chobani yogurt was traveling west on Interstate 88 (I-88) when it crashed on a curve and overturned in the town of Chenango. WBNG reported that all of the yogurt spilled on the highway's shoulder and down a hillside. The sheriff's office said crews were still cleaning up the crash scene May 15. The man who was driving the truck was ticketed for failure to reduce speed and improper lane use. The westbound lanes of I-88 were closed for a time after the crash.

Source: <http://www.timesunion.com/local/article/Tons-of-yogurt-spilled-in-highway-wreck-3559366.php>

23. *May 15, Davenport Quad-City Times* – (Colorado; Iowa) **Colorado issues quarantine for horse virus.** The Colorado Department of Agriculture quarantined a Douglas County ranch after confirming one case of a potentially fatal horse virus, the Davenport Quad-City Times reported May 15. State officials said the horse was brought to Colorado from Iowa and was euthanized after showing signs of the disease. State agriculture officials said the latest equine herpes virus case was not associated with a show or event like the one blamed for a serious outbreak in 2011. Infected animals usually get sick between 2-14 days after they are exposed to the virus.

Source: [http://qctimes.com/news/state-and-regional/iowa/colorado-issues-quarantine-for-horse-virus/article\\_c93dea87-f202-5fb9-8335-4d357d21a5b7.html](http://qctimes.com/news/state-and-regional/iowa/colorado-issues-quarantine-for-horse-virus/article_c93dea87-f202-5fb9-8335-4d357d21a5b7.html)

24. *May 14, WHNS 21 Greenville* – (South Carolina) **DHEC investigates E. coli outbreak in Spartanburg Co.** The South Carolina Department of Health and Environmental Control (DHEC) was investigating several cases of E. coli after many people reported symptoms connected with the bacteria, WHNS 21 Greenville reported May 14. DHEC officials said the outbreak was related to dining at a Spartanburg-area Mexican restaurant during the last week of April and early May. Officials said they were continuing to investigate the outbreak to determine if there was a significant public health risk, and if the threat and potential for transmission was ongoing. Health officials said they were interviewing more than eight people, two of whom reported the infection progressed to a severe condition associated with E. coli infection that can lead to kidney failure. DHEC officials said they would not release the name of the restaurant, per department policy, until a certain threshold is met. So far, they said there does not appear to be an ongoing threat.

Source: <http://www.foxcarolina.com/story/18373547/dhec-investigates-e-coli-outbreak-in-spartanburg-co>

For another story, see item [55](#)

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

## **Water Sector**

25. *May 15, WAGA 5 Atlanta* – (Georgia) **Water main break affects traffic in Sandy Springs.** A water main break on Abernathy Road in Sandy Springs, Georgia, continued to slow traffic May 15. The main gave way May 14 after joint failure, spilling water

that closed the road's westbound lanes. Emergency officials said the 12-inch main was repaired, but crews still had to fill the damaged area, pour cement, and then plate the area. Officials estimated the lanes would be open to traffic late the afternoon of May 15. They said the joint that failed was recently replaced by the City of Atlanta Watershed Management.

Source: <http://www.myfoxtatlanta.com/story/18407755/water-main-break-affects-traffic-in-sandy-springs>

26. *May 15, Tuscaloosa News* – (Alabama) **Uniontown sewage fix will cost more than \$4M.** A team of engineers and consultants unveiled a \$4.4 million plan May 14 to overhaul and upgrade the Uniontown, Alabama sewer system, which has leaked untreated wastewater since 2005. The work includes sewer line repairs, upgrades to the wastewater treatment plant, and the purchase of 40 acres to serve as a second sprayfield for treated wastewater. Construction is expected to take about 18 months to complete, officials said. The upgrades are extensive, and Uniontown officials agreed to borrow at least \$2.5 million to get the project started. The failures of Uniontown's 40-year-old sewer system have been extensively documented through Alabama Department of Environmental Management records for the past 7 years.

Source:

<http://www.tuscaloosanews.com/article/20120515/NEWS/120519851/1291/news?p=1&tc=pg>

27. *May 12, New Castle News Journal* – (Delaware) **United Water lifts 'boil water' advisory.** Delaware United Water lifted a precautionary boil water advisory May 12 that was put in place for many communities in Delaware May 11 following a major water-main break. The break was repaired, but the company advised customers using water for consumption to boil it until samples could be collected and tested. After consulting with the Delaware State Office of Drinking Water, the company lifted the advisory May 12 after tests determined the water system had not been compromised. The situation affected nearly 150 communities in the Brandywine Hundred area. The affected areas were located generally between Interstate 95 on the east, Route 202 to the west, Naamans Road to the north, and Silverside Road to the south.

Source: <http://www.delawareonline.com/article/20120512/NEWS/120512017/United-Water-lifts-boil-water-advisory?odyssey=tab|topnews|text|Home>

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

## **Public Health and Healthcare Sector**

28. *May 15, KGTV 10 San Diego* – (California) **Fire damages medical building in Bankers Hill.** An electrical fire in Bankers Hill damaged a medical building in San Diego, California, May 15. Fire units arrived to find smoke and flames all around the exterior of the building. Firefighters were able to knock the fire down quickly, but wood shingles on the exterior made it difficult to fully extinguish the flames. The flames were contained to the outside of the building, but the interior suffered smoke damage. Firefighters were forced to chop open the side of the building as smoke threatened the upper floors of the medical practice building. The fire was knocked

down in about 10 minutes. Firefighters said an electrical issue was to blame.

Source: <http://www.10news.com/news/31065602/detail.html>

29. *May 15, Associated Press* – (Illinois) **Chicago hospital worker charged with theft of patient's credit card information.** Authorities say a Chicago hospital worker was charged with stealing patients' credit card information to pay her own bills. A Cook County State's attorney announced the charges May 14. The woman worked at Northwestern Memorial Hospital for 4 years. Prosecutors said police began investigating suspicious credit card activity tied to her water bill. Computer records showed payments being made from her home or from the hospital. Victims were hospital patients and some were being treated for cancer. Police found patients' personal information when they executed a search warrant at the woman's home.

Source:

<http://www.therepublic.com/view/story/b33df9c73d634a80b4751de56bec982a/IL--Patient-Information-Theft/>

30. *May 12, Los Angeles Times* – (California) **Personal data for home care workers, recipients lost in the mail.** Sensitive personal information for more than 700,000 people who provide or receive home care for the elderly and disabled may have been compromised when payroll data went missing in the mail, California officials revealed May 11. The breach occurred when Hewlett-Packard, which handles the payroll data for workers in California's In-Home Supportive Services program, was shipping information including Social Security numbers to an office in Riverside in April. The package arrived damaged and incomplete. Advocates and union officials expressed alarm not only at the breach, but also at the procedure for transporting sensitive personal data — a package of microfiche sent via the U.S. Postal Service. The State opened an internal investigation and notified law enforcement, said a spokesman for the California Department of Social Services. Notices will be sent to everyone who may be affected, and officials were reviewing policies to prevent future problems.

Source: <http://www.latimes.com/news/local/la-me-0513-homecare-workers-20120513,0,1683191.story>

For another story, see item [40](#)

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

## **Government Facilities Sector**

31. *May 15, WBOC 16 Salisbury* – (Maryland) **Talbot school assault plan foiled.** The Talbot County, Maryland sheriff's office said Easton High School in Easton was the target of a planned attack by a current student, WBOC 16 Salisbury reported May 15. The plan was extensive, according to police, and would have allegedly involved the use of bombs and firearms to attack the building, students, and faculty. Parents were notified by voice message of the alleged plot 2 weeks after the arrest was made. The sheriff's office said the student was released to the custody of his family and was being monitored by a GPS ankle bracelet.

Source: <http://www.wboc.com/story/18382176/talbot-school-assault-plan-foiled>

32. *May 14, KFSN 30 Fresno* – (California) **Caustic substance found at Fresno IRS.** Federal investigators were trying to figure out who mailed a powdery substance to the Internal Revenue Service in Fresno, California, May 14. Employees were opening mail and found two different envelopes full of white powder. The fire department established a command center and their HAZMAT team determined the powder is caustic. “When it gets on your skin, if your skin was moist or if you had water it would react, it could cause burns or skin irritation,” a Fresno fire official said. The area was isolated and the powder removed.  
Source: <http://abclocal.go.com/kfsn/story?section=news/local&id=8661568>
33. *May 14, Associated Press* – (Washington) **Suspicious package outside Wash. justice center.** A Benton County sheriff’s officer said a package left outside the justice center May 14 in Kennewick, Washington, was made to look like a bomb with black tape and a pipe but had no explosive device. He said the package was filled with screws. It was blown up by the Richland bomb squad. Informational pickets spotted the package. Part of the building was evacuated.  
Source: <http://www.thenewtribune.com/2012/05/14/2144851/suspicious-package-outside-wash.html>
34. *May 14, TG Daily* – (National) **Anonymous claims access to classified U.S. databases.** A hacker affiliated with Anonymous claims the collective has access to U.S. classified databases, TG Daily reported May 14. The hacker faces 15 years in prison for assaulting the county Web site of Santa Cruz, California, and is currently hiding out in Canada to avoid prosecution, courtesy of what he describes as a new “underground railroad,” or a network of safe houses across the country. He told Canada’s National Post that the collective has access to “every classified database” in the U.S. government. According to the hacker, the digital keys were handed to Anonymous operatives by the same “people who run the systems.” He emphasized it was only a matter of time before the collective chose to disseminate database contents. “Now people are leaking to Anonymous and they’re not coming to us with this document or that document or a CD, they’re coming to us with keys to the kingdom, they’re giving us the passwords and usernames to whole secure databases that we now have free reign over,” he added.  
Source: <http://www.tgdaily.com/security-features/63368-anonymous-claims-access-to-classified-us-databases>
35. *May 14, Jacksonville Daily News* – (North Carolina; National; International) **Officials: Nearly \$2 million in guns, combat gear sold to gangs.** U.S. military officials confirmed a wide-reaching investigation by authorities in Jacksonville, North Carolina, uncovered a criminal conspiracy within the Armed Forces to steal and sell nearly \$2 million in guns and combat gear to gangs in the United States and foreign countries including China, the Jacksonville Daily News reported May 14. Commanders from Camp Lejeune and II Marine Expeditionary Force were working closely with the Naval Criminal Investigative Service (NCIS) during the investigation, said the deputy director of public relations for Marine Corps Installations East. The probe began more than a year and a half ago. NCIS recovered \$1.8 million in stolen guns and combat gear. Those involved are accused of stealing, over-ordering, or otherwise obtaining

equipment and selling guns locally and other gear over the Internet. With cooperation from Marine and Navy officials, NCIS was able to conduct 66 investigations involving 47 active duty Marines and sailors and 21 civilians who are now in various stages of prosecution. NCIS agents identified stolen property from the Army and Air Force which launched numerous investigations involving soldiers and airmen, military officials confirmed.

Source: <http://www.jdnews.com/articles/gear-103897-officials-guns.html>

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

## **Emergency Services Sector**

36. *May 15, Associated Press* – (Maine) **Radio jamming again a problem in York County.** Authorities thought the threat of a federal investigation finally stopped the person jamming Maine’s York County emergency radio transmissions, often delaying responses, but after several weeks without a problem the mystery jammer is apparently back at work. The Lebanon fire chief said the latest incident occurred May 12 as firefighters called for mutual aid to battle a mobile home fire in Lebanon. Firefighters were unable to communicate with dispatchers. The chief said response was delayed by 5 to 10 minutes. The mobile home was destroyed, and three others nearby were damaged.  
Source: <http://www.seacoastonline.com/articles/20120515-NEWS-120519853>
37. *May 15, Fitchburg Sentinel & Enterprise* – (Massachusetts) **Suspicious powder found at Shirley prison third time in recent weeks.** Fire crews and hazardous-materials teams May 14 responded to the Souza-Baranowski Correctional Center in Shirley, Massachusetts, for the third time in days after white powder fell from mail addressed to a prisoner. A correctional officer was opening a piece of prisoner’s mail sent through the prison’s internal services when white powder fell from the envelope, said a State Department of Corrections spokeswoman. Notification protocol was followed, including a call to the Lancaster Fire Department and other HAZMAT team members. Officials tested the substance and determined it was not a biohazard. Further testing will determine exactly what the substance was at a later date. In an incident the week of May 7, a worker at the prison found an envelope containing white powder that had been sent via the U.S. Postal Service. Before that, an employee found a suspicious pink powder in an internally sent message.  
Source: [http://www.sentinelandenterprise.com/local/ci\\_20626171/suspicious-powder-found-at-shirley-prison-third-time](http://www.sentinelandenterprise.com/local/ci_20626171/suspicious-powder-found-at-shirley-prison-third-time)
38. *May 14, Memphis Commercial Appeal* – (Mississippi) **Mississippi authorities see links in two recent roadway slayings, urge public calm.** Authorities said they know the recent shooting deaths of two people in separate incidents along north Mississippi highways are connected and are asking the FBI for help. The DeSoto County, Mississippi district attorney said in a news conference May 14 there is “speculation” the two victims may have been pulled over by someone impersonating a police officer. The speculation caused the Tate County Sheriff’s Department to post a warning for drivers on its Facebook page: “If someone attempts to pull you over with flashing lights

and you feel unsure of stopping, DON'T PULL OVER," the post read. "Use your cell phone and dial 911 and if it's a real officer then the dispatcher will confirm it for you and if it's not a real officer they will send help to you." The district attorney said if motorists are unsure if a vehicle stopping them is a law enforcement officer, the motorist is allowed by state law to turn on emergency flashers, call 9-1-1, and drive to a lighted public facility or to a police or sheriff's office. Motorists can also call \*47 on cell phones to report suspicious activity.

Source: <http://www.commercialappeal.com/news/2012/may/14/mississippi-authorities-see-links-two-recent-roadw/>

39. *May 14, San Diego Reader* – (California) **Email of retired government security agent in San Diego hacked by Anonymous, letter says.** The San Diego Reader reported May 14 that e-mail accounts of a retired agent for the California Department of Justice who was a member of a high-powered law enforcement computer security team in San Diego were compromised by Anonymous. Social Security numbers of an undisclosed number of unidentified individuals were contained in the stolen information. News of the incident was furnished in a notification letter from the response team posted online May 11 by the California attorney general's office, as required by State law for breaches involving unauthorized release of confidential electronic information.

Source: <http://www.sandiegoreader.com/weblogs/news-ticker/2012/may/14/email-of-retired-government-security-agent-in-san-/>

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

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

## **Information Technology Sector**

40. *May 15, Wired* – (International) **Popular surveillance cameras open to hackers, researcher says.** Three of the most popular brands of closed-circuit surveillance cameras are sold with remote Internet access enabled by default, and with weak password security — a classic recipe for security failure that could allow hackers to remotely tap into the video feeds, according to new research. The cameras, used by banks, retailers, hotels, hospitals, and corporations, are often configured insecurely — thanks to these manufacturer default settings, said a senior security engineer at Gotham Digital Science. As a result, he says, attackers can seize control of systems to view live footage, archived footage, or control the direction and zoom of adjustable cameras. The researcher and his team were able to view footage as part of penetration tests they conducted for clients to uncover security vulnerabilities.

Source: <http://www.wired.com/threatlevel/2012/05/cctv-hack/>

41. *May 15, The Register* – (International) **Apple scrubs old Leopards of Flashback trojan infections.** Apple released patches that defend users of its older Mac OS X 10.5 Leopard operating system against security threats. The May 14 security fixes help defend Mac users on the 2-year-old operating system against assaults by the Flashback trojan. Users of the newer Snow Leopard (10.6) and Lion (10.7) operating systems

received equivalent fixes in April. Apple's Leopard Flashback Removal Security Update is designed to clean Macs running the legacy OS that are not yet running an anti-virus package. In addition, the security update disables Safari's Java plugin by default. Leopard Security Update 2012-003 disables older versions of Adobe Flash Player, encouraging users to get the latest version directly from Adobe's Web site. Both updates can be applied via the Software Update feature built into Mac OS X, but will only work if the latest version of that particular track of the operating system, Mac OS X Leopard version 10.5.8, has already been applied. Apple is acting to prevent users of legacy versions of its operating system from harboring the Flashback trojan. Such support is unlikely to continue indefinitely and is likely to disappear entirely once Apple updates Mac OS X 10.7 Lion.

Source: [http://www.theregister.co.uk/2012/05/15/mac\\_leopard\\_security\\_update/](http://www.theregister.co.uk/2012/05/15/mac_leopard_security_update/)

42. *May 15, Softpedia* – (International) **'How to Earn Money' apps hide fraud trojan.** Cybercriminals are starting to focus their attention on scams that advertise methods and products that rely on applications. Experts from Bitdefender discovered a piece of software called "How to Earn Money," which can allegedly help users make cash without a hassle. In reality, the shady app hides malware, identified by Bitdefender as Trojan.Fraud.A. Once installed, the program places itself in the Program Files folder, it creates shortcuts, and starts pushing HTML pages that advertise a tool that can help users earn tens of thousands of dollars in just over a month. To gain possession of the tool, users must pay a fee of \$37 or \$47.  
Source: <http://news.softpedia.com/news/How-to-Earn-Money-Apps-Hide-Fraud-Trojan-269618.shtml>
43. *May 15, H Security* – (International) **Fraunhofer Institute finds security vulnerabilities in cloud storage services.** The Fraunhofer Institute for Secure Information Technology tested seven cloud storage service providers and published its results in a report. The authors of the report found vulnerabilities affecting registration and login, encryption, and shared access to data for several services. The study looked at CloudMe, CrashPlan, Dropbox, Mozy, TeamDrive, Ubuntu One, and Wuala. The functions examined by Fraunhofer were copying, backup, synchronization, and sharing. Only TeamDrive and Wuala offer all four of these features. CrashPlan and Mozy only offer a backup service — a service not offered by CloudMe, Dropbox, or Ubuntu One.  
Source: <http://www.h-online.com/security/news/item/Fraunhofer-Institute-finds-security-vulnerabilites-in-cloud-storage-services-1575935.html>
44. *May 15, H Security* – (International) **Avira AV update hangs systems.** A faulty update for Avira's paid-for anti-virus software blocks harmless processes and may, in some cases, stop computers from booting. The update results in the ProActiv behavioral monitoring component becoming oversensitive in treatment of executable files. According to user reports, ProActiv blocks trusted system processes such as cmd.exe, rundll32.exe, taskeng.exe, wuauc.lt.exe, dllhost.exe, iexplore.exe, notepad.exe, and regedit.exe. In some cases, this results in Windows failing to boot properly. It also appears to be blocking non-OS applications such as Microsoft Office, the Opera Web browser, and Google's Updater. All versions that include the ProActiv monitoring component are affected, including Avira Antivirus Premium 2012 and the enterprise

version; only 32-bit systems are affected, as ProActiv does not currently support 64-bit operating system. Users who installed the update are advised to disable ProActiv. In a statement to the H's associates at heise Security, Avira confirmed the problem and said developers are working on an automatic update to resolve the bug. The potential scale of the bug is huge — according to Avira, the faulty update was already downloaded more than 70 million times (this figure includes those running the free version of Avira which is not affected). The company stopped distributing the update.

Source: <http://www.h-online.com/security/news/item/Avira-AV-update-hangs-systems-1575974.html>

45. *May 14, SecurityWeek* – (International) **Trend Micro reveals top document attack vectors from April.** Trend Micro researchers recently revealed just how prevalent the use of certain document types is among attackers. By far, the two most popular document formats for hackers targeting Microsoft Office software are Word and Excel files, which were used in a combined 90 percent of attacks on Microsoft Office in April. The biggest reason for this is that the two most reliable exploits used by hackers targeted CVE-2010-3333 and CVE-2012-0158, which are both Word vulnerabilities. Source: <http://www.securityweek.com/trend-micro-reveals-top-document-attack-vectors-april>

For more stories, see items [11](#), [12](#), [34](#), [39](#), and [47](#)

### 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

46. *May 15, Naples Daily News* – (Florida) **WGCU back on the air after lightning strike.** After a day and a half of silence, WGCU 90.1 FM Fort Myers, Florida, was back on the air May 15. A lightning strike May 13 to a radio tower near Florida Gulf Coast University disrupted service to the public broadcasting station for 38 hours. The station relied on Internet radio and mobile device applications to continue programming. WGCU's companion television station was not affected during the outage, nor was its radio affiliate, WMKO 91.7 FM Marco Island. Source: <http://www.naplesnews.com/news/2012/may/15/wgcu-back-air-after-lightning-strike/>
47. *May 15, PCWorld* – (National) **Debut of cut-rate mobile plan marred by alleged malicious attack.** The launch of a cut-rate unlimited mobile plan offered by upstart Voyager Mobile was marred May 15 by what the company claims is “a malicious network attack to its primary website.” The company now says it is postponing the

launch of its budget plan until an unspecified date. Voyager posted a note to its Web site: “Due to the network outage, Voyager Mobile is postponing its launch to a time and date in the very near future.” Voyager declined to comment when asked about the alleged attack, and it is unclear why any group or individual would target this company. Source:

[http://www.pcworld.com/article/255609/debut\\_of\\_cutrate\\_mobile\\_plan\\_marred\\_by\\_alleged\\_malicious\\_attack.html](http://www.pcworld.com/article/255609/debut_of_cutrate_mobile_plan_marred_by_alleged_malicious_attack.html)

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

## **Commercial Facilities Sector**

48. *May 15, CNY Central* – (New York) **Three injured in Watertown apartment building fire, arson suspected.** Three people were hospitalized May 15 after their Watertown, New York apartment building was set on fire. The Watertown Fire Department battalion chief said the first arriving fire crews found the front porch of the building “lit up” with heavy fire, with flames blocking the two staircases that lead to apartments inside. The building contained eight apartments, four of which were occupied at the time of the fire. He said residents were inside when the fire started, and three individuals were unable to get out because the fire was blocking the stairs. The chief said the building was a “total loss.” He said a witness claimed to have seen someone pouring gasoline on the front porch, and the fire’s location could be an indicator the fire was set with the intention of keeping those inside from escaping. Source: <http://www.cnycentral.com/news/story.aspx?id=753928#.T7JpPIJqFBk>
49. *May 15, Merrillville Post-Tribune* – (Indiana) **Three taken to hospital after Portage blaze.** Two employees and a firefighter were taken to the hospital after a fire destroyed a Portage, Indiana business May 14. The assistant fire chief said two employees of National Transmission suffered from smoke inhalation, and the firefighter might have suffered a heat-related injury. The employees told fire officials they were in the front of the building when the fire started. They reported hearing a loud noise in the back of the building and then seeing a lot of smoke. It took more than 3 hours to fight the fire, and the assistant fire chief said they were delayed because the gas meter was destroyed by the fire, so they had to wait for it to be turned off. Verona Pizza, which sits right next to National Transmission, suffered some damage, as did some cars in a nearby lot. The chief said the damage from the fire was so bad that officials will likely never know what caused it. Source: <http://posttrib.suntimes.com/12527019-537/three-taken-to-hospital-after-portage-blaze.html>
50. *May 14, Associated Press* – (California) **6th discarded pipe bomb found in Palm Springs.** Six crude pipe bombs found scattered on desert streets over a 5-day period have Palm Springs, California police and residents on edge as federal authorities join the investigation, a police spokesman said May 14. The pipe bombs, crudely fashioned out of plastic or steel pipe, were clearly assembled by an amateur rather than a terrorist, a police official said. The police department called in the Riverside County Sheriff’s Bomb Squad to handle disposal. The police department, FBI, and Bureau of Alcohol,

Tobacco, Firearms and Explosives partnered to offer a \$15,000 reward for information leading to the arrest and conviction of whoever is responsible. All of the devices were found scattered on north Palm Springs streets within 1 mile of the first pipe bomb discovery May 8. The locations were near homes, mobile home parks, and the open desert. “This is taxing our resources, and they are dangerous,” a police official said. The first bomb was found by a man on his morning walk who took it home His son spotted it in his garage and said he thought it was a pipe bomb. The son took the device to the police department, which had to be evacuated until the sheriff’s bomb squad showed up to disarm what turned out to be a live bomb, a police sergeant said.

Source: [http://www.mercurynews.com/breaking-news/ci\\_20620795/6th-discarded-pipe-bomb-found-palm-springs](http://www.mercurynews.com/breaking-news/ci_20620795/6th-discarded-pipe-bomb-found-palm-springs)

51. *May 14, WVIT 30 New Britain* – (Connecticut) **Drywall causes white powder scare at ESPN.** Bristol, Connecticut police and fire officials responded to ESPN’s mail facility May 14 after white powder was found. Police said the powder was found in three packages at the facility. The Connecticut Department of Energy & Environmental Protection conducted a test and determined it was drywall powder. The building crews responded to is the one through which all routing packages, tapes, and creative materials are sent because of enhanced security, according to ESPN’s media delivery guidelines. The FBI was investigating to determine where the packages came from. Employees who were exposed to the powder went through decontamination. The scare came days after local schools the week of May 7 received letters with white powder. One of those letters said al-Qa’ida “is back.”

Source: <http://www.nbcconnecticut.com/news/local/White-Powder-Found-at-ESPN--151374945.html>

52. *May 14, Associated Press* – (Wyoming) **Bomb threat cancels Eastern Shoshone meeting.** Authorities have been investigating a bomb threat that canceled a meeting to discuss alleged problems at Wyoming’s Eastern Shoshone Housing Authority. About 110 people gathered for the May 12 general council meeting at Rocky Mountain Hall in Fort Washakie were evacuated because of the threat. One attendee told the Riverton Ranger the threat happened shortly after leaders declared there were enough people present to proceed with the meeting. An FBI spokesman confirmed the agency was among those investigating the threat.

Source: [http://trib.com/news/state-and-local/bomb-threat-cancels-eastern-shoshone-meeting/article\\_19b0149f-c782-5cc5-8970-e84e8f87dae7.html](http://trib.com/news/state-and-local/bomb-threat-cancels-eastern-shoshone-meeting/article_19b0149f-c782-5cc5-8970-e84e8f87dae7.html)

For another story, see item [40](#)

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

## **National Monuments and Icons Sector**

53. *May 15, MSNBC; Associated Press; Reuters* – (Arizona) **Snakes, mine shafts challenge crews battling Arizona wildfire.** Firefighters working to protect a historic mining town in northern Arizona were told to expect extreme conditions May 15, with temperatures in the 80s and gusts up to 35 miles per hour that could have fanned an

out-of-control wildfire. Crews were facing additional hazards as well: snakes and abandoned mining shafts. “There are a lot of mine shafts that you don’t see because of the amount of brush,” a spokeswoman for the fire team said. Add rugged terrain to the mix, she said, and conditions are “extremely difficult.” Located south of Prescott in the Prescott National Forest, the wildfire that started May 13 burned 1,700 acres of ponderosa pine and chaparral, and threatens 350 homes in Crown King. Tourists who were in the town left when a mandatory evacuation was ordered May 13, while homeowners were allowed to stay as long as they remained on their property. Some 300 fire personnel were already at the scene, and the first of 400 more were expected May 15. Six air tankers worked May 14 to douse hot spots. Two buildings and one trailer were destroyed, a Prescott National Forest spokeswoman said. The fire, still at zero percent containment, started at a “structure” and was human-caused, she said. Source: <http://usnews.msnbc.msn.com/news/2012/05/14/11705895-snakes-mine-shafts-challenge-crews-battling-arizona-wildfire>

54. *May 14, KUSA 9 Denver* – (Colorado) **Wildfire burning in Poudre Canyon near Hewlett Gulch Trail keeps growing.** Fire crews said they had zero percent containment on a wildfire that continued to burn northwest of Fort Collins, Colorado. The wildfire broke out in Poudre Canyon near the Hewlett Gulch Trail in Roosevelt National Forest May 14. Authorities said structures are near the fire, but none were in immediate danger. The fire was 250 to 280 acres in size and was less than 1 mile from Poudre Park. About 40 firefighters from the U.S. Forest Service and Larimer County Emergency Services responded. Authorities called in a single-engine air tanker. A Type 3 incident team was on the scene May 15, and a Type 2 was planned to follow after them. Three 20-person crews, a Type 1 helicopter, and a heavy air tanker were also ordered to the fire. The Hewlett Gulch Trail and the Greyrock Trail were closed. Source: <http://www.9news.com/news/article/267988/339/No-containment-on-fire-near-Hewlett-Gulch-?odyssey=obinsite>

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

## **Dams Sector**

55. *May 15, Cibola Beacon* – (New Mexico) **Dam at Bluewater Lake gets repairs.** Repairs began May 7 on the Bluewater Lake dam at Bluewater Lake State Park in Cibola County, New Mexico. Maintenance efforts were necessary to fix one of Bluewater Toltec Irrigation District’s (BTID) two main valves at the bottom of the lake used for irrigation. Divers tried to repair the actuator for the 24-inch valve. The actuator is used to open and close the valve, letting irrigation water flow out of the dam to be used by farmers. However, because of the broken valve, there has been no irrigation water from Bluewater Lake for almost 1 year. The team has used six of the 15 days of funding received from the State of New Mexico to fix the actuator. Once the actuator is fixed, however, there will still be a delay in irrigation water to area farmers due to lack of rain, according to officials. Source: [http://www.cibolabeacon.com/news/dam-at-bluewater-lake-gets-repairs/article\\_da0af680-9e81-11e1-a68f-001a4bcf887a.html](http://www.cibolabeacon.com/news/dam-at-bluewater-lake-gets-repairs/article_da0af680-9e81-11e1-a68f-001a4bcf887a.html)

56. *May 14, South Florida Sun-Sentinel* – (Florida) **Work approved to upgrade levees dividing western Broward County from Everglades.** The South Florida Water Management District approved \$18 million of work May 10 to upgrade a 38-mile-long, Broward County section of the East Coast Protective Levee. The levee is designed to protect Coral Springs, Weston, and other western communities from flooding by the Everglades. The levee does not currently meet federal safety standards, raising safety concerns and could lead to increased flood insurance costs if repairs are not made. The work involves: building filter berms and drains, flattening levee side slopes, reconstructing access ramps for ongoing maintenance, and re-compacting the top of the levee after work is finished. Inspectors' concerns about the levee include: erosion, levees being too low, overgrown vegetation obstructing maintenance, fencing and gates in disrepair, slopes being too steep, and culverts needing repair. The district has a 2-year window to make levee fixes before the Federal Emergency Management Agency triggers regulatory changes that could increase South Florida flood insurance costs. Source: <http://www.sun-sentinel.com/news/blogs/green-south-florida/sfl-levee-upgrades-broward-20120514,0,1517467.story?track=rss>
57. *May 14, KETV 7 Omaha* – (Nebraska; Iowa) **Corps of Engineers to work on Omaha riverfront.** The U.S. Army Corps of Engineers began repairs to the flood wall and a flap gate destroyed during the summer of 2011 flooding in Omaha, Nebraska, and Council Bluffs, Iowa, according to KETV 7 Omaha May 14. The quality control manager for the city said engineers will fill the wall with concrete and then fix the flap gate. Crews will determine whether the levees are structurally sound by drilling into the soil. Officials said seepage berms placed around Council Bluffs will stay in place because work on the levee will not start until the end of the summer. The Corps hopes all construction across the midwest will be complete by December 1. Source: <http://www.ketv.com/news/local-news/Corps-of-Engineers-to-work-on-Omaha-riverfront/-/9674510/13387334/-/item/0/-/mtwbbez/-/index.html>

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



**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.