



Homeland
Security

Daily Open Source Infrastructure Report

5 December 2012

Top Stories

- Separate accidents at two West Virginia coal operations November 30 left one worker dead, two others injured, and a fourth worker missing, company and State mine safety officials said. It was the sixth mining fatality in West Virginia this year. – *Associated Press* (See item [2](#))
- Customers of Bank of America, Citibank, and the former Washington Mutual Bank were taken for \$8 million after their accounts were compromised as part of an intricate identity theft and bank fraud scheme that was run for nearly 6 years from the Avenal State Prison in California. – *BankInfoSecurity* (See item [8](#))
- Systems that can track automotive traffic on roadways have flaws that could allow a skilled hacker to break in, according an advisory by the U.S. Industrial Control System Computer Emergency Readiness Team, Government Security News reported December 3. – *Government Security News* (See item [11](#))
- The U.S. Office of Inspector General, which investigates health care fraud, expects to recover about \$6.9 billion from audits and investigations this year. Targets of investigations include hospitals, nursing homes, and the pharmaceutical industry. – *Cincinnati Business Courier* (See item [20](#))

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

1. *December 4, Associated Press* – (Tennessee) **Tenn. refinery worker dies after chemical exposure.** An oil refinery worker died after being exposed to propane and acid at a Valero plant in Memphis, Tennessee, the Associated Press reported December 4. He is the second person to die in 2012 from an on-the-job injury at the plant. The plant has been cited for violations related to the safe handling and control of hazardous energy and chemicals. A Fire Department spokesman said two workers were injured when a sight glass on a pump ruptured, exposing them to a mixture of propane and hydrofluoric acid. A sight glass is a transparent tube or window that allows workers to monitor fluid levels within a tank, pipe, pump or boiler. One of the workers died at the hospital. The second worker and two firefighters have non-critical injuries. A company spokesman said Valero is investigating and that safety is the company's most important concern.
Source: <http://abcnews.go.com/US/wireStory/tenn-refinery-worker-dies-chemical-exposure-17870981#.UL4qSa6p3Tp>
2. *December 3, Associated Press* – (West Virginia) **One dead, one missing in separate coal accidents.** Separate accidents at two West Virginia coal operations November 30 left one worker dead, two others injured, and a fourth worker missing, company and State mine safety officials said. An electrician was killed when he became caught between a scoop and a continuous mining machine at the Pocahontas Mine A White Buck Portal near Rupert in Greenbrier County, West Virginia, said a representative of the State Office of Miners' Health Safety and Training. The mine is owned by White Buck Coal Co., a subsidiary of Virginia-based Alpha Natural Resources. Alpha identified the victim as an employee of its Alex Energy subsidiary. It was the sixth mining fatality in West Virginia this year. In north-central West Virginia, emergency officials were draining a coal slurry pond to search for a bulldozer operator who was unaccounted for after an embankment collapsed, sending three into the water. U.S. Mine Safety and Health Administration spokeswoman said a "massive failure"

occurred November 30 at the Nolans Run impoundment of Pennsylvania-based Consol Energy's Robinson Run mine in Harrison County. One dozer operator and two engineers were on the platform when it collapsed. Both engineers were rescued and were in non-critical condition.

Source: <http://www.chem.info/News/2012/12/Safety-One-Dead-One-Missing-in-Separate-Coal-Accidents/>

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

Chemical Industry Sector

See items [10](#) and [36](#)

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

Nuclear Reactors, Materials and Waste Sector

3. *December 4, Lacey Patch* – (New Jersey) **Oyster Creek returns to service following refueling and maintenance outage.** Oyster Creek Generating Station has returned to service after a 42-day refueling and maintenance outage. According to a December 4 Power Reactor Status Report by the Nuclear Regulatory Commission (NRC), the nuclear power plant was operating at 22 percent. The power generator was taken offline October 22 for a planned refueling outage. Since that outage, the NRC has reported the discovery of “indications,” or precursors to cracks, in the reactor nozzle and a pinhole leak in the reactor vessel head cooling system. Both issues have been resolved, an NRC spokesman said.

Source: <http://lacey.patch.com/articles/oyster-creek-returns-to-service-following-refueling-and-maintenance-outage>

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

Critical Manufacturing Sector

4. *December 4, U.S. Department of Transportation* – (National) **NHTSA recall notice - Ford Escape and Fusion fluid leak fire hazard.** Ford is recalling 80,057 2013 Escape vehicles manufactured from October 5, 2011 through November 26, 2012 equipped with 1.6L engines; and 2013 Fusion vehicles manufactured from February 3, 2012 through November 29, 2012 equipped with 1.6L engines. The engines may overheat leading to fluid leaks that may come in contact with the hot exhaust system. Fluid leaks in the presence of an ignition source such as a hot exhaust system may result in a fire. The remedy for this recall campaign is still under development. Until the recall remedy has been performed, Ford is advising owners to contact their dealer or call the Ford telephone hotline to arrange alternate transportation.

Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rel_ID=12V551000&summary=true&prod_id=1488829&PrintVersion=YES

5. *December 3, U.S. Department of Labor* – (Ohio) **U.S. Labor Department’s OSHA cites ATW Automation with 9 safety violations following worker’s death at Dayton, Ohio, manufacturing facility.** The U.S. Department of Labor’s Occupational Safety and Health Administration December 3 cited ATW Automation Inc. for nine safety violations after a worker sustained blunt force trauma injuries at the company’s machine manufacturing facility in Dayton, Ohio. The worker was caught and pinned by a conveyor that had lowered during a “power down” process, and he died from his injuries a few days later. One repeat violation was cited for failing to conduct and document periodic inspections of specific energy control procedures in the fabrication and tool room departments. Seven serious violations and one other-than-serious violation were also cited. The incident that led to the most recent inspection occurred July 27. Proposed penalties totaled \$63,000.

Source:

http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=23343

6. *December 3, U.S. Department of Labor* – (Connecticut) **U.S. Labor Department’s OSHA cites Pandrol USA in Bridgeport, NJ, for willful and serious violations, proposes \$283,500 in penalties.** The U.S. Department of Labor’s Occupational Safety and Health Administration (OSHA) December 3 cited Pandrol USA LP, a rail fastening system manufacturer, with 25 safety and health violations - including 3 willful - at the company’s Bridgeport, Connecticut facility. A complaint alleging hazards prompted OSHA’s inspection. Proposed penalties total \$283,500. The willful violations involved the employer’s failure to use energy control, or “lockout/tagout” procedures, for mechanical and hydraulic presses; provide machine guarding; and ensure that employees performing maintenance and repairs on machinery are properly trained on energy control procedures. Due to the willful violations, Pandrol has been placed in OSHA’s Severe Violator Enforcement Program, which mandates targeted follow-up inspections to ensure compliance with the law. Twenty serious violations related to OSHA’s noise exposure standard, electrical hazards, a lack of machine guarding and personal protective equipment, not periodically inspecting energy control procedures, failing to develop and implement a confined space program, and not mounting fire extinguishers. Two other-than-serious violations were also cited.

Source:

http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=23346

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

Defense Industrial Base Sector

Nothing to report

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

Banking and Finance Sector

7. *December 3, Marina del Rey Patch* – (California) **Marina del Rey man convicted of bank fraud.** A federal judge November 30 convicted a Marina del Rey, California man of 18 felony counts of bank fraud, identity theft, and money laundering that totaled \$600,000. The man and his brother were convicted of impersonating people to obtain credit card numbers under the victims’ names and applying online for fraudulent credit cards. The man’s brother pleaded guilty before the trial. The man also called several banks, including Chase and Bank of America, and used a person’s credit rating agency profile information to receive credit cards, which he and his brother then used to withdraw money from ATMs and purchase department store gift cards.
Source: <http://marinadelrey.patch.com/articles/marina-del-rey-man-convicted-of-bank-fraud>

8. *December 3, BankInfoSecurity* – (California) **ID theft scam run from prison.** Customers of Bank of America, Citibank, and the former Washington Mutual Bank were taken for \$8 million after their accounts were compromised as part of an intricate identity theft and bank fraud scheme that was run for nearly six years from the Avenal State Prison in California, BankInfoSecurity reported December 3. Federal authorities said members of the Armenian Power gang worked from behind bars with street gangs and bribed bank employees to steal personally identifiable information - including signatures, telephone numbers, prior addresses, and property documents - about elderly accountholders to impersonate them and take over their accounts. Defendants used the stolen information to change accountholder phone numbers and addresses in an effort to conceal their crime. Those changes put control of accounts into the hands of criminals. The losses were suffered by the victims and the affected institutions, according to the FBI. Two ring leaders accused of organizing the scheme were sentenced to 25 years each in federal prison, even while already serving time for other crimes. The two leaders of the fraud managed to conceal their scheme by communicating in code with gang members on the outside through phone conversations.
Source: <http://www.bankinfosecurity.com/id-theft-scam-run-from-prison-a-5327>

9. *December 3, CNN Money* – (International) **SEC charges China affiliates of ‘Big 4’ accounting firms.** The U.S. Securities and Exchange Commission (SEC) announced charges December 3 against the China affiliates of the “Big Four” U.S. accounting firms. The SEC accused PricewaterhouseCoopers Zhong Tian, KPMG Huazhen, Ernst & Young Hua Ming, and Deloitte Touche Tohmatsu of refusing to hand over auditing documents related to Chinese firms that trade on U.S. markets. China’s BDO China Dahua Co. Ltd. was also charged. Regulators said they have been trying for months to gain access to audit documents for nine China-based companies that they are investigating for potential wrongdoing. Deloitte, PricewaterhouseCoopers-China and Ernst & Young Hua Ming blame the dispute on conflicting rules in China and the United States. Under Chinese law, “accounting firms in China are not permitted to produce documents, including audit work papers, directly to any foreign regulator without Chinese government approval, so all firms in China have been unable to produce documents requested by the SEC,” a Deloitte spokeswoman said.
Source: <http://money.cnn.com/2012/12/03/investing/sec-china-accounting/>

Transportation Sector

10. *December 4, WTHI 10 Terre Haute* – (Indiana) **Roads reopened after chemical spill.** Vigo County, Indiana HAZMAT crews said that a sodium hydroxide spill has been cleaned up, and the roads are opened once again, WTHI 10 Terre Haute reported December 4. The tanker carrying the chemical had a leak in the storage container, which broke open further and spilled onto the streets. The dangerous chemical spill shut down several roads on Terre Haute’s south side. Vigo County Central Dispatch said Voorhees Street was closed from 3rd Street to 14th Street and all side streets heading north and south off of Voorhees. The chemical that spilled is called caustic soda; a solution of sodium hydroxide used in water.
Source: <http://www.wthitv.com/dpp/news/local/chemical-spill-shuts-down-th-streets#.UL4YYa6p3Tp>
11. *December 3, Government Security News* – (National) **Highway traffic monitoring system has exploitable electronic flaw, says CERT.** Systems that can track automotive traffic on roadways, providing speed and highway traffic behavior patterns has a flaw that could allow a skilled hacker to break in, according to the U.S. Industrial Control System Computer Emergency Readiness Team (ICS-CERT). A November 30 advisory issued by ICS-CERT said a specific system used by some municipal governments around the country has an authentication vulnerability that could allow unauthorized access. The advisory said Post Oak Bluetooth traffic systems that use Anonymous Wireless Address Matching (AWAM) were affected. AWAM systems detect vehicles that have Bluetooth — enabled networking devices aboard, including cellular phones, mobile GPS systems, telephone headsets, and in-vehicle navigation and hands-free systems. Each of those devices contains a unique electronic address that the AWAM system’s sensors can read as the device travels by on a roadway. An independent research group said ICS-CERT on November 30 identified an insufficient entropy vulnerability in authentication key generation in Post Oak’s AWAM Bluetooth Reader Traffic System. By impersonating the device, an attacker could obtain the credentials of the systems administrative users and potentially perform a Man-in-the-Middle (MitM) attack, intercepting communications within the organization. ICS-CERT said Post Oak has validated the vulnerability and produced an updated firmware version that mitigates the potential opening. ICS-CERT said Post Oak said its products are deployed in the transportation sector, mainly in the U.S.
Source: http://www.gsnmagazine.com/node/27933?c=cyber_security
12. *December 3, Los Angeles Times* – (California) **Jackknifed big-rig closes 134, 210 freeway connectors in Pasadena.** Two transition roads closed at the 134 and 210 freeways in Pasadena, California, December 3 after a big-rig jackknifed on a slick roadway, sending one trailer and cab down an embankment. The truck was carrying two trailers, one of which overturned and blocked the roadway connecting the eastbound 134 to the westbound 210. The westbound 210 connector to the 210 west, along with the eastbound 134 connector to the 210 west, were closed as crews prepared to tow the truck and repair a broken guardrail. The roads were closed for 5 hours.

Source: <http://latimesblogs.latimes.com/lanow/2012/12/jackknifed-big-rig-closes-134-210-freeway-connectors-in-pasadena.html>

13. *December 3, Everett Herald* – (Washington) **Loss of Everett bridge made for rough commute.** Police have recommended felony charges against a suspected drunken driver whose run-in with a guard rail along Highway 529 the weekend of December 1 helped create traffic in north Everett, Washington, December 2. Thousands of additional northbound drivers were forced onto I-5 for the evening commute, clogging virtually all downtown thoroughfares. Ambulance operators were adding 10-minute delays on emergency calls. The northbound bridge to Marysville was expected to reopen by December 4. Police alleged that an Everett woman was drunk, speeding and driving with a suspended license December 1 when she crashed during a brief police chase. Her SUV slammed into a guard rail and caused enough damage to force the closure of the Highway 529 bridge. The SUV was believed to be traveling at almost twice the posted speed limit, a sheriff's spokeswoman said. The wreck caused vertical and diagonal support beams to break away from connecting bolts on the bridge. It also damaged and cracked about 30 feet of the bridge's guardrail, according to the State Department of Transportation. Repairs were estimated to cost \$30,000. The State plans to seek reimbursement, possibly through the vehicle owner's insurance company. The bridge closure caused traffic on northbound I-5, U.S. 2 and city streets to back up for miles. The steel truss bridge that was damaged along Highway 529 was built in 1927 and is used by about 15,000 vehicles on a typical weekday.

Source: <http://www.heraldnet.com/article/20121203/NEWS01/712039909>

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

Postal and Shipping Sector

14. *December 4, Lubbock Avalanche Journal* – (Texas) **Postal worker gets probation for opening mail.** A former contract carrier for the U.S. Postal Service was sentenced November 30 to five years' probation and ordered to pay restitution for illegally opening mail, the Lubbock Avalanche-Journal reported December 4. A federal grand jury in June indicted the carrier on three counts of theft of mail by a postal employee and two counts of obstruction of mail. According to court documents, he was given notice February 2 that his contract would not be renewed when it expired. That same day, postal inspectors placed a package marked with the name of a jewelry repair shop for delivery on his route. The envelope contained a transmitter that would send out an alert when the envelope was opened. Court documents say he admitted that rather than delivering the envelope or returning it as undeliverable he opened it with a razor blade. The original indictment said the postal service had received complaints from customers on the carrier's route that several items — jewelry, computer game and movie mailers, and medication sent from the Department of Veterans Affairs — had not been delivered. He pleaded guilty in August to one count of obstruction of mail by a postal employee and must pay \$2,111 to the Department of Veterans Affairs and three other businesses.

Source: <http://lubbockonline.com/crime-and-courts/courts/2012-12-03/postal-worker-gets-probation-opening-mail#.UL4n5q59Wmg>

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

Agriculture and Food Sector

15. *December 4, Associated Press* – (New Jersey) **Students sickened by a relaxation drink at school.** Officials have removed a relaxation drink named after a reggae icon after several students at a New Jersey school were sickened, the Associated Press reported December 4. Marley’s Mellow Mood is promoted to reduce stress. The drink’s nutrition facts said it may cause drowsiness and is not intended for children. However, students at Satz Middle School and Holmdel High School could buy it on campus. Several middle school students were sickened November 30. The Asbury Park Press reported the school district’s food service provider removed a manager pending an investigation. Chartwells School Dining Services also removed the product. The company issued a statement in which it said it takes this situation very seriously. Source: <http://www.kmov.com/news/national/Students-sickened-by-Bob-Marley-drink-at-school-181984501.html>

16. *December 2, Examiner.com* – (National) **CDC says Salmonella outbreak linked to Sunland peanut butter appears over.** The Salmonella Bredeney outbreak that first appeared in September when several people were infected after eating a Trader Joe’s Peanut Butter brand appears to be over, according to a Centers for Disease Control and Prevention (CDC) outbreak update November 30. The final number of cases in this outbreak stands at 42 cases in 20 States. There were no reported fatalities linked to this outbreak, although a quarter of the cases required hospitalization for their illness. The recalls of Sunland peanut products began September 22 with Trader Joe’s voluntarily recalling its Creamy Salted Valencia Peanut Butter and removing the product from all store shelves. This was followed in quick succession by recalls of over 300 peanut-related products linked to the Portales, New Mexico company Sunland, Inc. Health officials said that although the outbreak appears over, many of these products have a long shelf-life, and they may still be in peoples’ homes. Consumers unaware of the recall could continue to eat these products and potentially get sick. After a month-long U.S. Food and Drug Administration (FDA) inspection of Sunland’s Portales plant, federal authorities suspended Sunland Inc.’s food facility registration November 26 prohibiting Sunland, Inc. from introducing food into interstate or intrastate commerce. FDA will reinstate Sunland, Inc.’s registration only when they determine that the company has implemented procedures to produce safe products. Source: <http://www.examiner.com/article/cdc-says-salmonella-outbreak-linked-to-sunland-peanut-butter-appears-over>

For more stories, see items [18](#) and [19](#)

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

Water Sector

17. *December 4, Huntington Herald-Dispatch* – (West Virginia) **Boil water advisory issued.** Lavalette Public Service District and Kenova Municipal Water System issued a

precautionary boil water advisory for some of its customers due to a water main break in Kenova Water County, West Virginia, over the weekend of December 1 and 2. A boil water advisory means that water should be boiled for one minute and cooled before consumption. Boiling kills bacteria and other organisms in the water. Kenova Water, the water provider for the district, experienced a water main break on Whites Creek Road over the weekend. The break was repaired and the water problem was expected to be resolved in 3 to 4 days.

Source: <http://www.herald-dispatch.com/news/briefs/x41558833/Boil-water-advisory-issued>

18. *December 3, KSBY 6 San Luis Obispo* – (California) **Stay out of the water at Leadbetter Beach.** Leadbetter Beach in Santa Barbara, California, was closed because of a sewage spill, KSBY 6 San Luis Obispo reported December 3. Santa Barbara city officials said approximately 6,600 gallons of untreated sewage spilled in Luneta Plaza. The sewage flowed into a storm drain that discharges at Leadbetter Beach. People were warned to stay out of the water until tests show it is safe again for recreational use. In addition, city officials said the public should wait at least 10 days to harvest shellfish in the affected area. Shellfish are filter feeders and those from contaminated waters represent an elevated risk of disease if consumed.

Source: <http://www.ksby.com/news/stay-out-of-the-water-at-leadbetter-beach/>

19. *December 3, Kitsap Sun* – (Washington) **Sewage spill reported in Port Gamble Bay.** A malfunctioning sewage pump on Port Gamble S'Klallam land in Washington caused a spill of about 30,000 gallons of sewage into Port Gamble Bay over the weekend of December 1 and 2, according to the Kitsap Public Health District. The pump was repaired December 3, but the Washington Department of Health closed beaches south of Point Julia to commercial shellfish harvesting. Recreational shellfish gatherers should consider the beaches closed to them, as well, said a water pollution identification and control manager for the health district. Although the local health district has no legal authority over recreational shellfish harvesting, he strongly advises against it. The chance of illness from contact with the water also is increased. The health district posted signs advising the closure. The advisory would remain in effect until at least December 10.

Source: <http://www.kitsapsun.com/news/2012/dec/03/sewage-spill-reported-in-port-gamble-bay/>

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

Public Health and Healthcare Sector

20. *December 4, Cincinnati Business Courier* – (National) **Health care fraud investigations to net \$6.9B.** The U.S. Office of Inspector General (OIG), which investigates health care fraud, expects to recover about \$6.9 billion from audits and investigations this year, the Cincinnati Business Courier reported December 4. Targets of investigations included hospitals, nursing homes, and the pharmaceutical industry. OIG reported 778 criminal actions against individuals or entities that engaged in crimes against Department of Health and Human Services programs, along with 367 civil

actions. It also excluded 3,131 individuals and entities from participation in federal health care programs.

Source: <http://www.bizjournals.com/cincinnati/blog/2012/12/health-care-fraud-investigations-to.html>

21. *December 3, KVUE 24 Austin* – (Texas) **Georgetown police investigating string of break ins at health clinic.** A string of break-ins at a Central Texas health clinic are under investigation by Georgetown, Texas police, KVUE 24 Austin reported December 3. Police said the break-ins have occurred four times over five months at the Scott & White Clinic located outside of Sun City. During the most recent break in November 26, police said a man wearing a mask broke into the clinic by throwing a rock through the front window of the building. He then stole prescription drugs like hydrocodone. Source: <http://www.kvue.com/news/Georgetown-police-investigating-string-of-break-ins-at-health-clinic-181899591.html>
22. *December 3, RAND Corporation* – (National) **US health security research not balanced enough to meet goals, study suggests.** Federal support for health security research is heavily weighted toward preparing for bioterrorism and other biological threats, providing significantly less funding for challenges such as monster storms or attacks with conventional bombs, according to a new RAND Corporation study. The findings, published in the December issue of the journal *Health Affairs*, come from the first-ever inventory of national health security-related research funded by civilian agencies of the federal government. Researchers say recent events such as Superstorm Sandy, tornadoes in the Midwest, and major earthquakes around the world highlight the need to prepare the nation's health care system for a broad array of natural and manmade disasters. Beginning in 2010, researchers canvassed seven non-defense agencies whose research addresses topics relevant to the objectives of the National Health Security Strategy, a plan completed in 2009 to guide efforts by the government and others to defend the nation from a large-scale public health threats, both natural and manmade. More than 1,000 of the studies (66 percent) were directed toward biological threats, including bioterrorism, emerging infectious diseases, foodborne illness, and pandemic influenza. Fewer than 10 percent of the total pool of projects addressed natural disasters such as earthquakes, hurricanes, tornadoes, or floods. The remaining projects addressed threats that were chemical (8 percent), radiological (5 percent), nuclear (4 percent), or explosive (4 percent). Source: http://www.eurekalert.org/pub_releases/2012-12/rc-uhs113012.php
23. *December 1, Associated Press* – (Tennessee) **Feds investigate center for Medicare fraud.** Documents unsealed in federal court give details of a federal investigation into allegations of Medicare fraud at Life Care Centers of America in Chattanooga, Tennessee, the Associated Press reported December 1. According to court records, prosecutors accuse Life Care supervisors of directing workers to max out unnecessary therapies for patients in order to get higher reimbursement from Medicare. The records show a federal probe began in 2008 after two whistle-blower lawsuits were filed against the company. In a letter to employees, Life Care denied the allegations, and said the company saved Medicare \$400 million from 2006 to 2010. Medicare paid \$4.2 billion to Life Care between 2006 and 2011.

Source: <http://www.sfgate.com/news/crime/article/Feds-investigate-center-for-Medicare-fraud-4083543.php>

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

Government Facilities Sector

24. *December 3, Omaha World Herald* – (Nebraska) **Douglas County courthouse closed early after bomb threat.** Authorities shut down the Douglas County Courthouse in downtown Omaha, Nebraska after someone phoned in a bomb threat December 3. A caller declared that there was a bomb in the courthouse, according to two officials with knowledge of the call. That had employees leaving the building about 20 minutes before their typical departures. Police were called, and authorities were searching the 100-year-old building. The threat came a month after a caller, or callers, phoned in bomb threats to courthouses in nine Nebraska counties. The November 2 calls were made to Cass, Gage, Jefferson, Johnson, Lancaster, Otoe, Richardson, Saline, and Seward Counties. None of those threats turned out to be credible.

Source: <http://www.omaha.com/article/20121203/NEWS/121209879/1685>

For another story, see item [15](#)

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

Emergency Services Sector

25. *December 4, Contra Costa Times* – (California) **SUV hits three Calif. firefighters at crash scene.** Three firefighters injured December 2 while tending to a car wreck on Highway 24 in Orinda, California, remained in serious but stable condition. Their injuries were not considered life threatening, according to the Moraga-Orinda Fire District. All three were injured when a vehicle traveling east lost control, struck a fire engine, and rolled into the three, the fire chief said.

Source: <http://www.firehouse.com/news/10837313/suv-hits-three-calif-firefighters-at-crash-scene>

26. *December 3, KLTV 7 Tyler* – (Texas) **Fire station out of service as crew copes with firefighter's death.** The Jackson Heights Fire Department in Tyler, Texas, was out of service December 3 after a firefighter was critically injured in a car crash November 30. He and two other Jackson Heights firefighters were on their way to another crash when the wreck happened. The station was shut down to the public due to the loss of the firefighter. The Smith County Firefighter's Association president said the Arp, Chapel Hill, and Winona Fire Departments will take Jackson Height's calls.

Source: <http://www.kltv.com/story/20250810/firestation-out-of-service-as-crew-cope>

27. *December 3, Oklahoma City Oklahoman* – (Oklahoma) **Murderer escapes from southern Oklahoma medium-security prison.** An inmate serving life without parole from an Oklahoma County conviction escaped from a medium-security prison December 3, a Corrections Department spokesman said. He was serving life without

parole for a 2007 first-degree murder conviction. He was being held at the Mack Alford Correctional Facility in Stringtown.

Source: <http://newsok.com/murderer-escapes-from-southern-oklahoma-medium-security-prison/article/3734385>

For more stories, see items [8](#) and [13](#)

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

Information Technology Sector

28. *December 4, Softpedia* – (International) **Hackers can use Twitter SMS vulnerability to post on users' behalves, expert finds.** A security researcher identified a vulnerability which can be leveraged by cybercriminals in attacks against Twitter users. According to the expert, an attacker only needs to know the mobile phone number associated with the target's Twitter account. Presuming that the victim has enabled the SMS service and presuming that a PIN code is not set, the attacker can publish posts on their accounts by sending messages from a spoofed number. The researcher explains that many SMS gateways allow for the sender's address to be set to an arbitrary identifier. Similar to email messages, an attacker can spoof the number to make it look like it comes from a specific number. The researcher claims that Facebook and Venmo were also affected, but they addressed the bug after he had reported the flaw to their security teams. Twitter responded December 4 stating that they fixed the vulnerability. A Romanian researcher that specializes in mobile security reveals that these types of vulnerabilities do not affect just social media platforms, but other services as well. "The problem is not only with Twitter, but also with other services (even banks) that authenticate the user based only on the phone number. It's like just knowing someone's username, no password needed, while in this case it's even easier as people do not consider their phone number as something private."

Source: <http://news.softpedia.com/news/Hackers-Can-Use-Twitter-SMS-Vulnerability-to-Post-on-Users-Behalves-Expert-Finds-311857.shtml>

29. *December 4, Help Net Security* – (International) **Tumblr worm proliferated due to XSS flaw.** A December 3 worm rampage that left many a Tumblr site "defaced" with a message by Internet troll group GNAA was the result of improper input sanitation. "It appears that the worm took advantage of Tumblr's reblogging feature, meaning that anyone who was logged into Tumblr would automatically reblog the infectious post if they visited one of the offending pages," explained a Sophos researcher. Those who were not logged in would be redirected to the standard login page. Once logged in, the offending post would the continued to do its activity and reblog the post on their Tumblr. "It shouldn't have been possible for someone to post such malicious JavaScript into a Tumblr post - our assumption is that the attackers managed to skirt around Tumblr's defences by disguising their code through Base 64 encoding and embedding it in a data URI," concluded the researcher. Tumblr disabled posting for a couple of hours and proceeded to clear the affected accounts. According to a Twitter post by the company, the issue was resolved.

Source: <http://www.net->

[security.org/secworld.php?id=14060&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+\(Help+Net+Security\)&utm_content=Google+Reader](http://security.org/secworld.php?id=14060&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+(Help+Net+Security)&utm_content=Google+Reader)

30. *December 4, Softpedia* – (International) **RoTDL admits It was hacked, takes responsibility for Google Romania hijacking.** The week of November 26, a number of high-profile Romanian Web sites – including Google.ro and Yahoo.ro – redirected their visitors to a defacement page set up by an Algerian hacker. After concluding that this was a case of DNS poisoning, experts revealed that this was most likely the result of a breach that affected RoTDL. RoTDL, the handler of Romania’s top level domains, had been quiet about the incident until December 3, when it came forward with a statement. According to the company’s representatives, the attack against their .ro domain administration server took place on the night between November 27 and 28. They reveal that the attackers modified the name servers of several popular domains to redirect their visitors to an arbitrary Web page. Immediate measures have been taken to prevent future incidents. The security breach is currently being investigated. The investigation’s results will be made public in the days ahead. RoTDL claims that DNS servers have not been affected and that no financial information is stored on the affected machines.
Source: <http://news.softpedia.com/news/RoTDL-Admits-It-Was-Hacked-Takes-Responsibility-for-Google-Romania-Defacement-311941.shtml>
31. *December 4, The H* – (International) **Fast cracking of MySQL passwords demonstrated.** A hacker by the name of Kingcope has found another security problem with the popular MySQL database. Using an already well-known characteristic of the database’s user management, it is possible to significantly increase the speed of a brute force attack. The trick allowed him to test up to 5000 passwords per second over the network if he has some access to the database. For this, the attacker requires an unprivileged account for the database. The script uses that account to log in and then uses the command ‘change_user’ to attempt to change the account during the MySQL session. Unlike presenting the password to the login process, this works with an already established network connection and very quickly rejects incorrect passwords. The hacker used the John The Ripper password cracker to create a password list and has documented the attack with a Perl script and record of a command line session. To crack a four-character password with remote access to the MySQL database took just 20 seconds with over 100,000 character combinations tested.
Source: <http://www.h-online.com/security/news/item/Fast-cracking-of-MySQL-passwords-demonstrated-1762031.html>
32. *December 3, Threatpost* – (International) **Bug hunter finds ‘blended threat’ targeting Yahoo Web site.** A Romanian bug hunter has discovered a “blended threat” targeting Yahoo’s Developer Network Web site that allows unauthorized access to Yahoo users’ emails and private profile data. At a security conference December 2, the researcher demonstrated an abbreviated version of an attack using the YQL console on developer.yahoo.com. Authenticated users also can access tables with their own Yahoo account data, such as emails and profile data, to mount queries. According to Computerworld, the researcher showed how an attacker could abuse a feature on the

site by loading a specific URL inside an iframe that returned the visitor's "crumb code" — session- and user-specific authorization code generated when someone visits the YQL console page. To get around a security measure, the security researcher used a fake CAPTCHA test to generate a YQL query that could divulge the user's Yahoo email account and private profile data. Another step is needed to actually read the emails — a step the researcher did not disclose to the conference audience. The researcher, who had yet to share his discovery with Yahoo, recommended the company mitigate the vulnerability by not permitting unauthorized third-party Web sites from loading pages inside an iframe using the developer.yahoo.com domain.

Source: http://threatpost.com/en_us/blogs/bug-hunter-finds-blended-threat-targeting-yahoo-web-site-120312

33. *December 2, IDG News Service* – (International) **Instagram vulnerability on iPhone allows for account takeover.** A security researcher published November 30 another attack on Facebook's Instagram photo-sharing service that could allow a hacker to seize control of a victim's account. The attack was developed by the researcher around a vulnerability he found within Instagram in mid-November. The vulnerability is in the 3.1.2 version of Instagram's application for the iPhone. The researcher found that while some sensitive activities, such as logging in and editing profile data, are encrypted when sent to Instagram, other data was sent in plain-text. He tested the two attacks on an iPhone 4 running iOS 6, where he first found the problem. The plain-text cookie can be intercepted using a man-in-the-middle attack as long as the hacker is on the same local area network (LAN) as the victim. Once the cookie is obtained, the hacker can delete or download photos or access the photos of another person who is friends with the victim. Security company Secunia verified the attack and issued an advisory. The researcher continued to study the potential of the vulnerability and found the cookie issue could also allow the hacker to take over the victim's account using Address Resolution Protocol (ARP) spoofing.

Source:

http://www.computerworld.com/s/article/print/9234236/Instagram_vulnerability_on_iPhone_allows_for_account_takeover

For another story, see item [11](#)

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@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

Nothing to report

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

Commercial Facilities Sector

34. *December 4, WCBS 2 New York; Associated Press* – (New Jersey) **Cause of 3-alarm Union City blaze under investigation.** Firefighters were on the scene of a huge 3-alarm blaze that burned through a Union City, New Jersey apartment building December 3. Investigators waited for things to cool down before they start looking for what started the fire in the four-story multi-family building. More than 20 apartments and at least two businesses on the first floor were destroyed. No one was injured, but dozens of residents were displaced by the fire. There was no word on exactly what sparked the blaze, but the North Hudson Regional Fire Chief said the fire apparently began on the fourth floor and was fueled by a tar roof. The Red Cross worked to relocate residents.
Source: <http://newyork.cbslocal.com/2012/12/04/cause-of-3-alarm-union-city-blaze-under-investigation/>
35. *December 3, WDSU 6 New Orleans* – (Louisiana) **Sheriff: Man ignited chemicals in Walmart, store evacuated.** A Walmart in Houma, Louisiana, was evacuated December 2 after a man ignited a chemical fire in the store, the Terrebonne Parish Sheriff's Office said. The incident began when crews were alerted to a possible chemical spill at the store. When investigators arrived at the store, they found a container, which included chlorine, which was ignited, causing a chemical reaction. The chemical reaction forced a thick cloud of smoke into the air, investigators said, and the store was then evacuated. The Sheriff's Office said that additional scientific testing will be conducted to determine the specific chemical makeup of the mixture.
Source: <http://www.wdsu.com/news/local-news/new-orleans/Sheriff-Man-ignited-chemicals-in-Walmart-store-evacuated/-/9853400/17634660/-/73hw7uz/-/index.html>
36. *December 3, WCTI 12 New Bern* – (North Carolina) **Marine in custody after hazmat situation at hotel.** Morehead City, North Carolina emergency officials confirmed a person wanting to commit suicide prompted the evacuation of a hotel December 1. That person was identified and arrested by Craven County deputies. A person speaking to the suspect called Morehead City Police. Fire officials evacuated the Hampton Inn plus a Taco Bell and Bistro by the Sea as a precaution. The fire chief said the suspect threatened to kill him or herself with a chemical, prompting the evacuation. Morehead City Police charged the suspect with damage to property, possession of a synthetic drug, possession of drug paraphernalia, and tampering with a fire suppression system. Chemicals and other pieces of evidence were found in the hotel room. Morehead City Police would not release the specifics of the items but said they could have created a chlorine-like gas.
Source: <http://www.wcti12.com/news/Marine-in-custody-after-hazmat-situation-at-hotel/-/13530444/17633480/-/13pibr5/-/index.html>
37. *December 3, KTVT 11 Dallas-Fort Worth* – (Texas) **4-Alarm Fire Burns Irving Apartment Building.** A four-alarm fire destroyed multiple units at an apartment

complex in Irving, Texas. The fire started December 3 at the Arbors of Las Colinas apartment complex. When firefighters arrived, they found one of the buildings — a three-story part of the complex — fully engulfed in flames. The building which burned contained 22 units. The Farmers Branch Fire Department and Dallas Fire-Rescue were called in to help with the fire. Officials in Irving said that 60 to 70 people were impacted by the blaze, as all of the affected apartment units were occupied. The American Red Cross arrived on the scene to assist those displaced residents. Several police officers had to be treated for smoke inhalation after rescuing residents from the burning building, but there were no reports of serious injuries.

Source: <http://dfw.cbslocal.com/2012/12/03/4-alarm-fire-burns-irving-apartment-building/>

38. *December 3, Associated Press* – (Pennsylvania) **Police say man shot ex inside church.** A suspect shot his ex-wife while during a church service at the First United Presbyterian Church of Coudersport, Pennsylvania, December 2 and, after leaving briefly, returned and shot her again to ensure she was dead, police said. Congregants eventually overpowered the suspect, ending the shooting. The shooting was detailed in a criminal complaint filed December 3 against the suspect. Police found a .40-caliber handgun and four spent shells at the church. Police also found a bullet lodged in a wooden pew and another beneath a pillow that was under the victim's head, though police did not immediately explain how it got there. An autopsy was scheduled December 3, and the Potter County Coroner said it was clear the victim died of gunshot wounds, though he could not immediately say how many and where.
39. *December 3, Associated Press* – (New Jersey) **Belmar to spend \$20M rebuilding wrecked boardwalk.** Belmar, New Jersey, approved a \$20 million spending plan December 3 to pay for a new boardwalk, as well as some of the cost of cleaning up the ruins of the old one. The Monmouth County community also considered building a sea wall to help protect against future storms. The borough's plans were the most ambitious of any that have come to a vote since Hurricane Sandy devastated many New Jersey shore communities in October. The mayor said the Federal Emergency Management Agency should pay for at least 75 percent of the cost of the boardwalk repairs, and said New Jersey's Congressional delegation was working to have the agency approve a 90 percent reimbursement rate. To help pay for the borough's share of the cost, Belmar would help pay for the work by increasing daily beach badge fees from \$7 to \$8, and seasonal fees from \$50 to \$55. The mayor said the boardwalk was essential not only to preserving a way of life in Belmar, but also to keeping small businesses open. He added Belmar was looking into building a steel sea wall along the coast to help lessen the damage from future storms. It would consist of 4-foot-tall steel panels that would be plowed over with sand, and dunes planted atop them. Both the sea wall and the higher beach badge fees would be voted on at a future meeting

Source:

http://www.nj.com/south/index.ssf/2012/12/belmar_to_spend_20m_rebuilding.html

For another story, see item [18](#)

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

National Monuments and Icons Sector

40. *December 3, Fort Collins Coloradoan* – (Colorado) **Some Fern Lake Fire evacuations may be lifted today.** Crews fighting the Fern Lake Fire in Colorado's Rocky Mountain National Park made progress against the blaze thanks in part to cooler temperatures and calmer winds, the Fort Collins Coloradoan reported December 3. More than 600 people evacuated from areas near Estes Park were still blocked from returning home while hundreds of others remained on pre-evacuation alert due to safety concerns. The need and scope of the evacuations was evaluated on an ongoing basis, a spokesman for the Larimer County Sheriff's Office said. The sheriff's office announced tentative plans to begin allowing residents who live north of Dunraven Inn along Colorado Highway 66 to return home December 4, and to also open U.S. Highway 36 to the Beaver Meadows Visitor Center. Weather forecasts predicted lighter winds in the fire area for the next few days with a slight chance of precipitation December 4 evening. The fire was mapped at approximately 4,400 acres; containment was estimated at 20 percent.

Source: http://www.coloradoan.com/article/20121203/NEWS01/312030012/Some-Fern-Lake-Fire-evacuations-may-lifted-today?nclick_check=1

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

Dams Sector

41. *November 30, New York Department of Environmental Protection* – (New York) **Department of Environmental Protection to Resume Installation of Siphons at Gilboa Dam.** The New York City Department of Environmental Protection (DEP) announced November 30 plans to resume the installation of new siphons at Schoharie Reservoir, which would help regulate water levels in the reservoir and allow workers to finish rebuilding the Gilboa Dam. The three-week-long project would install at least one of two siphons to be added to the dam. Each siphon would be capable of releasing 250 million gallons a day from the reservoir into the Schoharie Creek, allowing DEP to better manage reservoir levels and provide added flood protection downstream. Currently, diverting water through the Shandaken Tunnel and into the Ashokan Reservoir or operating the newly installed crest gates are the only ways to lower water levels. The new siphons are the latest step in a \$400 million full-scale rehabilitation project, which includes reinforcing the dam with 234 million pounds of concrete, reconstructing the spillway, and installing a new release tunnel around the dam from the Schoharie Reservoir into Schoharie Creek. The siphons would also help DEP meet its commitment of lowering the reservoir for snowpack mitigation during winter months – a measure that aims to further reduce spring flooding. Reconstruction of Gilboa Dam is expected to be finished in 2014, while the new release tunnel is expected to be complete in 2019.

Source: http://www.nyc.gov/html/dep/html/press_releases/12-92pr.shtml

For another story, see item [39](#)

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



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 10 days on the Department of Homeland Security Web site: <http://www.dhs.gov/IPDailyReport>

Contact Information

| | |
|-------------------------------------|---|
| Content and Suggestions: | Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703)387-2341 |
| Subscribe to the Distribution List: | Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes . |
| Removal from Distribution List: | Send mail to support@govdelivery.com . |

Contact DHS

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

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

Department of Homeland Security Disclaimer

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