



## Daily Open Source Infrastructure Report 17 December 2012

### Top Stories

- Hackers broke into the industrial control system of a New Jersey air conditioning company earlier this year, using a backdoor vulnerability in the system, according to a FBI memo made public the week of December 10. – *Wired.com* (See item [7](#))
- Officials confirmed that the State of California mistakenly published thousands of social security numbers on the Internet, KCRA reported December 11. – *KCRA 3 Sacramento* (See item [31](#))
- Twenty-seven people, including 20 children, were killed December 14 when a gunman opened fire inside his mother’s kindergarten class at a Newtown, Connecticut elementary school. – *Fox News* (See item [33](#))
- Federal prosecutors announced charges December 13 against four officers from a south Texas anti-drug task force, who allegedly took thousands of dollars in bribes to guard large shipments of cocaine. – *Associated Press* (See item [35](#))

---

### 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 14, KTWO 2 Wyoming* – (Wyoming) **Three dead in Converse County oil well explosion.** Samson resources company confirmed that three people died in an explosion and fire at one of its oil wells in Converse County, Wyoming, December 14. The company said the victims were all contract personnel. The Converse County sheriff's office is investigating the incident and may release more information at a later time.  
Source: <http://www.k2tv.com/news.php?id=767>
2. *December 13, Bismark Tribune* – (North Dakota) **Oil well blowout reported near Lake Sakakawea.** A roaring out-of-control oil well spewed an orange-colored mix of gas, oil, and saltwater as high as 50 feet into the air December 13 near Lake Sakakawea in North Dakota, staining the snowy white ground as far as 1,000 feet from the well in the prevailing wind direction. A backhoe bucket was finally lowered over the wellhead, capping the spew, and forcing all the escaping liquids to remain inside a containment berm around the well. The Slawson Exploration well is about 10 miles southwest of Parshall, near the Van Hook Arm recreation site. A Slawson superintendent said the bucket was pulled back off the well later because of fire and safety concerns. Crews prepped the location and were prepared to go in December 14 to get the well under control, he said. Officials also received reports December 13 of a spill from an oil well near Johnson's Corner east of Watford City. That well was shut in within a few hours. The superintendent said he did not yet know what failed during the workover operation. He said the well had been in production for about a month and is among 20 Slawson wells in the immediate area and 300 in North Dakota. He said if the well is controlled by December 14, as expected, the workover operation could resume. A State-owned wildlife management area borders the field where the well is located. The saltwater that came up with the oil was the most toxic. A North Dakota Health Department environmental engineer said well records will detail out how much oil, gas, and saltwater spilled during the blowout.  
Source: [http://bismarcktribune.com/bakken/oil-well-blowout-reported-near-lake-sakakawea/article\\_face38bc-4548-11e2-869c-0019bb2963f4.html](http://bismarcktribune.com/bakken/oil-well-blowout-reported-near-lake-sakakawea/article_face38bc-4548-11e2-869c-0019bb2963f4.html)
3. *December 12, Associated Press* – (Vermont) **Barre deals with underground gasoline leak.** A failure in an underground hose at a Barre, Vermont gas station allowed as much as 3,000 gallons of fuel to leak into the ground, with some finding its way into the sewer system, environmental and emergency responders said December 12. With the leak at the North End Deli on North Main Street fixed, State officials were trying to determine the extent of the spill, where the gasoline was going, and how to keep it out of the sewer system and remove it from the soil. The leak was the third from Wesco in Vermont since 1998, including one in 2011 in Essex. It is not unusual for gas stations to spill gasoline inadvertently, but this case was unusual because the gas ended up in the sewage line. In Barre, some residents had detected gasoline fumes in their homes after the fuel migrated into the sewer system. The leak was traced December 11 to the gas station. December 12, the city removed manhole covers and installed fans to ventilate the sewage system. Most of the gasoline in the system was expected to evaporate. The gasoline vapors in the sewage system never reached explosive levels,

said the head of Vermont's hazardous response team. Nor did the gasoline reached levels that would harm human health, officials said.

Source:

<http://www.burlingtonfreepress.com/viewart/20121212/NEWS02/312120030/Barre-deals-with-underground-gasoline-leak?odyssey=tab|topnews|text>

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

## **Chemical Industry Sector**

4. *December 13, Associated Press* – (California) **Walgreens must pay \$16M for illegal dumping.** A California judge ordered drugstore chain Walgreens to pay \$16.57 million to settle a lawsuit claiming more than 600 of its stores in the State illegally dumped hazardous waste. The settlement announced December 13 stems from a lawsuit filed in June by district attorneys around the State. The legal action followed inspections of trash bins at Walgreens stores. It accused the stores of illegally handling and disposing pesticides, bleach, paint, pharmaceutical waste, and other items. The stores were also accused of unlawfully disposing of customer records containing confidential medical information. A Walgreen Co. spokesman said the company did not acknowledge any wrongdoing and settled the case to avoid protracted litigation. He said Walgreens ships all hazardous materials are shipped to a hazardous waste disposal facility, where they are incinerated.

Source: <http://www.usatoday.com/story/money/business/2012/12/13/walgreens-illegal-dumping/1767869/>

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

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

5. *December 12, Ventura County Star* – (California) **Excessive radiation found at Santa Susana Field Lab site.** After nearly 3 years of study, the U.S. Environmental Protection Agency (EPA) confirmed that at a portion of the Santa Susana Field Laboratory in California, some radiological contamination exceeds established limits, the Ventura County Star reported December 12. The survey includes test results of samples of groundwater, sediment, and subsurface soil in the Northern Buffer Zone and Area IV, which was once home to 10 small nuclear reactors. EPA officials collected 3,735 soil and sediment samples and 215 groundwater and surface samples from the site. Of the 34 surface water samples collected, two instances of maximum contamination levels being exceeded were found, while four areas had high levels of contamination in sediment. There were nearly 300 instances of Cesium-137 in soil samples exceeding maximum levels, while 153 samples had levels of Strontium-90 that far exceeded the background level. Those background levels were going to be used to plot the cleanup of radiological contamination at the site, which will be overseen by California's Department of Toxic Substances Control. At a public meeting December 12 in Simi Valley to discuss the survey results, EPA officials said the background limits could not be duplicated because of differences in laboratories. They added that they discovered the problem when they went from using one lab to another during the

survey.

Source: <http://www.vcstar.com/news/2012/dec/12/excessive-radiation-found-at-santa-susana-site/>

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

## **Critical Manufacturing Sector**

6. *December 13, Springfield Republican* – (Connecticut; Massachusetts) **2 Bridgeport, Conn., men face federal charges in theft of 111 guns from Smith & Wesson plant in Springfield.** A federal grand jury indicted two Bridgeport, Connecticut men in connection with the theft of 111 handguns from the Smith & Wesson manufacturing plant in Springfield, Massachusetts, during November. The affidavit charges one man, a delivery driver, delivered the three cases of stolen guns to the second man, who apparently sold several of them on the street. Only 28 of the 111 handguns have been recovered, according to officials. According to the federal affidavit, the driver, who worked with Pace Motor Lines of Stratford, had been dispatched November 8 to pick up an order of five crates of guns from Smith & Wesson in Springfield. Surveillance footage from the loading area showed the driver placing eight crates onto his truck. Also, a check of the global position tracking device on the truck showed that on the return trip to Connecticut, he stopped at his residence for approximately 35 minutes before returning to the Pace facility, where he delivered the five cases and ended his shift. A U.S. Attorney said an investigation involving the Bureau of Alcohol, Tobacco, Firearms, and Explosives and the Bridgeport and Stratford police is ongoing to find the remaining weapons.  
Source:  
[http://www.masslive.com/news/index.ssf/2012/12/two\\_bridgeport\\_conn\\_men\\_face\\_f.ht ml#incart\\_river\\_default](http://www.masslive.com/news/index.ssf/2012/12/two_bridgeport_conn_men_face_f.ht ml#incart_river_default)
7. *December 13, Wired.com* – (New Jersey; International) **Hackers breached heating system via industrial control system backdoor.** Hackers broke into the industrial control system (ICS) of a New Jersey air conditioning company earlier this year, using a backdoor vulnerability in the system, according to a FBI memo made public the week of December 10. The intruders first breached the company's ICS network through a backdoor in its Niagara AX ICS system, made by Tridium. This gave them access to the mechanism controlling the company's own heating and air conditioning, according to a memo prepared by the FBI's office in Newark. The breach occurred in February and March, several weeks after someone using the Twitter moniker @ntisec posted a message online indicating that hackers were targeting supervisory control and data acquisition (SCADA) systems, and that something had to be done to address vulnerabilities. The individual had used the Shodan search engine to locate Tridium Niagara systems that were connected to the internet and posted a list of URLs for the systems online. One of the IP addresses posted led to the New Jersey company's heating and air conditioning control system. The company used the Niagara system not only for its own HVAC system, but also installed it for customers, which included banking institutions and other commercial entities, the memo noted. An IT contractor who worked for the company told the FBI that the company had installed its own

control system directly connected to the internet with no firewall in place to protect it. Although the system was password protected in general, the backdoor through the IP address apparently required no password and allowed direct access to the control system. The backdoor URL gave access to a Graphical User Interface (GUI), “which provided a floor plan layout of the office, with control fields and feedback for each office and shop area,” according to the FBI. “All areas of the office were clearly labeled with employee names or area names.” Forensic logs showed that intruders had gained access to the system from multiple IP addresses in and outside the U.S.  
Source: <http://www.wired.com/threatlevel/2012/12/hackers-breach-ics/>

8. *December 13, U.S. Department of Labor* – (Ohio) **U.S. Labor Department’s OSHA fines Timken Co. \$170,500 after complaint inspection finds 12 safety violations at Canton, Ohio, steel mill.** The U.S. Department of Labor’s Occupational Safety and Health Administration December 13 cited Timken Co. for 12 alleged safety violations, including 5 repeat, after conducting a complaint inspection in June at the steel mill in Canton, Ohio, which manufactures roller bearings. Proposed penalties totaled \$170,500. Five repeat safety violations involved failing to machine guard ingoing nip points, points of operation and rotating parts. Additionally, the company lacked guardrails on elevated platforms and failed to ensure electrical boxes with unused openings were closed. Seven serious safety violations involved failing to reduce compressed air for cleaning to 30 pounds per square inch or below; maintain floors in dry condition; conduct annual training for workers designated to use portable fire extinguishers; provide an emergency eyewashing station; ensure each authorized worker affixed a personal lockout device to a group lock box to prevent the unintentional release of hazardous energy; and properly adjust machine guarding.  
Source: [http://www.osha.gov/pls/oshaweb/owadisp.show\\_document?p\\_table=NEWS\\_RELEASES&p\\_id=23406](http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=23406)
9. *December 13, KTVU 2 Oakland* – (California) **Fremont machine shop gutted by 3-alarm blaze.** A fast response from Fremont, California fire crews brought a large three-alarm fire in the city’s Warm Springs neighborhood quickly under control December 13, but could not keep the blaze from gutting a machine shop. Crews responded to a report of a structure fire at C&H Enterprises. When firefighters arrived, they saw heavy smoke and flames and could not make their way into the structure, the fire captain said. The roof of the building collapsed and crews battled from the tops of their fire engines’ extended ladders, he said. The business, which performs precision machining, welding, and fabricating, has a placard posted to inform people there are combustible and flammable materials inside, he said. All 60 employees safely evacuated the building and workers at other nearby businesses were asked to shelter in place as crews battled the fire. The fire was eventually contained and the shelter in place was lifted 2 hours later, he said. Alameda County and Hayward fire departments assisted with mutual aid throughout Fremont, while crews battled the fire.  
Source: <http://www.ktvu.com/news/news/local/firefighters-battle-blaze-industrial-building-fremontWPD/>

## Defense Industrial Base Sector

Nothing to report

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

## Banking and Finance Sector

10. *December 14, BankInfoSecurity* – (International) **DDoS attacks: PNC struck again.** PNC Financial Services Group confirmed that its online banking site December 13 was bombarded with high volumes of traffic for the second time the week of December 10, causing some users to have trouble logging into their accounts. A U.S. Bank spokesman also confirmed a distributed denial of service (DDoS) hit against U.S. Bank December 12. A PNC spokesman said the bank’s site experienced “higher than usual” traffic volumes. “We will continue to communicate directly to our customers through our social media and other online channels, including our website,” he said. The two banks, and others, were named by a hacktivist group as targets in a Pastebin post for the group’s second phase of DDoS attacks.  
Source: <http://www.bankinfosecurity.com/ddos-attacks-pnc-struck-again-a-5356>
11. *December 14, The Columbia State* – (National) **20 from Spartanburg, Cherokee counties charged in mail theft, cashing altered, fake checks.** Federal authorities charged 20 people from South Carolina’s Spartanburg and Cherokee counties in a conspiracy involving mail theft and cashing altered or counterfeit checks. The suspects appeared in court December 13 to be formally indicted on federal charges involving mail and check fraud. The conspiracy, which dates back to 2011 and continued into this year, netted about \$900,000 and involves “thousands” of victims, including residents and merchants who investigators said were scammed, an Assistant U.S. Attorney said. According to the indictment, the 20 people charged took mail from mail boxes, stole identification, altered checks stolen from mail boxes for their own use, counterfeited checks for their own use, used fake identification when negotiating stolen or counterfeit checks, and divided the proceeds from the checks. The conspiracy was investigated by the U.S. Postal Inspection Service, the Spartanburg County Sheriff’s Office, and the Cherokee County Sheriff’s Office.  
Source: <http://www.goupstate.com/article/20121213/ARTICLES/121219841?tc=ar>
12. *December 14, Softpedia* – (International) **60Gbps: Size of some DDoS attacks launched by hacktivists.** A group of hacktivists re-initiated their campaign against U.S. financial institutions, and security experts from Arbor Networks analyzed the attacks and revealed that some of them were as large as 60Gbps, Softpedia reported December 14. The first series of distributed denial-of-service (DDoS) attacks launched by the hacktivists in September used a lot of compromised PHP Web applications as bots. One of the most important PHP-based tools utilized at the time was Brobot. KamiKaze and AMOS were also used, but not as often as Brobot, which is also known as “itsoknoproblembro.” Attacks the week of December 10 looked similar to the ones that used Brobot, but some changes have been made. “Some attacks looked similar in construction to Brobot v1, however there is a newly crafted DNS packet attack and a

few other attack changes in Brobot v2,” experts wrote. They emphasize that despite the fact that some of the attacks were 60Gbps in size, this is not what makes them so significant. Instead, it is the fact that they’re focused and part of an ongoing campaign. Arbor warns that the intrusion prevention systems (IPS) and the firewalls deployed by many enterprises are not effective in dealing with DDoS attacks. Instead, organizations need to use an on-premises DDoS mitigation solution.

Source: <http://news.softpedia.com/news/60Gbps-Size-of-Some-DDOS-Attacks-Launched-by-al-Qassam-Cyber-Fighters-314829.shtml>

13. *December 13, CNN* – (National) **FBI seeks help in catching ‘Ray-Bandit’ bank robber.** The FBI released photos of a serial bank robber known as the “Ray-Bandit” who has successfully robbed 13 banks across the country in hopes that the photos will lead to a tip from the public about his identity and whereabouts, CNN reported December 13. The string of robberies began in July in Wisconsin and included banks in Indiana, Illinois, Iowa, and Nebraska through early October. Only one robbery attempt, in Indiana, was unsuccessful, the FBI said. The robber apparently left the Midwest and has resurfaced twice in California and twice in Virginia. Authorities dubbed him the “Ray-Bandit” because of the Ray-Ban-style glasses he has worn during some of the robberies. In addition to sunglasses and a cap, which often bears a Ford Shelby Cobra logo, the robber has worn fake beards, false teeth and dyed his hair different colors. He seems to cover his fingertips with rubber thimbles. He also seems to gravitate to banks in supermarkets, the FBI said.  
Source: <http://www.cnn.com/2012/12/13/us/fbi-bank-robber/>
14. *December 13, U.S. Attorney’s Office, Eastern District of Texas* – (National) **Provident CFO indicted in \$485 million investment fraud scheme.** A Plano, Texas man was indicted in connection with a \$485 million investment fraud scheme in the Eastern District of Texas, according to a December 13 court press release. He charged with conspiracy to commit mail fraud. According to the indictment, the man, who served as chief financial officer of Provident Royalties, is alleged to have conspired with others to defraud investors in an oil and gas scheme that involved over \$485 million and 7,700 investors throughout the United States. Specifically, beginning in September 2006, he and other individuals are alleged to have made materially false representations and failed to disclose material facts to their investors in order to induce the investors into providing payments to Provident. Among these false representations were statements that funds invested would be used only for the oil and gas project for which those funds were raised; among the omissions of material fact were the facts that another of Provident founders had received millions of dollars of unsecured loans; that he had been previously charged with securities fraud violations by the State of Michigan; and that funds from investors in later oil and gas projects were being used to pay individuals who invested in earlier oil and projects. Two others involved in the alleged fraud were convicted, and two others were charged and are awaiting trial.  
Source: <http://www.fbi.gov/dallas/press-releases/2012/provident-cfo-indicted-in-485-million-investment-fraud-scheme>
15. *December 13, Chicago Tribune* – (Illinois) **‘Second Hand Bandit’ convicted of bank robberies.** A federal jury in Chicago found a man guilty December 13 of two bank

robberies and two attempted holdups. He made off with a combined nearly \$600,000 in the heists, authorities said. The FBI labeled him the “Second Hand Bandit” because he wore used clothes during the robberies. Authorities suspected him in as many as 21 holdups but charged him in just the four. Security footage played for jurors showed the man jumping bank counters and wielding a handgun as he ordered employees to open vaults and ATMs at the banks.

Source: <http://www.chicagotribune.com/news/local/breaking/chi-second-hand-bandit-convicted-of-bank-robberies-20121213,0,5446834.story>

16. *December 12, U.S. Department of the Treasury* – (International) **Treasury levies additional sanctions against business network linked to Sinaloa Cartel drug lord “El Azul”**. The U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) announced December 12 the designation of one entity and three individuals linked to a leader of Mexico’s Sinaloa Cartel also known as ‘El Azul’. The action, pursuant to the Foreign Narcotics Kingpin Designation Act (Kingpin Act), prohibits U.S. persons from conducting financial or commercial transactions with the designees, and also freezes any assets they may have under U.S. jurisdiction. The action targets Desarrollos Everest, S.A. de C.V., a real estate development company based in Culiacan, Sinaloa, Mexico. The company is co-owned by a wife of the Sinaloa leader who was previously designated because she acts on behalf of her husband. Also targeted was Residencial del Lago, a residential community located in Culiacan owned or controlled by Desarrollos Everest, S.A. de C.V. OFAC also designated three Mexican individuals in connection with the targeted companies.

Source: <http://www.albanytribune.com/12122012-treasury-levies-additional-sanctions-against-sinaloa-cartel-drug-lord-el-azul/>

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

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

## **Transportation Sector**

17. *December 14, KTWO 2 Casper* – (Wyoming) **Converse County bridge destroyed in fire**. A one lane wooden bridge over the North Platte river in Converse County, Wyoming, was destroyed in a fire December 13. Authorities said the fire broke out, and the Coal Shadow bridge was fully involved in flames when crews from both Converse and Natrona counties arrived. They were unable to save the structure, and were still on the scene several hours later. Fire investigators from Cheyenne were looking into the cause of the fire, but neighbors told the media they thought it was started by someone shooting off fireworks. Neighbors said around 60 cars used the bridge on a daily basis. Source: <http://www.k2tv.com/news.php?id=1706>
18. *December 14, Leaf Chronicle* – (Tennessee) **Clarkville-Montgomery County School bus rear-ended Friday morning**. The bus driver and 15 Clarksville-Montgomery County, Tennessee students injured in a school bus accident December 14 were all listed in ‘good’ condition. School bus 9857 was rear-ended near the corner of Dunbar Cave Road and Warfield Boulevard. Ten students and the bus driver were transported to a

medical center with complaints of neck and/or head pain. Another five students were picked up at the scene by their parents and transported to the hospital to have them checked out. Transportation officials worked with the Clarksville Police Department at the scene, which was cleared. There were 57 students on board. Those not transported to the hospital were picked up by a second school bus which transported them to Rossvie Middle and Rossvie High schools.

Source: <http://www.theleafchronicle.com/viewart/20121214/NEWS01/312140010/>

19. *December 14, USA Today* – (National) **FAA orders GE to repair regional-jet engines after fires.** The Federal Aviation Administration (FAA) ordered General Electric Co. to repair 300 of its turbofan engines because bad valves caused two engine fires. The repairs were projected to cost \$7.55 million according to the FAA's order, published December 13 in the Federal Register. The CF34-8C and CF34-8E engines are on Bombardier CRJ700/900 and Embraer 170/175 aircraft. The order affects about 15 percent of the fleet for the engines, which were built from 2001 to 2006, when General Electric switched valve suppliers. The order is to prevent "engine fuel leakage, uncontrolled fire and damage to the airplane," the FAA said. The flaw involves a piece of equipment called the operability bleed valve, which takes air out of the engine's compressor during start-up. As the valve fittings aged, FAA found they occasionally leaked and twice caused an engine fire. One fire occurred on takeoff, and the pilot shut down the engine and activated the fire-extinguishing system before landing safely, according to GE. The other fire occurred after landing a plane, when the pilot noticed a fire alert and shut off fuel to the engine before taxiing safely to the gate.

Source: <http://www.usatoday.com/story/todayinthesky/2012/12/12/ge-engines/1765035/>

20. *December 13, WXYZ 7 Detroit* – (Michigan) **Bus collides with truck on Detroit's east side, several people injured.** At least 10 people were hurt when a bus collided with a semi truck, WXYZ 10 Detroit reported December 13. It happened on Moross near Edsel Ford on Detroit's east side. The injured passengers were taken to a nearby hospital. Their conditions have not been released.

Source: <http://www.wxyz.com/dpp/news/region/detroit/bus-collides-with-semi-truck-in-detroit>

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

## **Postal and Shipping Sector**

21. *December 14, Wilkes-Barre Citizens Voice* – (Pennsylvania) **West Side brothers charged with stealing mail.** Two brothers were arrested for theft of mail December 13, Kingston Township, Pennsylvania police said. They worked as independent contractors to deliver The Citizens' Voice newspaper, and the contract for their delivery route was terminated that day, said the circulation director for The Citizens' Voice. They were charged with theft, conspiracy, and receiving stolen property, police said.

Source: <http://citizensvoice.com/news/west-side-brothers-charged-with-stealing-mail-1.1416130>

22. *December 14, Eugene Register Guard* – (Oregon) **Two men charged in burglaries at post offices.** Two men were arrested in connection with burglaries earlier this year at the Elmira and Marcola post offices, Eugene, Oregon police said. They were arrested 2 days apart, the first December 10, the second December 12, on two counts of burglary and additional federal crimes following a federal grand jury indictment, police said. Property crimes detectives learned of the pair’s alleged connection to the burglaries during a search warrant August 30. Their investigation led them to an address following reports of a stolen boat and the burglary of a Eugene area storage unit in which numerous weapons were taken, police said. In investigating the burglaries at the storage unit and at a Veneta residence, detectives uncovered evidence — including more than \$2,000 in stamps, a postal tote, and text messages — that linked the two men to the post office crimes, police said. Detectives worked with the U.S. Postal Investigation Service to piece together a case that included the theft of packages, blank money orders, and printing machines.  
Source: <http://www.registerguard.com/web/updates/29177043-55/police-burglaries-detectives-arrested-post.html.csp>
23. *December 12, WMAR 2 Baltimore* – (Maryland) **Benson Post Office robbed at gunpoint.** Police in Harford County, Maryland, are looking for the man responsible for robbing a Post Office December 12. An official with the Harford County Sheriff’s Office said officers responded to the Benson Post Office for reports of a robbery. The man apparently waited in line with other customers until he got to the counter, at which time he displayed a handgun, leaned across the counter and took an undisclosed amount of money from the register. The man then fled the area on foot.  
Source: [http://www.abc2news.com/dpp/news/crime\\_checker/harford\\_county\\_crime/benson-post-office-robbed-at-gunpoint](http://www.abc2news.com/dpp/news/crime_checker/harford_county_crime/benson-post-office-robbed-at-gunpoint)

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

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

## **Agriculture and Food Sector**

24. *December 13, U.S. Food and Drug Administration* – (National) **Salinas Firm conducts precautionary recall on a select salad product due to possible health risk.** Taylor Farms Retail, Inc. of Salinas, California, December 13, initiated a precautionary recall of 110 cases of Taylor Farms Hearts of Romaine 10-ounce bags bearing UPS number: 0 30223 04032 3 with the package code: TFRS332A09 with best buy date of December 13. This product is being recalled out of an abundance of caution following a single random finished package test conducted by the Food and Drug Administration which tested positive for *Listeria monocytogenes*. There have been no complaints or illnesses reported in association with this recall. No other Taylor Farms products or brands are included in this recall.  
Source: <http://www.fda.gov/Safety/Recalls/ucm332108.htm>

25. *December 13, The Packer* – (National) **FDA gives an extra month for facility registration.** The Food and Drug Administration (FDA) gave the food industry 30 more days before it starts enforcing food facility registration requirements, The Packer reported December 13. The Food Safety Modernization Act of 2011 calls for food facilities to renew registration with FDA every other year during the period beginning October 1 and ending December 31 of each even-numbered year. The FDA said December 12 it will exercise “enforcement discretion” and not begin policing the registration requirement until January 31, 2013. Because of FDA delays in fine-tuning the registration process, operators of food facilities were prevented from registering/re-registering with the FDA until October 22, about 3 weeks after the expected start date. Some of the new requirements for the registration process include providing the email for the company’s point of contact and better describing what kind of food products are produced at the facility. The new food safety law also gives FDA the authority to suspend a food facility’s registration if the food from the company has a “reasonable probability” of causing serious health consequences or death. The FDA has already exercised that authority with peanut butter manufacturer Sunland Inc., in November following a foodborne disease outbreak linked to the firm.  
Source: <http://www.thepacker.com/fruit-vegetable-news/FDA-gives-an-extra-month-for-facility-registration-183383451.html>
26. *December 13, U.S. Department of Labor* – (Texas) **U.S. Labor Department’s OSHA cites two Fort Worth, Texas, companies for multiple process safety management violations.** The U.S. Department of Labor’s Occupational Safety and Health Administration (OSHA) December 13 cited Five Star Custom Foods Ltd. for 25 serious safety and health violations. Subcontractor Packers Sanitation Services Inc. was also cited for two serious safety violations concerning exposure to hazardous chemicals at the company’s facility in Fort Worth, Texas. Penalties totaled \$134,000 collectively. OSHA officials opened an investigation on June 12 under the agency’s national emphasis program on process safety management, known as PSM, for covered chemical facilities. Investigators found that employees, while conducting operations in the facility’s refrigeration system, were exposed to the catastrophic release of toxic and corrosive chemicals. An additional 11 safety violations involve failing to develop machine-specific lockout/tagout procedures for the control of hazardous energy; maintain work areas free of slip, trip and fall hazards; keep exit areas unobstructed; and to address electrical wiring deficiencies.  
Source:  
[http://www.osha.gov/pls/oshaweb/owadisp.show\\_document?p\\_table=NEWS\\_RELEASES&p\\_id=23412](http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=23412)

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

## **Water Sector**

27. *December 13, Klamath Falls Herald and News* – (Oregon) **Chiloquin sewage leak brings mandate from DEQ.** The owner of the property where Melitas Restaurant, Motel, and RV Park are located was fined \$77,524 by the Oregon Department of Environmental Quality (DEQ) for allowing sewage to leak onto his property, the

Klamath Herald and News reported December 13. In 2009, Klamath County inspectors found the wastewater treatment system at the property in Chiloquin had failed, according to a news release. Klamath County inspectors warned the owner and a project to connect the site to the city sewer system began. Sometime later, the release said, the project stopped. In September, Klamath County inspectors again visited the site to find that the septic lines had leaked. The inspectors reported their observations to the DEQ. The owner was ordered to prevent sewage from surfacing on the property and to connect the property to the city's sewage system. In all, the project likely will cost the owner more than \$100,000. DEQ stated a large portion of the penalty represents "the economic benefit the owner gained by not connecting to the city's sewer system." His appeal allowed him to discuss whether DEQ should lower the penalty and if he can perform a supplemental project to benefit the environment. DEQ will lower the penalty when he connects to Chiloquin's sewer system, the news release stated.

Source: [http://www.heraldandnews.com/members/news/inside/article\\_f539413a-45b8-11e2-ad3e-0019bb2963f4.html](http://www.heraldandnews.com/members/news/inside/article_f539413a-45b8-11e2-ad3e-0019bb2963f4.html)

28. *December 13, eNews Park Forst* – (Pennsylvania) **U.S., Pennsylvania, and Scranton, Pa., Sewer Authority settle violations of sewage overflows.** The United States and the Commonwealth of Pennsylvania announced December 13 a settlement with the Scranton Sewer Authority (SSA) resolving alleged Clean Water Act violations involving sewer overflows to the Lackawanna River and its tributaries. In a proposed consent decree, the Scranton Sewer Authority agreed to implement a 25-year plan to control and significantly reduce overflows of its sewer system, thereby helping improve water quality of the Lackawanna River and local streams. The plan is estimated to cost \$140 million to implement. The proposed settlement was filed in federal court in Scranton by the U.S. Department of Justice on behalf of the U.S. Environmental Protection Agency (EPA) and by the Pennsylvania Department of Environmental Protection (PADEP). The settlement also requires SSA to pay a \$340,000 civil penalty, which will be split evenly between the United States and Pennsylvania. The settlement addressed problems with SSA's combined sewer system, which when overwhelmed by stormwater, frequently discharges raw sewage, industrial waste, nitrogen, phosphorus, and polluted stormwater into the Lackawanna River and its tributaries, part of the Chesapeake Bay Watershed. The volume of combined sewage that overflows from the system is approximately 700 million gallons annually.

Source: <http://www.enewspf.com/latest-news/science-a-environmental/39119-us-pennsylvania-and-scranton-pa-sewer-authority-settle-violations-of-sewage-overflows.html>

29. *December 13, Sampson Independent* – (North Carolina) **Water line break brings boil water notice.** Clinton, North Carolina crews worked through December 13 to fix a water line break that caused water service to be cut off in areas around North Boulevard throughout the day. A boil water notice was delivered to residents and businesses in northern Clinton December 13. The break was discovered after calls came in to city officials from residents complaining of low water pressure. Crews subsequently discovered the break and later the city manager said water had been restored to some areas, but not all. Boil water notices were also delivered to residences and businesses in the North Boulevard, Nathan Dudley Road, and Martha Lane areas. "(The) boil water

order will be lifted after water is restored and we can test the water,” the city manager stated. That test takes 24 hours, he said. The advisory would remain in effect until further written notification was issued.

Source: [http://www.clintonnc.com/view/full\\_story/21119746/article-Water-line-break-brings-boil-water-notice](http://www.clintonnc.com/view/full_story/21119746/article-Water-line-break-brings-boil-water-notice)

30. *December 13, U.S. Environmental Protection Agency* – (Massachusetts; New Hampshire) **Columbia, N.H. sand and gravel facility pays fine for Clean Water Act violations.** CSG Holdings, Inc. paid \$150,000 to resolve the U.S. Environmental Protection Agency’s (EPA) claims that it allowed polluted stormwater and process water from its Columbia, New Hampshire facility to flow into nearby waters, violating Clean Water Act provisions to prevent pollution from stormwater runoff at industrial sites. CSG Holdings is the former operator of Columbia Sand and Gravel, a sand and gravel mining facility on the banks of the Connecticut River. EPA alleged that CSG Holdings discharged process waste waters and stormwater from the facility without proper permits and violated federal Oil Pollution Prevention Regulations by failing to prepare and implement a Spill Prevention, Control, and Countermeasure Plan. Monitoring confirmed that stormwater discharges from the facility contained high levels of total suspended solids, a pollutant that can adversely affect water quality and stress aquatic animals and plants. The Clean Water Act prohibits the discharge of process waste waters without a permit and requires that industrial facilities, such as sand and gravel facilities, have controls in place to minimize pollutants from being discharged with stormwater into nearby waterways. Each site must have a stormwater pollution prevention plan that sets guidelines and best management practices that the company will follow to prevent runoff from being contaminated by pollutants. Without on-site controls, runoff from sand and gravel facilities can flow directly to the nearest waterway and can cause water quality impairments such as siltation of rivers, beach closings, fishing restrictions, and habitat degradation.

Source:

<http://yosemite.epa.gov/opa/admpress.nsf/d0cf6618525a9efb85257359003fb69d/c735941ad7978f1885257ad3005c9cce!OpenDocument>

For another story, see item [3](#)

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

## **Public Health and Healthcare Sector**

31. *December 11, KCRA 3 Sacramento* – (California) **State of Calif. mistakenly publishes thousands of SSN online.** Officials confirmed that the State of California mistakenly published thousands of Social Security numbers on the Internet, KCRA reported December 11. The confidential information was available on the State’s Medi-Cal Web site for anyone to see for a period of 9 days, before the mistake was discovered and the numbers removed. The list includes Medi-Cal providers in 25 California counties. State officials from the Department of Health Care Services admitted in an interview to the posting of nearly 14,000 Social Security numbers belonging to Medi-Cal providers working for In-Home Supportive Services. “This was inadvertent and we sincerely

regret this has happened,” said the deputy director for public affairs for the Department of Health Care Services.

Source: <http://www.kcra.com/news/State-of-Calif-mistakenly-publishes-thousands-of-SSN-online/-/11797728/17723434/-/tad6swz/-/index.html?absolute=true>

For more stories, see items [4](#) and [34](#)

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

## **Government Facilities Sector**

32. *December 14, San Deigo Union-Tribune* – (California) **Navy helicopter crew still hospitalized.** A Navy MH-60R helicopter crash landed at North Island Naval Air Station in San Diego County, California, December 12, putting all four crew members in the hospital. The helicopter, assigned to North Island’s HSM-75 Wolfpack squadron, was significantly damaged in what the Navy described as a “hard landing” on the tarmac. Two of the crew were taken to UC San Diego Medical Center; the other two were taken to Scripps Mercy Hospital. They remained there December 13 in stable condition and were not expected to be released that day. The crash is being investigated as a Class A mishap. A spokesman said the helicopter crew experienced an “in-flight emergency,” but he did not have further details. An investigation overseen by the Naval Safety Center in Norfolk, Virginia, will probably take months to become public.  
Source: <http://www.utsandiego.com/news/2012/dec/14/tp-navy-helicopter-crew-still-hospitalized/>
33. *December 14, Fox News* – (Connecticut) **At least 26 dead in shooting at Connecticut elementary school.** Twenty-seven people, including 20 children, were killed December 14 when a gunman opened fire inside his mother’s kindergarten class at a Newtown, Connecticut elementary school. The shooter gunned down his mother and her entire class at Sandy Hook Elementary School; at the time of this report none of the pupils in the classroom were accounted for, according to local news sources. The gunman was found dead inside the school, according to officials. A source told Fox News that the shooter’s father, who was divorced from his ex-wife, was killed at his home in New Jersey. Police were also searching for two friends of the killer, who were unaccounted for at the time of this report. The shooter’s girlfriend and another friend were missing in New Jersey, according to law enforcement sources. An official with knowledge of the situation said the shooter was armed with a .223-caliber rifle. Four weapons in total were recovered from the scene. The motive was not yet known. The elementary school has close to 700 students.  
Source: <http://www.foxnews.com/us/2012/12/14/police-respond-to-shooting-at-connecticut-elementary-school/>
34. *December 13, WDAF 4 Kansas City* – (Missouri) **Seven public employees arrested in insurance fraud scheme.** Federal prosecutors said that six Kansas City, Missouri municipal employees and a Jackson County employee were arrested in connection to an alleged insurance fraud scheme. The 7 employees were charged in a 21-count indictment returned by a federal grand jury December 12. The defendants were each

charged with three counts of wire fraud. According to prosecutors, the defendants engaged in a scheme to defraud their healthcare provider – Blue Cross and Blue Shield of Kansas City – through a benefits program called Points to Blue. Prosecutors said that within the first 6 months of the program the accused public workers began falsifying entries on the Points to Blue Web site in order to obtain the maximum benefit. The defendants would, in addition to making false entries on their own behalf, solicit coworkers to engage in the fraud scheme as well – submitting false activities on the behalf of a coworker or a coworker’s dependent in exchange for a portion of the \$250 award. Prosecutors alleged that as a result of the fraud scheme, 1,253 fraudulent gift cards were issued, totaling \$310,960. In a statement, the City of Kansas City said that they were cooperating fully with the investigation, stressing that no public funds were misappropriated as a part of the alleged fraud. If convicted, each defendant could face up to 60 years in prison and a \$750,000 fine.

Source: <http://fox4kc.com/2012/12/13/six-kcmo-employees-arrested-in-insurance-fraud-scheme/>

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

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

## **Emergency Services Sector**

35. *December 14, Associated Press* – (Texas) **4 officers from Texas anti-drug task force accused of guarding large cocaine shipments.** Federal prosecutors announced charges December 13 against four officers from a south Texas anti-drug task force who they said took thousands of dollars in bribes to guard large shipments of cocaine. The officers, two from the Mission police department and two Hidalgo County sheriff’s deputies, were members of the “Panama Unit,” which is a joint task force between the two agencies that targets drug trafficking, according to prosecutors. The U.S. Immigration and Customs Enforcement department that conducts internal reviews received a tip in August about a police officer and another task force member stealing drugs. October 19, a deputy and another individual escorted a load of 20 kilograms of cocaine north from McAllen to the Border Patrol checkpoint in Falfurrias about an hour away. The officers earned thousands of dollars more for allegedly escorting four more cocaine shipments in November that were part of the sting operation, prosecutors contend. None of the officers have been arraigned, but one Mission police officer made an initial appearance in federal court December 13 on charges of twice possessing cocaine with intent to distribute. A U.S. Magistrate Judge set the officer’s bond at \$100,000 and ordered him to remain under house arrest with electronic monitoring if he should make bond. She denied his request for a court-appointed attorney.

Source: <http://www.grandforksherald.com/event/apArticle/id/DA357ECG3/>

36. *December 13, Kentucky Enquirer* – (Kentucky) **Man charged with murder in ambulance crash.** A Warsaw, Kentucky man was arrested nearly 5 months after State Police said he slammed into an ambulance killing the patient inside. He was booked into the Carroll County jail December 11, according to jail records. He is charged with murder, leaving the scene of an accident, driving under the influence, criminal

mischievous, and two counts of first degree assault. He was driving a vehicle north on U.S. 127 in Gallatin County July 24 when police said he crossed the center line and hit an ambulance that was traveling south. The ambulance, which was carrying a patient and two emergency medical technicians, flipped and landed on its roof. The patient was taken to a local medical center where he died. The emergency medical technician and ambulance driver were treated at the hospital and later released. He was being held without bond December 13.

Source: <http://nky.cincinnati.com/article/AB/20121213/NEWS0103/312130040/Man-charged-murder-ambulance-crash>

37. *December 13, Associated Press* – (Alabama) **Ala. police officer charged with drug trafficking.** A former Montgomery, Alabama police officer was charged with trafficking marijuana after authorities executed a search warrant and caught him making a delivery, the Associated Press reported December 13. The Montgomery Advertiser reported the officer resigned from the department December 12. Mobile County Sheriff's officials said he was caught delivering more than 3 pounds of high-grade marijuana from Montgomery to a house in Mobile County. The sheriff's office said he was also involved with a 16-acre marijuana growing operation that was shut down in Chunchula, about 20 miles northwest of Mobile. In October, authorities received an anonymous tip and found over 100 marijuana plants drying in a shed, over 150 potted plants, and two boxes of the drug set to be packaged.

Source: <http://www2.alabamas13.com/news/2012/dec/13/ala-police-officer-charged-drug-trafficking-ar-5164422/>

38. *December 13, Washington Times* – (Washington, D.C.) **Bedbugs in firehouse have staff sleeping in trucks.** A bedbug infestation at a northwest Washington, D.C. fire station left firefighters sleeping in their personal vehicles or in the firetrucks to avoid being bitten by the bugs in their bunkrooms, a report on the conditions at Washington, D.C. firehouses found, the Washington Times reported December 13. The 180-page report by the Office of the Inspector General details a wide swath of problematic conditions at Washington, D.C. fire stations, including a lack of working smoke detectors, leaking roofs, flooded basements, rodent infestations, and inoperable heating or cooling systems. Among the findings, 19 stations had significant rodent problems with one reporting that dead mice had been found in a refrigerator, seven did not have functional heating systems in living quarters, 27 did not have fire extinguishers, and 22 reported that the monitor that displays call information either was not working or was unreliable. Complicating matters is the fact that the department has no formal policy for reporting and overseeing repairs. In response to questions about inspection schedules, department officials wrote in October that several areas of maintenance, including roofs and bay doors for the trucks and ambulances, are now undergoing preventative maintenance and the department is working on prioritizing repairs.

Source: <http://www.washingtontimes.com/news/2012/dec/13/bedbugs-in-firehouse-have-staff-sleeping-in-trucks/>

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

## Information Technology Sector

39. *December 14, Softpedia* – (International) **Upclicker uses left mouse button to execute malicious code when no one is looking.** Experts have identified a trojan that relies on a mouse hooking function to evade sandbox environments. Cybercriminals are aware of the fact that automated analysis systems do not use the mouse, so they have developed their creations so that they step into play only when mouse movement is detected. The trojan analyzed by FireEye, Upclicker, is interesting because the malicious code is executed only after the user clicks the left mouse button and releases it. Upclicker establishes malicious communication only when this particular action is performed. Experts from Symantec previously identified a similar trojan which relied on mouse actions to determine whether or not it was being monitored by security experts.

Source: <http://news.softpedia.com/news/Upclicker-Uses-Left-Mouse-Button-to-Execute-Malicious-Code-When-No-One-Is-Looking-314915.shtml>

40. *December 14, Threatpost* – (International) **Carberp banking trojan goes commercial; Adds bootkit and \$40k price tag.** Weeks after the banning of Aquabox, the keeper of the Citadel banking trojan, from an underground forum, another player has popped up to fill the market gap, this time with a new version of the Carberp trojan. This is a first for the Carberp gang, which until now had never sold its malware in the open, said a communications specialist and team leader for RSA Security's FraudAction team. The new version of the banking malware comes with beefed up data-stealing capabilities and the addition of the Rovnix bootkit and builder kit for a hefty \$40,000 price tag. For fees ranging between \$2,000 and \$10,000, customers can buy the kit as a service, sans the builder and bootkit. The addition of Rovnix, the researcher said, is an especially interesting twist in that it infects a computer's volume boot record, giving it ring0 privileges and making not only difficult to detect, but clean up.

Source: [http://threatpost.com/en\\_us/blogs/carberp-banking-trojan-goes-commercial-adds-bootkit-and-40k-price-tag-121412](http://threatpost.com/en_us/blogs/carberp-banking-trojan-goes-commercial-adds-bootkit-and-40k-price-tag-121412)

41. *December 13, Softpedia* – (International) **Latin America targeted by information-stealing Dorkbot worm.** Dorkbot, the malware involved in the recent Skype spam campaign that might have affected over 1 million users, is currently one of the most active threats that targets Latin America. According to experts from security firm ESET, the malicious element has been seen all over the world, but it is most prevalent in countries such as Columbia, Mexico, Chile, and Peru. Overall, 54 percent of Dorkbot infections have been recorded in Latin America. The worm, which specializes in stealing sensitive information such as usernames and passwords, is also designed to recruit its victims into a botnet. It spreads via various mediums, including Skype, Windows Live Messenger, Twitter, and Facebook. In most cases, victims are lured with promises of new phones or discounts. Currently, the Dorkbot that's making the rounds in Latin America is designed to steal online banking credentials from internauts. A Dorkbot removal tool provided by ESET is available for download.

Source: <http://news.softpedia.com/news/Latin-America-Targeted-by-Information-Stealing-Dorkbot-Worm-314512.shtml>

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

## Internet Alert Dashboard

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 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

42. *December 13, The Register* – (International) **Yet another eavesdrop vulnerability in Cisco phones.** A university student presenting at the Amphion Forum demonstrated turning a Cisco VoIP phone into a listening device, even when it is on the hook, The Register reported December 13. The vulnerability demands a fairly extensive reconfiguration of the phone, according to Dark Reading. This, at least, means the attacker needs greater sophistication than previous eavesdropper attacks reported by The Register in 2007 and 2011. A number of 7900-series phones are affected, according to Forbes. The latest vulnerability is based on a lack of input validation at the syscall interface, according to Columbia University graduate student. He said this “allows arbitrary modification of kernel memory from userland, as well as arbitrary code execution within the kernel. This, in turn, allows the attacker to become root, gain control over the DSP [Digital Signal Processor], buttons, and LEDs on the phone.” In the demonstration, the student modified the DSP to surreptitiously turn on the phone’s microphone and stream its output to the network. To simplify the demonstration, he programmed the necessary reconfiguration onto an external circuit which he plugged into the phone’s Ethernet port, and then captured what was spoken near the VoIP phone on his smartphone. The student told Dark Reading that the phones contain a number of vulnerable third-party libraries, which he promises to discuss at the upcoming Chaos Computer Conference, 29C3. Cisco said workarounds and a software patch are available to address the issue, tagged with the bug id CSCuc83860. Source: [http://www.theregister.co.uk/2012/12/13/cisco\\_voip\\_phones\\_vulnerable/](http://www.theregister.co.uk/2012/12/13/cisco_voip_phones_vulnerable/)

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

## Commercial Facilities Sector

43. *December 14, Mineral Wells Index* – (Texas) **Fire hits Adell church.** A multiple-alarm fire December 13 destroyed a church building used by Adell Community Fellowship in Parker County, Texas. Firefighters from across the county and beyond responded to the fire that became a six-alarm fire with 18 agencies responding, according to the Parker County public information officer. A passerby saw smoke coming from the sanctuary building and called 911 before turning off the propane to the building, the senior pastor said. The two-story metal structure housed Sunday morning services for about 80 to 90

members of the congregation, as well as Wednesday night youth services, he said. The primary need for assistance was manpower, as it was the middle of a weekday, a time when many volunteer firefighters are traditionally at work, according to the Parker County fire marshal. Firefighters from as far away as Wise County were requested. To get water to the scene, tanker trucks from various Parker County fire departments and Precinct 2 shuttled water to the site and firefighters pumped from collapsible temporary water tanks. However due to the size of the structure and because it was a church, he requested the Tarrant County Arson Task Force to assist in the investigation, adding that he knew of nothing to indicate it was arson.

Source: <http://mineralwellsindex.com/topstory/x1332357311/Fire-hits-Adell-church>

44. *December 14, Denver Post* – (Colorado) **Four people set afire in attack at Denver apartment late Thursday.** Denver police detectives looked for a motive in an attack December 13 in the Sunnyside neighborhood. According to police, two men showed up at the door of an apartment. They sprayed two men and two women inside with gasoline, or some other flammable liquid, from a pump garden sprayer, then one of the attackers tossed a match or lighter. One of the women suffered life-threatening burns and was rushed to a local hospital in serious condition. The three others in the apartment in the 4300 block of Lipan Street had comparatively minor burns, said a police spokesman. The fire was out before fire crews arrived, and none of the nearby apartments was affected. Police investigated whether there is any link to an attempted robbery in the Curtis Park neighborhood about 3 miles away. A fire was set using a pump sprayer, but no one was injured. A police spokeswoman said that while that case was similar, it did not appear to be related.

Source: [http://www.denverpost.com/recommended/ci\\_22190174](http://www.denverpost.com/recommended/ci_22190174)

45. *December 13, WTNH 8 Bridgeport* – (Connecticut) **Police stand-off at apartment complex.** Police investigated a shooting inside of an apartment complex in Rocky Hill, Connecticut, WTNH 8 Bridgeport reported December 13. One victim was shot twice. The alleged shooter was found with a gunshot wound after a police stand-off. State Police, the Rocky Hill Police Department, and SWAT were on scene and locked it down completely. No one was able to go in and no one was able to go out for about 3 hours. The victim was taken to the hospital.

Source: [http://www.wtnh.com/dpp/news/hartford\\_cty/police-stand-off-at-apartment-complex#.UMtVdq7kGok](http://www.wtnh.com/dpp/news/hartford_cty/police-stand-off-at-apartment-complex#.UMtVdq7kGok)

For more stories, see items [7](#) and [9](#)

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

## **National Monuments and Icons Sector**

46. *December 13, Seattle Post-Intelligencer* – (Washington) **Washington old-growth poacher stole a ‘national antiquity’.** A Brinnon, Washington logger caught stealing protected, old-growth trees from national forest land on the Olympic Peninsula, pleaded guilty December 13 to damaging government property, and admitted to cutting down more than a dozen trees in the Rocky Brook area of Olympic National Forest. U.S.

Forest Service workers launched an investigation after learning the trees had been cut and removed from the national forest. Investigators determined trees had been taken from hundreds of feet past the boundary line.

Source: <http://www.seattlepi.com/local/article/Washington-old-growth-poacher-stole-a-national-4116933.php#photo-3889890>

47. *December 12, Q13 FOX News Seattle* – (Washington) **Washington state park closed after dog attacks.** Fort Ebey State Park, a 645-acre state park on Whidbey Island, Washington, remained closed December 12 after two “aggressive, unattended” dogs attacked park hikers, Washington State Park officials reported December 12. According to officials, the unattended dogs were discovered in the park December 11, but officials had trouble catching them. The park remained closed December 12 as the search for the dogs continued. “At this time, rangers and county animal control officers are working to confirm the location of the dogs and place them under control,” officials said in a release. “Until this occurs, the park will remain closed.”

Source: <http://q13fox.com/2012/12/12/washington-state-park-closed-after-dog-attacks/>

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

## **Dams Sector**

48. *December 14, Rutland Herald* – (Vermont) **With levee work, Bennington finishes recovery from Irene damage.** Work being done by the U.S. Army Corps of Engineers on the flood wall of the levee in Bennington, Vermont, was the last needed to repair local infrastructure damaged by Tropical Storm Irene in 2011, according to the town manager, the Rutland Herald reported December 14. The Corps determined it would take responsibility for repairing the damage to the flood wall so the work was done at no direct cost to the town. During the heavy rains of Irene, the waters of the Roaring Branch rose and began moving quickly, picking up debris along the way. Enough debris to build up a dam-like structure formed in front of a bridge which passes over North Branch Street. The water undermined the flood wall, also known as a retaining wall, which raised concerns about how it might hold up during a heavy rain event in the future. The town did some repair work, which left the levee safe, but more work was needed to make the flood wall more secure. Bennington’s planning director and zoning administrator said the repairs consisted of boring holes in the wall’s footings and pumping concrete at high pressure to fill any voids underneath the footings. The footings will then be capped and riprap would be added in front of the flood wall and continue along to the bridge, he said. The project should be finished in about a week. The town began work on a process need to obtain recertification of its levee in 2011, a process that was required by a change the Federal Emergency Management Agency made to its flood maps.

Source: <http://www.rutlandherald.com/article/20121214/NEWS02/712149913>

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



**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 <a href="mailto:cikr.productfeedback@hq.dhs.gov">cikr.productfeedback@hq.dhs.gov</a> or contact the DHS Daily Report Team at (703)387-2341
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@hq.dhs.gov](mailto: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](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.