



Homeland Security

Daily Open Source Infrastructure Report for 30 November 2009

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

For information, click here:
<http://www.dhs.gov>

Top Stories

- DarkReading reports that researchers at Red Condor detected a new phishing attack that promises to enhance the security of the user’s mailbox and then downloads a banking Trojan instead. Red Condor says it has stopped more than 3.5 million messages belonging to the spam campaign, which was detected on November 20. (See item [46](#))
- According to the Associated Press, the Governor of New Jersey asked the President on November 25 to declare much of the Jersey shore a disaster area due to damages exceeding \$49 million from a recent coastal storm. Tourism is New Jersey’s second-largest industry, accounting for nearly \$39 billion a year, much of it from the shore. (See item [54](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

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

SUSTENANCE AND HEALTH

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

SERVICE INDUSTRIES

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

FEDERAL AND STATE

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

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

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

1. *November 27, Topeka Capital-Journal* – (Kansas) **Gas spill closes Topeka Blvd.** The Shawnee County Sheriff’s Office said more than 1,000 gallons of gasoline spilled onto the roadway at 1:20 a.m. on November 27 in the 6900 block of S.W. Topeka after a Ryder truck struck a tractor trailer causing it to overturn, said a sergeant. The Ryder

truck pulled out from a stop sign and struck the the gasoline truck, which was traveling northbound, at the main entrance to Forbes Field. The tractor trailer was hauling about 8,500 gallons of gasoline. Due to the hazardous conditions, the road will be closed November 27 from S.W. University Boulevard to S.W. Gary Ormsby Drive. Drivers are encouraged to use S.W. 57th and south US-75 highway as an alternate route. The Topeka Fire Department; Metropolitan Topeka Airport Authority; Shawnee Heights Fire Department; the Topeka Chapter of the Red Cross; HazMat crews, of Overland Park; Shawnee County Emergency Management and Shawnee County road crews assisted the sheriff's department at the scene. The sergeant said in a news release that there were injuries in the accident, but additional information was not immediately available.

Source: http://cjonline.com/news/local/2009-11-27/gas_spill_closes_topeka_blvd

2. *November 25, KTRK 13 Houston* – (Texas) **Overtaken truck shuts down 59 ramp.** An overturned big rig just off the North Loop and Highway 59 may cause some delays for travelers heading to Bush Intercontinental Airport on November 25. The accident happened just before 6 a.m. on the North Loop westbound ramp to the Eastex northbound lanes in Houston. All lanes of the ramp are closed off to traffic and HazMat crews will take a while to clean up oil and fuel spill. Investigators say the driver may have tried to take the ramp too fast, causing the rig to overturn. “The sludge oil is used to clean up the bottom of tanks and it does possibly contain some sort of Benzene,” said an officer with the Houston Police Department. Environmental crews are at the scene as well. Houston police says the big rig driver was not injured in the wreck.

Source: <http://abclocal.go.com/ktrk/story?section=resources/traffic&id=7137922>

3. *November 25, Merced Sun-Star* – (California) **Propane tanks targeted by thieves.** Thieves took several propane tanks in Hilmar the week of November 23, the Merced County Sheriff's Department reported. The first theft was reported around 6 p.m. on November 20, according to the sheriff's spokesman. Someone cut the lock from a propane tank storage area in the 8000 block of Lander Avenue, taking 22 tanks. On Tuesday, around 8:30 a.m. more tanks were reported stolen from another location in the 8000 block of Lander Avenue. It is unknown whether the thefts were related, he said.

Source: <http://www.mercedsunstar.com/victorpatton/story/1193663.html>

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

Chemical Industry Sector

4. *November 26, Connecticut Post* – (Connecticut) **Blaze hits chemical warehouse in Fairfield.** Fire struck a chemical warehouse off the Post Road in the Southport section of town early Thursday, requiring an hours-long hazardous materials cleanup at the business. No one was hurt, despite heavy flames that erupted shortly before 2 a.m. in a storage warehouse at Superior Plating Co. Officials said initial tests show there was no significant environmental impact from the fire. “What made this fire difficult is that some of the chemicals are water reactive,” the fire chief added. Two drums in particular

contained chemicals used to treat ground water. Once hit with water, the chemicals began decomposing and generating heat, which then began melting the metal drums. “The cleanup could possibly take several days,” warned the fire chief. The cause of the fire has not yet been determined. Superior Plating produces chrome and nickel products used to treat and coat metals. The warehouse was built from concrete block, which remained intact. Fairfield Engines 1, 2, 4 and 5; Ladder 2, Rescue 1 and Car 3 were dispatched to the scene, assisted by the Fairfield County Hazardous Materials Team, crews from the state Department of Environmental Protection and the Fairfield Fire Haz-Mat trailer.

Source: http://www.connpost.com/ci_13873376?source=most_email

5. *November 26, Associated Press* – (Minnesota) **Twin Cities freeway ramps open after spill.** A tanker truck carrying sodium hydroxide tipped over about 11:30 a.m. Wednesday as it used the ramp from southbound Highway 52 onto eastbound Interstate 494 in Inver Grove Heights. It leaked a large quantity of the chemical, which is corrosive but not dangerous to breathe. The State Patrol says crews were cleaning up the spill into Thursday morning. The ramp finally reopened just after 2 a.m.

Source: <http://www.inforum.com/event/article/id/260899/group/home/>

6. *November 25, Tonawanda News* – (New York) **Chemical fire guts building.** At around 1:30 a.m. a City of Tonawanda police officer noticed smoke and flames coming from The Environmental Service Group’s building during a nightly check of the area, the fire chief said. The warehouse where the fire started stores various types of hazardous waste, and firefighters had to force their way into the structure. As crews began spraying water into a Dumpster they believe to have been the source of the blaze, it exploded. “It knocked some guys down and sprayed molten metal through the general area,” he added. The chief suspects a mixture of magnesium oxide and other chemicals inside the Dumpster caused the reaction, but no one was injured in the explosion. Once the fire was put out, the Department of Public Works pulled the Dumpster out of the building because the metals were continuing to react with the water inside. A HazMat team from the Town of Tonawanda also responded due to the nature of the facility, and firefighters informed the Department of Environmental Conservation as a precaution in case there was any hazardous runoff. He said \$200,000 is an early estimate of the damage, adding that it could grow after further inspection. The cause of the blaze is still undetermined.

Source: http://www.tonawanda-news.com/local/local_story_329231405.html

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

Nuclear Reactors, Materials and Waste Sector

7. *November 27, Reuters* – (Tennessee) **TVA Tenn. Sequoyah 2 reactor slips to 3 pct power.** Tennessee Valley Authority’s (TVA) 1,126-megawatt Sequoyah 2 nuclear power unit in Tennessee was at 3 percent power early Friday after being manually tripped from 30 percent power on Thursday, the U.S. Nuclear Regulatory Commission (NRC) said in an event report. The unit was tripped based on “indications that the 2A

main feedwater pump turbine was losing vacuum,” according to the report. It had been ramping up from a refueling and maintenance outage begun October 26. All plant system responses to the trip were as expected and an investigation will be conducted to identify the cause of the indicated loss of vacuum and the required corrective actions, the NRC report said. The Sequoyah station is located in Soddy-Daisy, Tennessee, about 150 miles southeast of Nashville.

Source: <http://www.reuters.com/article/marketsNews/idUSN2742001420091127>

8. *November 27, Reuters* – (Pennsylvania) **FirstEnergy Pa Beaver Valley reactor up to 20 pct.** FirstEnergy Corp’s 846-megawatt Beaver Valley 2 nuclear power unit in Pennsylvania was at 20 percent power early Friday, after exiting a refueling and maintenance outage that had begun October 12, the U.S. Nuclear Regulatory Commission (NRC) said in its power reactor status report. Last week the company declared an “unusual event” at the plant, the lowest of the NRC’s four emergency classifications, due to unidentified leakage greater than 25 gallons per minute in the reactor coolant system. The NRC said previously it was looking into why a cross connect valve between the unit’s two trains of shutdown cooling opened, but allowed the company to restart the unit. The 1,738-MW Beaver Valley station is located in Shippingport, Pennsylvania, in Beaver County, about 35 miles northwest of Pittsburgh. The adjacent 892-MW Unit 1 continued to run at full power on Friday, the NRC report said.

Source: <http://www.reuters.com/article/marketsNews/idUSN2741878220091127>

9. *November 26, Knoxville News Sentinel* – (Tennessee) **NRC cites plant for violations.** Nuclear Fuel Services is being ordered to correct operational deficiencies after an investigation found a senior executive with the company had consumed alcohol on duty in violation of federal rules and a physician working for the company provided incomplete information on whether the executive was fit for duty. The Nuclear Regulatory Commission (NRC) has issued orders requiring Nuclear Fuel Services and a physician it contracts with to correct deficiencies in its Unicoi County plant related to the former executive the NRC says violated its fitness-for-duty requirements. The plant also was cited for a failure to administer hearing tests to security officers. According to the NRC, Nuclear Fuel Services is ordered to modify its fitness-for-duty procedures and training and establish policies for the reporting of substance abuse concerns, including creating a corporate ethics hot line and procedures to allow anonymous reporting. The action follows an NRC investigation that found the Nuclear Fuel Services executive consumed alcohol before a scheduled working tour of the facility in 2006 in violation of federal regulations. “The NRC determined that the company failed to immediately relieve the executive of his duties and also failed to administer testing to determine his fitness for duty. Additional apparent violations were identified related to the company’s review of the matter and the executive’s return to work. That executive is no longer employed by NFS and the company was acquired by Babcock & Wilcox in early 2009,” the federal agency said in a statement. Nuclear Fuel Services reprocesses radioactive material into nuclear fuel used in nuclear plants and nuclear-powered vessels in the U.S. Navy.

Source: <http://www.knoxnews.com/news/2009/nov/26/nrc-cites-plant-for-violations/>

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

Critical Manufacturing Sector

10. *November 27, Associated Press* – (Indiana) **Fire damages N. Indiana aluminum processing plant.** Firefighters decided to let a blaze burn itself out at an aluminum processing plant in northern Indiana. Emergency crews were called Thursday night to the U.S. Granules plant in Plymouth, where a fire started in a shed and spread to the main building. No injuries were reported, but dozens of firefighters worked to contain the fire as they could not use water on it because of possible chemical reactions. The fire chief says crews removed combustible items away from the fire and that it would burn itself out. The cause was not immediately known. The company's Web site says the plant processes aluminum foil scrap into granules for industrial explosives, drain cleaners, and other products.
Source: <http://www.chicagotribune.com/news/chi-ap-in-plymouth-factoryf,0,2667711.story>

11. *November 25, KATU 2 Portland* – (Oregon) **Malfunction blamed for fire at Freightliner plant.** A fire that destroyed four Freightliner semi trucks early Wednesday morning was caused by a mechanical/electrical malfunction, according to fire investigators. The fire broke out around 3:15 a.m. at the Freightliner plant located on Swan Island, Portland in the 5300 block of North Channel. A woman on her way to work spotted the flames and called 911. When firefighters arrived, they had to cut a lock on a gate at the facility to reach the fire. Four trucks were completely destroyed and four 50-foot trailers were badly damaged. The loss is estimated at \$1 million. There was some concern about run-off from the firefighting effort making its way into the Willamette River. A fireboat was dispatched to check the outflows in the area and no evidence of contamination was found.
Source: <http://www.katu.com/news/local/73756247.html>

12. *November 25, Chattanooga* – (Tennessee) **2 fire halls approved near Volkswagen plant.** Two fire halls have been approved near the new \$1 billion Volkswagen plant in Chattanooga, including one to be situated near the plant entrance and specifically designed for the plant. Also, the city is building a new fire hall nearby that will serve as a backup for the VW plant and also serve the growing area near the plant. The City Council on November 24 approved a contract with Bradanna, Inc. to construct Fire Station No. 7 at Enterprise South in the amount of \$1,876,000 with a contingency in the amount of \$187,600.00, for a total cost not to exceed \$2,063,600. Also, the city Bond Board approved a \$3.2 million contract with Walbridge Aldinger Company, a Michigan firm, to build the fire hall that is exclusively for the plant. The city and county are covering that cost as part of the incentive package to land VW.
Source: http://www.chattanooga.com/articles/article_163826.asp

For another story, see item [4](#)

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

Defense Industrial Base Sector

See item [26](#)

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

Banking and Finance Sector

13. *November 27, Lansing State Journal* – (Michigan) **Williamston man pleads guilty in Ponzi scheme.** A 28-year-old Williamston man has pleaded guilty in federal court to running a \$1.3 million Ponzi scheme, authorities said. According to the U.S. Attorney's Office in Grand Rapids, the man admitted the week of November 23 that he set up a stock trading company, known as Kingdom First Trading, and solicited investors by promising returns higher than market rate. He consistently lost money in trading, but hid that from investors by e-mailing fake account statements that said they were earning sizable profits and accumulating large balances, authorities said. He took money from new investors to pay earlier investors. He also used that money for rent, automobiles and jewelry, authorities said. He will be sentenced on March 15, 2010 and faces up to 20 years in prison. He pleaded guilty Monday to wire fraud, according to court records. As part of the plea agreement, he must pay more than \$1.31 million in restitution to the victims.

Source:

<http://www.lansingstatejournal.com/article/20091127/NEWS01/311270006/1001/NEWS/Williamston-man-pleads-guilty-in-Ponzi-scheme>

14. *November 27, Wall Street Journal* – (International) **Technical glitch shuts London trade for hours.** London Stock Exchange Group PLC (LSE) on November 26 was hit by a technical glitch, forcing it to suspend the trading of U.K. stocks for more than three hours. The exchange stopped trading of shares at 10:33 a.m. GMT (5:33 a.m. EST) after receiving reports that some stocks had "connectivity issues," a spokesman said. Trading resumed at 2 p.m. GMT, but the cause of the problem was still being investigated. The glitch comes a day after the chief executive officer reiterated plans for the LSE to replace its TradeElect trading engine with a new, faster one. It also comes after another glitch earlier this month when 300 stocks could not be traded for an hour and a half before the market closed. An LSE spokesman said that "There were a number of connectivity issues this morning, so we placed all the order-driven securities into an auction period."

Source:

http://online.wsj.com/article/SB10001424052748703499404574559372702658330.html?mod=rss_markets_main

15. *November 23, WRTV 6 Indianapolis* – (Indiana) **Police: Skimmers take unsuspecting customers' cash.** Several suspected ATM skimming incidents have been reported in recent weeks in communities north of Indianapolis, prompting police to release a surveillance picture of one man believed to be involved. A Carmel police detective said the man pictured recently used a victim's credit card to buy electronics at Fry's

Electronics on 96th Street in Fishers and a Best Buy store on Michigan Road in Carmel. He said he thinks the victim's credit card may have been swiped and reproduced through a skimmer at an area gas station and that similar crimes have occurred recently in Fishers, Westfield, Noblesville, Lawrence and Indianapolis. "There have been several victims throughout Hamilton County, and that card information has been used everywhere from Avon to Muncie...down to Greenwood and a lot of places in between," said the Carmel police lieutenant. Consumers should closely look at any device in which they are swiping a credit or debit card.
Source: <http://www.theindychannel.com/news/21698452/detail.html>

16. *November 23, The Register* – (International) **iPhone worm infects devices and redirecs Dutch online bank users to a phishing site.** The second worm to infect jailbroken iPhone users reportedly targets customers of Dutch online bank ING Direct. Surfers visiting the site with infected devices are redirected to a phishing site designed to harvest online banking login details, the BBC reports. ING Direct told the BBC it planned to warn users' of the attack via its website, as well as briefing front line call center staff on the threat. The chief research officer at F-Secure said the threat had in any case been neutralized. "It [the worm] was targeting ING. The websites it needed for this to work have now been taken down." Anti-virus analysts, still in the process of analyzing the malware, caution that the attack is a bit more complex than simple phishing and seems to involve an attempt to snatch SMS messages associated with online banking transactions. Although the "Duh" or Ikee-B worm exploits the same SSH backdoor as the original Ikee worm, the latest malware is far more dangerous than its predecessor. Doh turns compromised devices into a botnet under the control of unidentified hackers. The Rickrolling ikee worm, by contrast, only changes users' wallpaper to an image of a pop singer. As previously reported, compromised phones are left under the control of a botnet server in Lithuania. Duh changes the root password of compromised iPhones, allowing crooks to log into compromised units and carry out malicious further actions. A SophosLabs researcher used a password cracking tool to discover the malware changes iPhone root passwords from 'alpine' to 'ohshit'. In addition to the two iPhone worms, an earlier hacking/extortion attack (targeting iPhone users in the Netherlands) also exploited the default password SSH backdoor on jailbroken iPhones. Security experts strongly advise users of jailbroken phones to change their passwords from 'alpine' immediately to avoid further attacks along the same lines.
Source: <http://cyberinsecure.com/iphone-worm-infects-devices-and-redirecs-dutch-online-bank-users-to-a-phishing-site/>

For another story, see item [46](#)

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

Transportation Sector

17. *November 27, Associated Press* – (New Jersey) **Report: FAA accused of 'gross mismanagement' at Newark airport.** A federal agency that handles whistle-blower

complaints has accused the Federal Aviation Administration (FAA) of endangering public safety by not changing landing procedures at Newark Liberty International Airport. In a November 19 letter to a White House counsel, the Office of Special Counsel (OSC) reported that it found “a substantial likelihood” that the actions of FAA officials constitute “gross mismanagement and a substantial and specific danger to public safety.” The letter stems from a whistle-blower complaint filed last year by an air traffic controller that described safety issues with planes landing on intersecting runways at the Newark airport. A Controller contended that simultaneous arrivals on the runways often led to loss of separation between aircraft and increased the risk of midair collisions and runway incursions. The Department of Transportation’s Office of the Inspector General agreed with the allegations in a report filed last month, and the FAA said it would make changes to the landing procedures by October 26. The FAA reported 10 days later that it had done so when it actually had not, according to the OSC letter. An investigator told the OSC “the procedures have not been implemented and FAA has not completed critical steps that FAA represented it had accomplished,” Associate Special Counsel wrote. One key change was to have controllers on Long Island stagger arrivals into Newark to relieve pressure on controllers to keep the aircraft out of each other’s way.

Source: http://www.usatoday.com/travel/flights/2009-11-27-faa-safety-newark_N.htm

18. *November 25, WNYW 5 New York* – (New York) **Jet aborts takeoff at LaGuardia Airport.** An AirTran jet heading from LaGuardia to Akron, Ohio had to abort takeoff Wednesday evening because of some kind of mechanical trouble, sources said. Flight 206 had 114 passengers and 5 crew members on board, the FAA said. No one was hurt. Emergency crews responded and escorted the plane back to the gate. The Port Authority said a smoke condition was reported on the plane around 9:30 p.m. Passengers told Fox 5’s that they heard a loud noise when the jet was taxiing down Runway 13, which was closed for a time.

Source: http://www.myfoxny.com/dpp/traffic/traffic_news/091125-jet-aborts-takeoff-laguardia

19. *November 25, Panama City News Herald* – (Florida) **Runway extension still on hold.** Construction officials at the new Panama City-Bay County International Airport met November 25 to decide what to do if the Federal Aviation Administration (FAA) approval does not come through in the next few days to extend the concrete runway to 10,000 feet. Crews began installing low-visibility navigation equipment along the 8,400-foot runway this week in anticipation of a January 18 FAA test flight, the test date needed to meet the May 18 grand opening. But without quick FAA approval on the extension, which takes about six week to complete, the FAA will test only the shorter runway forcing the airport to open with only an 8,400-foot capability, said the project manager. Phoenix Construction officials have said they needed to begin construction on the 1,600-foot extension this week to make the January 18 deadline. Officials want to decide if work could begin early next week if FAA approval comes at the last minute. Airport Authority board members had hoped to open the new \$318 million Northwest Florida Beaches International Airport with the full 10,000-foot runway by the grand opening date, when Southwest Airlines is set to make its first

flight into the facility. The navigation equipment, called an ILS, or Instrument Landing System, is required on all FAA-sanctioned runways and allows planes to land in low visibility using only their instruments, such as during heavy fog or rain conditions. The equipment, which arrived Monday and should be completely installed by the end of the year, consists of a localizer at the end of the runway that points the plane in the right direction, and an elevation sensor off to the side of the runway that allows for the proper glide slope, the project manager said. The cost of the equipment is borne by the FAA.

Source: <http://www.newsherald.com/news/bay-79387-extension-hold.html>

For more stories, see items [1](#), [2](#), and [5](#)

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

Postal and Shipping Sector

See item [30](#)

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

Agriculture and Food Sector

20. *November 25, Associated Press* – (Maine) **Maine cops say baked beans plant fire was arson.** Fire investigators say a fire that damaged the B&M Baked Beans factory in Portland was arson. Portland fire officials say the fire in a storage facility filled with cardboard was reported at about 2:45 a.m. Sunday. Officials say the fire was extinguished by the building's sprinkler system. The building did sustain smoke damage. There were no injuries.

Source: <http://www.claimsjournal.com/news/east/2009/11/25/105582.htm>

21. *November 25, South Coast Today* – (Massachusetts) **Police investigating string of soda bottle explosions in New Bedford.** Police are looking for a suspect believed to be responsible for a string of soda bottle explosions in New Bedford's South End. The "chemical reaction devices" — made with aluminum foil and chemicals stuffed inside 2-liter plastic bottles — have been placed in front of convenience stores and restaurants late at night in the area of County Street, Cove Road, and Rodney French Boulevard. Though the explosions were loud, there have been no reported injuries or property damage. The most recent incident occurred around 11:20 p.m. November 24 when police received a report of an explosion in front of the 7-Eleven convenience store at 1024 Cove Road. A man believed to be the suspect was seen running from the area, and disappeared behind the Howland Green Library. Police said two devices were found at the scene: the one that detonated and a second device that had been placed inside a garbage can in front of the convenience store. The device had malfunctioned. Police also found a third device behind the library. Because of the similarity of the devices, police and fire investigators believe the same suspect is responsible for other weekend explosions. On November 21, around 1:18 a.m., two devices detonated in front of the

South End Police Station at 168 Cove St. and Campino Cafe at 821 South First St. A third device also detonated around the same time in front of Tony's Bar at 118 County St. Around 12:39 a.m. November 22, police said the suspect threw two devices off a nearby rooftop that landed in front of Tony's Bar and Fernando's Sports Bar on County Street. One device detonated while the other malfunctioned. A state police bomb squad arrived to deactivate the device. The devices were designed to explode when the chemical reaction resulted in pressure building inside the plastic soda bottles.

Approximately 120 pounds of pressure is needed to detonate the device, police said.

Source:

<http://www.southcoasttoday.com/apps/pbcs.dll/article?AID=/20091125/NEWS/911259988/1018/OPINION>

22. *November 24, U.S. Food and Drug Administration* – (Louisiana) **FDA seeks permanent injunction against Sharkco Seafood International Inc.** The U.S. Food and Drug Administration (FDA) is seeking a permanent injunction against Sharkco Seafood International Inc., located in Venice, Louisiana. The injunction is intended to stop the seafood processing company from distributing scombrototoxin-forming fish in interstate commerce. Consumption of scombrototoxin-forming fish that are not properly preserved or refrigerated can result in scombroid food poisoning, a foodborne illness that results from eating spoiled or decayed fish. The government's complaint filed by the United States Attorney's Office for the Eastern District of Louisiana charges Sharkco Seafood and its owners with violating the Federal Food, Drug, and Cosmetic Act by failing to establish and implement an adequate Hazard Analysis and Critical Control Point (HACCP) plan for their scombrototoxin-forming fish. FDA requires all seafood processors and distributors to have a HACCP plan that determines and monitors food safety hazards associated with their products. According to the government's complaint, FDA inspections showed that the defendants failed to have an adequate written HACCP plan for their scombrototoxin-forming fish operation, despite numerous warnings by FDA. The formation of scombrototoxin can be adequately controlled when fish are appropriately preserved or refrigerated. Once formed, however, scombrototoxin cannot be removed or destroyed by washing, freezing, or cooking the affected fish. No illnesses have been associated with Sharkco Seafood's scombrototoxin-forming fish products.

Source:

<http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm191966.htm>

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

Water Sector

23. *November 26, Sun Gazette* – (Virginia) **One dead, water supply still impeded after water-main break.** The Arlington County government continues to grapple with a significant water-main break in the northern part of the county, while mourning a government employee who died Wednesday in an accident at the site. The employee, 59, was electrocuted about 8:40 a.m. on November 25 after he and a second employee came into contact with a power line as they were removing lighting at the site of the

water-main break, on Old Glebe Road and North Dittmar Road. County work crews had been grappling with the break since November 23. The lighting was being used to help crews work through the night to repair the broken pipe. Immediately after the electrocution, power was cut to approximately 1,000 homes in the area, and traffic was restricted in the vicinity. Power later was restored to homes. The Arlington County Police Department and Virginia Occupational Safety and Health Administration are jointly investigating the cause of the accident. County officials say crews believed that they had repaired the 36-inch water main November 24, and were performing follow-up operations when the accident occurred. New cracks opened in the repaired pipe November 25, and work continued to repair the water main. The county “is deploying every available resource to repair the pipe,” which feeds a large cistern that supplies water throughout north Arlington, government officials said. “Drinking water remains completely safe, but the water level in our cistern is low and we ask residents to restrict their water usage until further notice,” said the acting director of the county’s Department of Environmental Services. The rupture has reduced the water supply in a 12-million gallon cistern to just 4 million to 5 million gallons. The county government is importing water from the City of Falls Church to replenish the cistern, county government officials said.

Source: <http://www.sungazette.net/articles/2009/11/26/arlington/news/nw343.txt>

24. *November 25, Water Technology Online* – (California) **2010 will feel full stimulus for water: analysts.** The impact on water industry companies of most of the federal stimulus spending on water/wastewater infrastructure will be felt in 2010, financial analysts at investment firm Janney Montgomery Scott (JMS) wrote in a November 24 report. The report also says that recent media investigations about the lack of enforcement of water quality regulations — such as an ongoing series of articles in the New York Times — is “turning up the heat” to make politicians and the public more aware of water infrastructure issues. After the current recession has run its course, growth rates in the municipal water and wastewater industry will resume during the next two to three years their previous “catch-up” growth rates of 2 to 2-1/2 times the rise in gross domestic product, according to JMS. Noting that \$30 billion to \$40 billion in annual funding is needed to fix the huge backlog in improvements of aging water infrastructure, the report noted that “stimulus funding support hardly fills local demand.” As has long been the case, JMS analysts believe, gaining public and political support for increased financing — including increased water/wastewater service rates — is the key in the United States, which the report said, “has been lulled into complacency by decades of cheap water service.” JMS notes that this heightened public awareness of water’s true costs may be starting to take hold in California, where there has been “relatively little public outcry” over some recent significant rates increases during water shortages. “Californians are finally realizing the value of water,” the analysts wrote.

Source: http://www.watertechonline.com/news.asp?N_ID=73013

25. *November 25, Minnesota Public Radio* – (Minnesota) **Study finds chemicals widespread in Minn. waters.** Minnesota scientists say it appears endocrine-disrupting chemicals and pharmaceuticals are found in even the most pristine lakes in the state.

Researchers say they are not sure why the chemical compounds are so widespread, but they say more research is needed to better understand the potential impact on wildlife and humans. The Minnesota Pollution Control Agency (MPCA) sampled a dozen lakes and four rivers across the state. Some of the samples came from water close to cities and others were from lakes in remote northern forests. An environmental research scientist said they looked for 110 compounds including residue from plastic bottles, household detergents and pharmaceutical drugs. Bisphenol A, a compound found in polycarbonate plastics, was found in 82 percent of lakes, the common painkiller acetaminophen was found in 50 percent of samples, 4-octylphenol diethoxylate, a detergent ingredient was found in 36 percent of lakes and 71 percent of rivers. One of the puzzles for researchers is Northern Light Lake north of Grand Marais. Endocrine-disrupting compounds are thought to come mostly from sewage treatment plants, or septic systems. Northern Light Lake has neither; it is an undeveloped lake with just a public boat ramp. Minnesota researchers say right now they only have a snapshot of chemical contamination in the state's waters. They plan to continue testing lakes and streams, looking for trends. The MPCA also plans to start testing groundwater next year to see if the chemicals that appear ubiquitous in surface water are also making their way into underground aquifers.

Source: <http://minnesota.publicradio.org/display/web/2009/11/24/water-quality-testing/>

26. *November 24, Environment News Service* – (Wisconsin) **Wisconsin groundwater standards for explosives could set national precedent.** A move by the Wisconsin Department of Natural Resources (WDNR) to set standards for a carcinogenic explosive in groundwater is being applauded by rural neighbors of the Badger Army Ammunition Plant, but is expected to draw opposition from the U.S. military. The WDNR recently received approval from the state's Natural Resources Board to hold public hearings on the addition of 15 new substances to the state's groundwater quality standards including all forms of dinitrotoluene, DNT — a carcinogenic explosive that has contaminated drinking water wells near the Badger Army Ammunition Plant in the rural townships of Merrimac, Sumpter and Prairie du Sac. If approved by the legislature, Wisconsin will set a precedent for other states that could be significant for over 100 sites across the country contaminated with DNT. Based on recommendations from senior toxicologists at the Wisconsin Division of Public Health, all six forms, or isomers, of DNT will be regulated as a single entity. The proposed standard is 0.05 parts per billion.

Source: <http://www.ens-newswire.com/ens/nov2009/2009-11-24-094.asp>

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

Public Health and Healthcare Sector

27. *November 26, Associated Press* – (Texas) **16 employees fired from TX hospital district.** Sixteen employees have been fired from the Harris County Hospital District for alleged violations of patient privacy laws involving the records of a first-year resident, according to a district official. The Houston Chronicle reports that the workers were fired on November 20 for looking at the medical records of a first-year Baylor

College resident assigned to Ben Taub General Hospital. A District spokeswoman told the Associated Press on November 25 that some of the 16 employees who were terminated worked at Ben Taub and at Northwest Health Center.

Source:

<http://www.dallasnews.com/sharedcontent/APStories/stories/D9C6U6CO0.html>

28. *November 25, WISN 12 Milwaukee* – (Wisconsin) **Laptop with personal information stolen from Aurora St. Luke’s.** A Milwaukee hospital is warning thousands of its patients that personal information about them may have been stolen. A laptop computer was stolen in mid-October at Aurora St. Luke’s Medical Center on Milwaukee’s south side. Approximately 6,400 patients who were in-patients at St. Luke’s will be getting a letter in the mail. It warns them that their name, Social Security number, and other information may have landed in the hands of thieves. “The computer was stolen from a locked office in a secure physician office building that’s located adjacent to the hospital, and the computer belongs to an employee of Cogent Healthcare of Wisconsin,” said a spokesperson for Cogent Healthcare. On Wednesday, Cogent began notifying those people in a letter that also assured patients that copies of their medical records were not stored on the laptop.

Source: <http://www.wisn.com/news/21726827/detail.html>

29. *November 25, Foster’s Daily Democrat* – (New Hampshire) **Pathology lab doctors say WDH punishing them for reporting privacy breaches by rogue employee.** Two doctors who run the pathology lab at Wentworth-Douglass Hospital in Dover, New Hampshire say they will soon be out of a job because the WDH President and CEO is punishing them after they discovered “massive and systematic violations of patients’ privacy” by a rogue hospital employee. The two doctors, who run the contracted and independent Piscataqua Pathology Associates, laid out their case in a recent letter to members of the WDH board of trustees, explaining how the hospital is ending a 28-year relationship with their practice three years after they first became suspicious of the employee breaching patient privacy. The breach took place between May 21, 2006, and June 29, 2007, at the hands of a hospital employee who improperly altered 1,500 reports and accessed them 1,847 times, according to a copy of the letter obtained by Foster’s. A WDH spokeswoman confirmed the employee was terminated when an audit revealed the employee was behind the problem, and she stressed patient safety was not compromised. Foster’s has obtained a copy of the audit, the veracity of which was confirmed by the hospital. Among the findings are 150 instances where a physicians’ name was removed or switched, indicating patients’ reports could have been sent to the wrong place. The audit also indicates the breach extended into at least one other state. The doctors’ letter to trustees claims the ex-employee, who was not employed by Piscataqua Pathology Associates, infiltrated the reports on hospital time “utilizing passwords the Hospital failed to change.” The WDH spokesperson said she did not know enough to explain whether that allegation meant the ex-employee retained access rights to the software used in the pathology lab beyond a point she was supposed to. The breach is just now coming to light because an audit launched to survey the damage was not completed until late May.

Source:

http://www.fosters.com/apps/pbcs.dll/article?AID=/20091125/GJNEWS_01/711259913

30. *November 25, KNXV 15 Phoenix* – (Arizona) **Bomb squad investigates parcel sent to health worker.** A police bomb squad is checking out a package delivered to a behavioral health services worker Friday. The Phoenix Police sergeant said a package was delivered to a case worker at the Terros Behavioral Health Services office located near 31st Street and McDowell Road around 2 p.m. He said the package's sender had just been incarcerated at the Arizona State Hospital, a state mental health institution. The case worker felt that the package was suspicious and called police, he said. There is no word so far about the package's contents.
Source: <http://www.abc15.com/content/news/phoenixmetro/central/story/Bomb-squad-investigates-parcel-sent-to-health/7asloLE5wkWmSIrWpkqOIw.csp>

31. *November 25, WKBT 8 La Crosse* – (Wisconsin) **Tomah hospital, high school briefly locked down for person with gun.** Tomah Memorial Hospital and Tomah High School were locked down briefly Wednesday after a person reportedly had a gun at the hospital. Tomah Police say officers were called to Tomah Memorial just after 11:30 a.m. for someone who was possibly suicidal and was headed to the hospital with a loaded handgun. After getting this information, police locked down both the hospital and high school. Officers found the person inside the hospital and took them into custody, but did not find a gun. Officers did find a gun with ammunition in the person's vehicle parked in front of the hospital. Tomah Memorial and Tomah High School both resumed normal activities after being locked down for about 11 minutes. Tomah Officers verified the location of the handgun and determined there was no longer a public safety concern. The Tomah Memorial Hospital and the Tomah High School were notified and both facilities resumed normal operating procedures.
Source: <http://www.wkbt.com/Global/story.asp?S=11574432>

32. *November 25, Tampa Bay Newspapers* – (Florida) **Bomb squad called in.** The Florida State Fire Marshal's Office bomb squad was called in to help dispose of five containers of ether that had crystallized November 23 at Smith & Nephew, a wound management product development company at 11775 Starkey Road in Largo. The 120,000 square foot facility has been working with a skeleton crew of approximately 13 workers since the company ceased operations on September 25. The week of November 23, five containers of crystallized ether were discovered in a refrigerator. This material is considered to be highly explosive — similar to approximately one pound of C4. "The facility administrator immediately took proactive steps to ensure the safe removal and disposal of the product," said the Seminole Fire Rescue District Chief. "A unified command system was established consisting of the Florida Department of Environmental Protection, the Florida Fire Marshal's Bomb Squad, Pinellas County Sheriff's Office and The City of Seminole Fire Rescue Department." The bomb squad's remote controlled robot was sent in to remove the containers from the refrigerator. The crystallized ether was then transported in a bomb disposal container to the Pinellas County Waste Management site on 28th Street and detonated safely.

Source: http://www.tbnweekly.com/pubs/largo_leader/content_articles/112509_1le-02.txt

33. *November 25, Las Vegas Review-Journal* – (Nevada) **UMC risking steep fines over patients' privacy.** Because of recent changes in federal law, University Medical Center could face steep fines over allegations of violations of patients' privacy. One part of the economic stimulus law enacted in February calls for federal agencies to impose fines as high as \$1.5 million on medical providers who inadequately protect patients' data. Fines jumped from \$100 per violation to as much as \$50,000 each for the most willful negligence. Penalties are capped at \$1.5 million total for offenses within a calendar year. The new rules went into effect in September but cover any infractions that happened after the American Recovery and Reinvestment Act was signed into law on February 17. Recently, hospital executives were alerted to accident victims' personal information being dispensed to local attorneys who could use it to solicit business from these patients. A more pressing concern is that the pilfered data could lead to identity theft. Officials suspect at least one employee is behind the scheme. A hospital spokesman said UMC is following the federal guidelines. "The only way UMC would face fines or penalties is if we had confirmed evidence of a breach and chose to do nothing." The FBI has begun an investigation into UMC's security breach. The new rules allow state attorneys general to get involved in some instances, even though HIPAA is a federal law. Still, the state attorney general spokeswoman said her office has no plans to jump in unless invited. The Clark County auditor, although rating the hospital a relatively high 82 percent for HIPAA compliance, observed flawed safeguards. Patient records were left unattended on desks or on computer screens, he wrote. Outgoing e-mails containing sensitive data were not encrypted. Many employees did not record information that was disclosed to third parties, creating the possibility for identity theft, he said. This type of reporting helps pinpoint who was authorized to receive the data and who was not, he said. "However, UMC is currently unable to provide patients with a meaningful report," he wrote.
- Source: <http://www.lvrj.com/news/umc-risking-steep-fines-over-patients-privacy-73391682.html>

34. *November 24, WebMD* – (National) **MRSA strain on the rise in hospitals.** A potentially dangerous and rapidly spreading strain of the "superbug" MRSA poses a much greater public health threat than previously thought, new research shows. Community-associated MRSA (CA-MRSA) is spreading in hospitals and other health care facilities, according to a study in the December issue of *Emerging Infectious Diseases*. The CA-MRSA strain of superbug can be picked up in fitness centers, schools, and other public places, and is increasing the already significant burden of MRSA (methicillin-resistant *Staphylococcus aureus*) in hospitals, the researchers report. The study, which analyzed data from more than 300 microbiology labs across the United States, found a sevenfold increase in the proportion of CA-MRSA in outpatients between 1999 and 2006. This community-associated strain is making its way into hospitals, the researchers say, increasing threats to patient safety because patients and their doctors move back and forth between inpatient and outpatient units of hospitals. Over the length of the study, the scientists report finding that the proportion

of MRSA had increased more than 90 percent among outpatients with staph, and now accounts for more than 50 percent of all Staphylococcus aureus infections. This was due, the findings suggest, almost entirely to an increase in CA-MRSA strains. Similar increases in inpatients suggest these strains are spreading rapidly into hospitals.

Source: <http://www.webmd.com/skin-problems-and-treatments/news/20091124/mrsa-strain-on-the-rise-in-hospitals>

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

Government Facilities Sector

35. *November 27, Coloradoan* – (Colorado) **Justice Center to keep security.** Saving money on security at the Larimer County Justice Center in downtown Fort Collins has proven more difficult than county officials thought. Keeping both entrances to the building at 201 LaPorte Ave., open and staffed - as well as staffing the courthouse in Loveland - is expected to cost \$185,000 next year, about \$20,000 more than in 2009. Efforts to cut back on security and save money have not worked out, a county Manager told the county commissioners November 25. Having inadequate security could be a liability issue for the county, he said. The Larimer County Sheriff's Office provided security at the entrances of the justice center and the Loveland courts until this year, when the service was cut because of budget problems. The responsibility was shifted to the county's facilities department, which was given a \$100,000 budget. Security at the courthouse entrances has been handled by a private contractor. Security inside the courtrooms still is provided by deputies from the Sheriff's Office. The deputies rely on the private security guards to screen people as they enter the building. The guards regularly find weapons and contraband, he said. In July, officials considered closing one entrance to the justice center but met resistance from judges who hold court in the building. The judges' concerns included the possibility of having long waits to get into the building.

Source: <http://www.coloradoan.com/article/20091127/NEWS01/911270310/Justice-Center-to-keep-security>

36. *November 27, Los Angeles Times* – (District of Columbia) **Secret Service breakdown blamed for White House gate-crashing.** The Secret Service has launched a "comprehensive investigation" of its security measures after two aspiring reality-TV stars crashed the President's state dinner at the White House on November 25. The couple strolled into the dinner honoring the Indian Prime Minister and mingled with the power people of Washington — even though they were not on the invitation list. More than a dozen photos were posted on Facebook showing the couple with various luminaries, including the Vice President, the White House Chief of Staff and a well known "CBS Evening News" anchor. A Secret Service spokesman said initial results of the investigation showed that "...procedure wasn't followed" at one security checkpoint, allowing the uninvited guests to enter. An administration official said the gate-crashing was apparently a breakdown in Secret Service screening and not the work of the White House social office. The White House requested an investigation, but the Secret Service had already begun one after discovering the incident. The spokesman

stressed that everyone at the party, including the gate-crashers, passed through rigorous safety checks. Once inside, the couple easily blended into the crowd of more than 300. Source: <http://www.latimes.com/news/nation-and-world/la-na-crashers27-2009nov27,0,5113097.story>

37. *November 24, Orange County Register* – (California) **1 arrested as 300 protest at UC Irvine.** As many as 300 UC Irvine students and supporters marched around the Orange County campus on November 25, waving signs and chanting slogans against a 32 percent undergraduate fee increase approved last week by the Board of Regents. About 15 helmet-clad campus police officers stood between students and the entrance to the campus administration building as demonstration leaders rallied the cheering and shouting crowd. At one point, students stood face to face with campus police, separated by plastic crowd control barriers. The students yelled and demanded entrance into Aldrich Hall so they could speak with the school Chancellor. Later, about 70 students approached the side entrance of the building to make another attempt to enter. A handful of officers then arrived from inside and pushed some of students back. One student was arrested for attempted vandalism and resisting arrest as students tried to enter, campus police said. Two students were eventually allowed into the building just after 1:30 p.m. About 20 minutes later, the students emerged from the building, saying they were told the chancellor was not at the university. Students rallied last week in large numbers at UCLA, where the regents made the decision to raise fees to \$10,302, taking over buildings and getting arrested. Protests also occurred at UC Berkeley and at UC Davis, but only about 30 or so students demonstrated at UC Irvine. Tuesday's numbers were estimated at 200 to 300. A University spokeswoman said the school supports the right of the students to demonstrate. Source: <http://www.ocregister.com/articles/students-221028-irvine-campus.html?pic=1>

38. *November 24, Homeland Security Today* – (National) **Inauguration security was sound, IG says.** Security arrangements made by the U.S. Secret Service for the inauguration of the President were “reasonable” and the agency’s after-action review of procedures for inaugural events were “prompt and thorough,” concluded the Inspector General (IG) of the Department of Homeland Security (DHS) in a recent report. The house Homeland Security Committee Chairman tasked the IG office with examining the security procedures of the Secret Service during the inauguration after a Washington Post article, dated January 30, raised concerns that security was lax for some VIP events. The IG examined the Secret Service’s methods and its after-action review conducted with the Capitol Police, Washington Metropolitan Police, and US Park Police—which culminated in a report, *The Multi-Agency Response to Concerns Raised by the Joint Congressional Committee on Inaugural Ceremonies for the 56th Presidential Inauguration*, on March 17. The IG report, titled *US Secret Service After-Action Review of Inaugural Security*, responded to concerns over the adequacy of security at select events and the quality of the after-action review of security concerns. Specifically, guests who were screened for weapons and other banned items were able to mingle with the general public before boarding buses to reserved seats for the inaugural events, the report noted, prompting questions as to whether the screening methods were effective. The Secret Service and its partner agencies also conducted a

thorough after-action review, the report found, identifying areas for improvement. The IG office recommended that the Secret Service inform it of the implementation of any changes that arise from those improvements.

Source: <http://www.hstoday.us/content/view/11210/128/>

39. *November 24, Purdue Exponent* – (Indiana) **Students protest student arrests for leaving suspicious box.** A Purdue student who was arrested on November 26 in connection with a suspicious package left at the Visitor Information Center has still not been formally charged, but that is not stopping students from protesting his arrest. A senior in the College of Engineering from Andover, Massachusetts, was arrested by Purdue Police on Thursday morning in connection with a package found in the Visitor Information Center. He faces preliminary charges of terroristic mischief and possession of stolen property. The package was x-rayed and found to contain a parking ticket, a wheel lock and \$20. The Purdue Police Chief said the case is still under investigation. The next step is for the Tippecanoe prosecutor's office to review the case and decide what to formally charge the student with. On Monday afternoon in front of The Exponent building, half a dozen students and members of the community gathered to voice their opinions on the student's arrest.

Source:

http://www.purdueexponent.org/index.php/module/Section/section_id/18?module=article&story_id=18951

For another story, see item [31](#)

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

Emergency Services Sector

40. *November 27, Associated Press* – (Oklahoma) **Police SUV found, suspect arrested in McClain Co.** McClain County authorities say they have arrested a man suspected of firing shots at a Dibble police officer and stealing the officer's SUV patrol vehicle. Officials say the SUV was found Friday afternoon in a rural area, and the man accused of driving it away was arrested later at another site. A manhunt was launched early Friday morning after authorities said a man fired shots at the Dibble officer and then fled in the officer's patrol vehicle, following a traffic stop. Officials say the officer managed to return fire and shot out the rear window of the white Ford Expedition as the suspect sped away.

Source:

http://www.normantranscript.com/localnews/local_story_331154508.html?keyword=topstory

41. *November 26, Las Vegas Review-Journal* – (Nevada) **Vegas fusion center fights terrorism, street crime.** When a tip arrived about a threat of violence at a southern Nevada high school football game, a Clark County School District police officer helped plan a response. When a Colorado man was arrested on terrorism charges, a Department of Homeland Security analyst probed whether he had Las Vegas ties.

Though the two cases are very different, the officials who worked them were in the same cubicle-filled room at the Southern Nevada Counterterrorism Center. Open for more than two years, the Las Vegas “fusion” center is battling terrorism and street crime, a dual mission that has affected how local and federal law enforcement agents view each other and their jobs. The fusion center concept is grounded in the idea that information flow between police agencies is the key to stopping terrorism. In Las Vegas and elsewhere, the concept has evolved to include a broader “all crimes, all hazards” approach. A sign that federal law enforcement has embraced this strategy came last month when the U.S. Attorney General visited Las Vegas and praised the local fusion center as a national model. The maturation of the facility coincides with the Nevada Governor’s decision last month to fold the State’s Office of Homeland Security into the Nevada Division of Emergency Management. Some federal agents have complained Las Vegas police have been slow to share valuable information. A police counterterrorism officer acknowledged that information exchange has not been seamless. He blamed computer software problems and “institutional issues that have taken us a while to get around.” “There was information we weren’t used to sharing with each other,” he said.

Source: http://www.mercurynews.com/news/ci_13872322

42. *November 25, Greenville Herald Banner* – (Texas) **Jail evacuation drill deemed successful.** A non-emergency jail evacuation at the Hunt County Jail on November 24 went smoothly and several areas for improvement were identified, according to the Hunt County Sheriff. Beginning at approximately 1:30 p.m., Sheriff’s deputies and jailers partnered with the Greenville Police Department and Texas Department of Public Safety to conduct a non-emergency jail evacuation simulating severe damage to the jail leaving it uninhabitable following a severe storm. The drill was videotaped for training purposes and to identify areas for improvement. “It went really well. We did have some communication issues because DPS, GPD and Sheriff’s deputies talk on different radio channels,” said the Hunt County Undersheriff. “The IRIS notification system will help us in the future,” he added, referencing county’s participation in the emergency notification system following Monday’s meeting of the Commissioners Court. During the drill, maximum security inmates, portrayed by volunteers, were transferred to the City of Greenville Jail via Greenville Independent School District buses escorted by DPS and GPD officers. The jail was under lockdown throughout the drill and no inmates were used. “There were a few glitches,” said the Hunt County Sheriff. “We had two major accidents in the county during the drill, and the deputies responding to those would have covered the perimeter at the jail. But that also gave us a good test of what we can expect during an actual situation.”

Source: http://www.heraldbanner.com/local/local_story_329230549.html

43. *November 25, Associated Press* – (Arizona) **8 injured after riot involving more than 100 inmates at Arizona prison; unit on lockdown.** A fight broke out on November 25 among more than 100 inmates at an Arizona prison, injuring 7 inmates and a corrections officer, a corrections official said. The officer suffered bumps and bruises, and five of the inmates were flown to a Phoenix hospital, the Arizona Department of Corrections spokesman said. The prison was on lockdown for several hours, he added.

The two other inmates were taken by vehicle, while the officer did not need to go to the hospital. Several of the inmates had head injuries but none of the injuries were life-threatening, said a spokesman for the Maricopa Medical Center. The Corrections spokesman said no weapons were used in the fight, which broke out around 9 a.m. in a high-security unit of the Lewis prison complex, about 35 miles west of Phoenix. It was mostly in the recreation yard and the kitchen. He said the reason why the fight broke out was under investigation. He said prison guards ended the fight with verbal commands and by using pepper spray on some inmates. “It was a quick response by officers that ensured limited injuries and ensured staff and inmates were protected,” he said.

Source: <http://www.whnt.com/news/nationworld/sns-ap-us-prison-fight-arizona,0,6586290.story>

For more stories, see items [12](#) and [21](#)

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

Information Technology Sector

44. *November 27, The Register* – (International) **Smut-laden spam disguises WoW Trojan campaign.** A malicious spam campaign that attempts to harvest online game passwords under the guise of messages containing smutty photos is doing the rounds. The tainted emails have subject lines such as “Do you like to find a girlfriend like me?”, and an attached archive file called “my photos.rar”. The supposed video files actually harbored video files and a password-stealing Trojan called Agent-LVF, which is designed to steal the login credentials of World of Warcraft gamers. Security firm Sophos reckons it is likely the stolen credentials and associated in-game assets will be sold through underground sites, earning hackers a tidy profit in the process. “A surprising amount of malware is designed to steal registration keys, passwords and data from players of computer games,” said a consultant at Sophos. “This isn’t just about doing better in a computer game. Criminals are stealing virtual assets like armour, money and weapons to trade for hard cash in the real world.”

Source: http://www.theregister.co.uk/2009/11/27/wow_trojan_spam/

45. *November 25, ComputerWorld Canada* – (National) **H1N1’s IT threats may not be taken seriously.** It appears that the threat of an H1N1 outbreak has not prompted enterprises to re-evaluate their disaster recovery plans or better enable a mobile workforce, according to a new Cisco Systems Inc. study. The networking giant found that only 22 percent of survey respondents consider their remote-access infrastructure to be disaster-ready. The survey polled 500 IT security decision-makers at U.S. health-care, financial, retail, and public sector organizations last month. In addition, the reported indicated that 21 percent of respondents admitted to having no employees enabled to work remotely and 53 percent said that less than half of their employees are capable of working from home. The director of security solutions marketing at Cisco said many of these organizations will be the hardest hit in the event of a flu pandemic. But even less extreme circumstances, such as a major road closure or a winter storm,

would probably have a noticeable impact on the business as well. Ensuring that all essential workers are enabled with remote-access capabilities is crucial, he added, to operating business as usual during unexpected events. Providing remote VPN connectivity back into the office might be enough for a mobile worker that just requires e-mail or a select few applications, but for employees who require real-time communication and full telephony capabilities, some investments should be made, he said. A security analyst at Fusepoint Managed Services Inc. said the first issues he would address as an IT security leader would be technology-related. “Do we have the tools and technologies in place for employees to be working remotely?” he said. “Do we have the bandwidth? Do we have the storage capability within our phone systems and e-mail servers to be able to queue two or more weeks of data from more than 40 percent of your missing staff?”

Source: <http://www.itworldcanada.com/news/h1n1s-it-threats-may-not-be-taken-seriously/139420>

46. *November 25, DarkReading* – (International) **New exploit masquerades as Flash Player upgrade.** Researchers have detected a new phishing attack that promises to enhance the security of the user’s mailbox — and then downloads a malicious Trojan instead. The email requests that recipients click on a link in the body of the email to update the “security mode” of their emailboxes, according to researchers at Red Condor, an email security tool vendor. Users who click on the link are taken to a Website that advises them to update to the latest version of the Macromedia Flash Player by downloading “flashinstaller.exe.” This executable is actually a banking Trojan that is known to disable firewalls, steal sensitive financial data, and provide hackers with remote access capabilities, Red Condor says. The malware is more commonly known as Win32:Zbot-MGA (Avast), W32/Bifrost.C.gen!Eldorado (F-Prot), PWS-Zbot.gen.v (McAfee), or PWS:Win32/Zbot.gen!R (Microsoft), the researchers note. The spam campaign was detected late on November 20; within the first six hours, Red Condor says it blocked more than 500,000 email messages. So far, the company says it has stopped more than 3.5 million messages belonging to this campaign.

Source:

<http://darkreading.com/security/attacks/showArticle.jhtml?articleID=221901213&cid=ref-true>

47. *November 25, eWeek* – (International) **Symantec Web site hack exposes user data.** A hacker recently demonstrated how a SQL injection vulnerability in a Symantec Web site could be exploited to reveal user data. Symantec says the vulnerability only impacts customers in Japan and South Korea. A Web site operated by security firm Symantec was hacked — giving an attacker a sneak peak at sensitive customer data. The Romanian hacker known as Unu exploited a blind SQL injection problem to get his hands on clear-text passwords associated with customer records and other data. Unu used sqlmap and Pangolin to demonstrate the vulnerability, and published screenshots to his blog. According to Symantec, the vulnerability was on its pcd.symantec.com site, which is used to facilitate customer support for Symantec’s Norton products in Japan and South Korea. “At this time, we believe that this incident does not affect Symantec

customers anywhere else in the world,” a Symantec spokesperson said November 24. “This incident impacts customer support in Japan and South Korea but does not affect the safety and usage of Symantec’s Norton-branded consumer products. Symantec is currently in the process of ensuring that the Website is appropriately secured and will bring it back online as soon as possible.” According to Unu, his goal was not to cause harm, but to create a stir so the problem would be fixed. A Trend Micro Advanced threats Researcher said sensitive data should never be stored in clear text and bounds checking of input data can help avoid buffer overflows and SQL injection attacks. Source: <http://www.eweek.com/c/a/Security/Symantec-Website-Hack-Exposes-User-Data-639128/>

48. *November 25, IDG News Service* – (International) **Metasploit releases IE attack, but it’s unreliable.** Developers of the open-source Metasploit penetration testing toolkit have released code that can compromise Microsoft’s Internet Explorer browser, but the software is not as reliable as first thought. The code exploits an Internet Explorer bug that was disclosed recently in a proof-of-concept attack posted to the Bugtraq mailing list. That first code was unreliable, but security experts worried that someone would soon develop a better version that would be adopted by cyber-criminals. The original attack used a “heap-spray” technique to exploit the vulnerability in IE. But for a while Wednesday, it looked as though the Metasploit team had released a more reliable exploit. They used a different technique to exploit the flaw, but Metasploit eventually pulled its code. Microsoft said via e-mail Wednesday afternoon that it was “currently unaware of any attacks in the wild using the exploit code or of any customer impact.” The two versions of the browser that are vulnerable to the flaw — IE 6 and IE 7 — are used by about 40 percent of Web surfers. The flaw lies in the way IE retrieves certain Cascading Style Sheet objects, used to create a standardized layout on Web pages. Concerned IE users can upgrade their browser or disable JavaScript to avoid an attack. Source: http://www.computerworld.com/s/article/9141485/Metasploit_releases_IE_attack_but_it_s_unreliable?taxonomyId=17

49. *November 24, Forbes* – (International) **The year of the mega data breach.** According to the Identity Theft Resource Center (ITRC), government agencies and businesses reported 435 breaches as of November 17, on track to show a 50 percent drop from the number of breaches reported in 2008. That would make 2009 the first year that the number of reported data breaches has dropped since 2005, when the ITRC started counting. But the decrease in data breaches is deceptive. In fact, the number of personal records that were exposed by hackers has skyrocketed to 220 million records so far this year, compared with 35 million in 2008. That represents the largest collection of lost data on record. “Why are organizations that have these massive amounts of our data still not encrypting it?” the ITRC director says. “When we know we have these super breaches going on, why are they resisting a technology that could prevent them?” Setting aside 2009’s two “super breaches” — Heartland Payment Systems and the National Archive and Records Administration — the ITRC only recorded around 14 million lost records this year, a comparatively small number. But the chief executive of the Ponemon Institute doubts that the ITRC accounting is complete. Ponemon does not

believe the adoption of DLP and encryption is stemming the flood of personal data. He says those technologies are often implemented spottily and can not keep up with all the new places from which data can be stolen, from smart phones to Web collaboration tools. “We shouldn’t take false comfort in the idea that companies are doing a better job of this,” Ponemon says. “There’s no question that more companies are using DLP and encryption tools. But there’s always a human factor, and many people simply don’t take these technologies seriously.”

Source: <http://www.forbes.com/2009/11/24/security-hackers-data-technology-cio-network-breaches.html>

For more stories, see items [16](#) and [53](#)

Internet Alert Dashboard

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

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

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

Communications Sector

50. *November 27, Associated Press* – (Iowa) **Animal knocks out cable in eastern Iowa town.** An animal chewed through a cable line, knocking out cable and Internet service to roughly 1,000 customers in an eastern Iowa town. The disruption occurred Thursday afternoon in Bellevue, near Dubuque. Officials say service is slowly being restored to subscribers of Bellevue’s municipal cable system. One official says cable and Internet service was restored by about 8:30 p.m Thursday, but that it is taking time to get all customers back on line.

Source: <http://www.kcautv.com/Global/story.asp?S=11579874>

51. *November 25, ZDNet* – (National) **DreamHost customers hit with nightmare.** Hosting company DreamHost had trouble keeping its customer sites up and running as it migrates to a new data center. The problems began to appear on November 22 and were stretching almost into Thanksgiving. Customers reported that their sites were down for 24 hours at a clip and when there was a recovery it was not a reliable one. Among the problems are the following. DreamHost has been upgrading their shared hosting hardware. The upgrade went wrong. Customer support did not know what was going on.

Source: <http://blogs.zdnet.com/BTL/?p=27841>

52. *November 25, U.S. Environmental Protection Agency* – (National) **Verizon Wireless voluntarily discloses environmental violations.** Verizon Wireless has agreed to pay a \$468,600 civil penalty to settle self-disclosed violations of federal environmental regulations discovered at 655 facilities in 42 states. Verizon voluntarily entered into a

corporate audit agreement with the U.S. Environmental Protection Agency and conducted environmental compliance audits at more than 25,000 facilities nation-wide. The Environmental Appeals Board at EPA has approved an administrative settlement resolving violations Verizon found through its compliance audits. Verizon audited facilities that include cell towers, mobile switch centers, call centers, and administrative offices. As a result of its audit, the company reported violations of clean water, clean air, and emergency planning and preparedness regulations to EPA. Verizon promptly corrected the violations found during its audit, which included preparing and implementing spill prevention, control, and countermeasure plans, applying for appropriate air permits, and submitting reports to state and local emergency planning and response organizations informing them of the presence of hazardous substances.

Source:

<http://yosemite.epa.gov/opa/admpress.nsf/d0cf6618525a9efb85257359003fb69d/aa169813e7e6464085257679006910ef!OpenDocument>

53. *November 25, IDG News Service* – (International) **Redirecting DNS requests can harm the Internet, says ICANN.** The Internet Corporation for Assigned Names and Numbers (ICANN) on Tuesday condemned the practice of redirecting Internet users to a third-party Web site or portal when they misspell a Web address and type a domain name that does not exist. Rather than return an error message for Domain Name System requests for nonexistent domains, some DNS operators send back the IP address of another domain, a process known as NXDOMAIN substitution. The target address is often a Web portal or information site. Handling DNS requests this way has a number drawbacks that could lead to the Internet not working properly, according to ICANN. For example, users sending e-mail to a domain that does not exist should get an immediate error message. However, if the message is redirected to a site set up to handle Web traffic, it is likely to get queued and an error message will not arrive for days, ICANN said. Also, users will get longer response times if the site to which they are supposed to be redirected goes down. Redirection sites are prime targets for attacks by hackers that want to send users to their own servers. There are also privacy issues, according to ICANN. If sensitive data is redirected via a country with a different jurisdiction and local law, there could be consequences for both users and registries, it said. ICANN published its opinions and findings in a draft memo before the introduction of new generic top-level domains (gTLDs). The organization discourages the practice of redirecting requests for nonexistent domains, and suggested banning it in a draft of the agreement owners of the new gTLDs would have to sign. ICANN wants domain owners wishing to redirect DNS requests to first explain why doing so will not cause any problems.

Source:

http://www.pcworld.com/article/183135/redirecting_dns_requests_can_harm_the_internet_says_icann.html

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

Commercial Facilities Sector

54. *November 25, Associated Press* – (New Jersey) **NJ Governor Corzine seeks Presidential declaration of disaster area for Jersey Shore.** The Governor of New Jersey asked the President on November 25 to declare much of the Jersey shore a disaster area due to damage from a recent coastal storm. The Governor wrote that damages will exceed \$49 million. He said emergency funds to restore beaches, dunes and structures are needed immediately to protect lives and homes from further winter storms now that many coastal areas are unprotected. “Beach erosion is extensive,” the letter stated. “Many of the beaches along our coast have been eroded to the point they offer little protection from future storms. The damages already sustained to the beaches and dunes will render New Jersey particularly vulnerable to these weather systems until restoration is completed.” The Governor also wrote that the beaches are a crucial part of the state and local economies. Tourism is New Jersey’s second-largest industry, accounting for nearly \$39 billion a year, much of it from the shore. The storm, which lasted from November 11 to 15, caused extensive erosion in Cape May, Atlantic and Ocean counties. Roofs were blown off buildings, a key shore bridge was damaged and had to be closed when it was struck by a wayward barge, dunes were wiped out and entire communities flooded.

Source: <http://cbs3.com/local/New.Jersey.Governor.2.1334593.html>

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

National Monuments and Icons Sector

Nothing to report

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

Dams Sector

55. *November 27, KWMU 90.7 St. Louis* – (Missouri) **FEMA implements emergency plan program for Missouri dams.** The Federal Emergency Management Agency (FEMA) has launched a new program to insure that Missouri’s dams have plans in place in case of an emergency. Of the more than 450 “high-hazard potential” dams in the state, only 34 have action plans designed to notify emergency responders in an organized manner. An employee of a Kansas City-area company contracted by FEMA to encourage dam owners to implement emergency action plans stated: “For instance, in areas around St. Louis and in the Kansas City area, there are a number of dams that are suburban neighborhood-type dams, and some of them do have the plans and some of them don’t.” He says to his knowledge, none of the dams are facing any type of critical situation, but he also says most of them are getting old. He cites one dam in Kansas City built in the 1920s that does not have an emergency action plan.

Source:

<http://www.publicbroadcasting.net/kwmu/news.newsmain/article/1/0/1582599/St..Louis.Public.Radio.News/FEMA.implements.emergency.plan.program.for.Missouri.dams>

56. *November 25, SnoValley Star* – (Washington) **FEMA gives flooding help to North Bend.** North Bend neighborhoods and some Snoqualmie residents are getting a boost from the federal government to help with flooding. The Federal Emergency Management Agency (FEMA) is giving \$750,000 to raise or buy out homes in high-risk flood areas to minimize future damage in North Bend. The flood district also received two grants worth a total of about \$2.4 million to raise homes in the Snoqualmie River basin. About \$900,000 will pay to elevate six homes and buy one in the Shamrock Park neighborhood, which borders North Bend. The county submitted the project for consideration under the program to Washington state in the wake of the January 2009 floods. Unlike most rivers in Western Washington, the Snoqualmie River does not have a headwater dam to help control its flow. Improvements are being made to the South Fork levee system in North Bend. The work is part of a multiyear, \$7 million project that began in 2008 to refurbish five miles of levee system. Segments of the Middle Fork levee system are being removed to increase the river channel's capacity, which is expected to protect downstream residents. Program funds may be used to protect either public or private property, or to purchase property that has been subjected to, or is in danger of, repetitive damage, according to the acting FEMA Regional Administrator.

Source: <http://snovalleystar.com/2009/11/25/fema-gives-flooding-help-to-north-bend>

57. *November 25, Mankato Free Press* – (Minnesota) **Corps: Dam fix \$10 million.** A study on the stability of the Rapidan Dam is complete, leaving the Blue Earth County Board with a decision on whether to pay for a \$10 million fix or continue with what they hope will be relatively minor maintenance. The \$187,000 U.S. Army Corps of Engineers study estimated it would cost \$29 million to remove the county-owned dam entirely. The question boils down to risk. "How much risk are you willing to accept and how much will you pay to avoid that risk?" said a civil engineer with the Corps. The Rapidan Dam as it stands now offers "far less security than most people would accept," the engineer said. The dam does not meet Corps standards. But the Corps does not own the dam and is not telling the county what they should do with it. The trouble with the Rapidan Dam is the concrete slabs and rock extending from the base of the dam downriver. Over time, water rushing over the dam has landed with such force that it's chipped away at the highly erodible sandstone foundation. The foundation varies by location; in some places it's as porous as sand. This sort of erosion is now believed to be the cause of a concrete gap discovered beneath the dam in 2007 that prompted the emergency closure of the nearby park. The solution would be to install a new basin at the foot of the dam that dissipates the energy of the crashing water in a way that is not harmful to the dam. That is estimated to cost at least \$10 million with much of the cost coming from the difficulties in laying concrete in a river.

Source: http://www.mankatofreepress.com/local/local_story_329211637.html

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

DHS Daily Open Source Infrastructure Report Contact Information

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

Contact Information

Content and Suggestions:

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

Subscribe to the Distribution List:

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

Removal from Distribution List:

Send mail to support@govdelivery.com.

Contact DHS

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

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

Department of Homeland Security Disclaimer

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