Daily Open Source Infrastructure Report
9 February 2012

Top Stories

- A shooting suspect shot three people, killing one, at a Dallas Area Rapid Transit bus station before he was shot and killed by police. – *CNN* (See item **14**)
- Symantec confirmed February 7 the pcAnywhere source code published on the Web February 6 by hackers who tried to extort $50,000 from the company was legitimate, and said it expected the rest of the code stolen in 2006 to be made public. – *Computerworld* (See item **35**)

Fast Jump Menu

PRODUCTION INDUSTRIES

SUSTENANCE and HEALTH

SERVICE INDUSTRIES

FEDERAL and STATE

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: LOW, Cyber: LOW
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) - [http://www.esisac.com]

1. *February 8, Devner Post* – (Colorado) **Suncor begins building trench to stop flow of contaminants near Denver.** Suncor Energy crews were working on a collector trench on property owned by Metro Wastewater, trying to stop the black gunk flowing from under its refinery north of Denver from reaching Burlington Ditch, Sand Creek, and the

South Platte River, the Denver Post reported February 8. On January 23, the state health department reported liquid hydrocarbons were detected in the water table at the southwest corner of the refinery property, near its boundary with Republic Paperboard Co. This suggested that contaminants already detected on the Metro Wastewater property had begun to seep in from another direction and threatened Burlington Ditch. The health department ordered indoor air-quality monitoring at Republic Paperboard and mitigation of the new migration of the petroleum-related contamination. The trench should be completed by the end of the month. The company also is working to complete an underground clay wall at the refinery to block toxic material from leaving the Suncor property.
Source: http://www.denverpost.com/news/ci_19916057

2. *February 7, WHNS 21 Greenville* – (South Carolina) **Tanker truck flips, explodes in Anderson Co.** A tractor trailer hauling 9,000 gallons of gasoline flipped over and then burst into flames in Anderson County, South Carolina, February 7. The single-vehicle crash happened at 10:15 a.m. near the intersection of Shady Grove and Holiday Dam roads. Troopers said the driver of the tanker was traveling south on Shady Grove Road when the truck ran off the left side. They said the driver overcorrected and then the truck ran off the right side of the road, hitting a power pole and knocking down power lines, which ignited the fuel in the tanker. The Friendship fire chief said the fire was contained within 10 to 15 minutes once crews arrived. He said crews used foam solution to extinguish the fire. After the blaze was put out, Anderson County haz-mat teams worked to clean up the scene and remove about 4,000 gallons of gasoline that was left in the truck. The driver was injured and was taken to a hospital. He was charged with driving too fast for conditions.
Source: http://www.foxcarolina.com/story/16694749/hp-overturned-tanker-truck-catchs-fire-in-anderson-co

3. *February 7, WTAM 1100 Cleveland* – (Ohio) **Gas leak evacuations outside Medina are over.** A natural gas leak in Montville Township, Ohio, prompted a road closure and forced the evacuation of about 200 homes February 7. Columbia Gas of Ohio said the pipeline had been temporarily repaired and permanent repairs were scheduled for February 8. The Montville police said a company doing work in the Rustic Hills development hit a main gas line, causing the leak.
Source: http://www.wtam.com/cc-common/news/sections/newsarticle.html?feed=122520&article=9726672

For another story, see item **15**

[Return to top]

Chemical Industry Sector

4. *February 8, Associated Press* – (Ohio; Indiana) **Chemical company fined for unauthorized manufacturing.** The Justice Department said a chemical company has agreed to pay $1.4 million in civil penalties for the unauthorized manufacturing of certain substances at plants in Ohio and Indiana. Authorities said the government and

Dover Chemical Corp. entered a proposed settlement February 7. The company has agreed to stop making short-chain chlorinated paraffins, which can cause cancer and genetic and nervous system problems in humans. The company will submit other chlorinated paraffin products to the U.S. Environmental Protection Agency for review. Chlorinated paraffins are used in things such as lubricants, plastics and paints. The settlement involves plants in Dover, Ohio, and in Hammond, Indiana. It faces court approval. The Dover-based company said the settlement does not amount to an admission of liability.
Source: http://www.manufacturing.net/news/2012/02/chemical-company-fined-for-unauthorized-manufacturing

5. *February 7, KENS 5 San Antonio* – (Texas) **Train hauling hazardous materials derails in Kinney County.** A portion of US 90 between Del Rio and Bracketville in Texas was closed February 7 after a train carrying hazardous chemicals ran off the tracks. A Union Pacific spokeswoman said about 30 cars carrying pipes, pellets, lube oil, and some hazardous materials ran off the tracks. The roadway was reopened around 1:30 p.m. Officials from several agencies said no spills occurred. The Union Pacific spokeswoman said the train was traveling from Houston to California.
Source: http://www.kens5.com/news/Reports-Train-derails-in-Kinney-County-138860364.html

6. *February 6, Fierce Homeland Security* – (National) **CFATS can be fixed, DHS officials tell skeptical House Republicans.** DHS officials emphasized progress in a troubled program overseeing chemical facility safety before a skeptical audience of Republican lawmakers during a February 3 hearing. “Bad news is something we can do something about,” said the head of the DHS National Protection and Programs Directorate, while before the House Energy and Commerce Subcommittee on Environment and the Economy. He oversees at a high level the Chemical Facility Anti-Terrorism Standards (CFATS) program; an internal review conducted in late 2011 found it suffered from a lack of trained personnel, inadequate spending controls, and other problems. Another investigation in summer 2011 found CFATS program officials in May 2010 had improperly classified the risk levels of some facilities due to faulty computer modeling made with improper inputs. New risk level assessments resulted in 148 facilities being downgraded to a lower level, and 99 facilities being excluded from CFATS regulation altogether. DHS officials said CFATS had improved its performance over the past few months. From November 28 through January 28, the program office conditionally authorized site security plans at 43 Tier 1 facilities, one official said, whereas in the previous 23 months, it had conditionally authorized only 10. In prepared testimony, the head of oversight of CFATS said the program has likely resulted in more than 1,600 facilities completely removing chemicals of interest, and more than 700 other facilities reducing their holdings.
Source: http://www.fiercehomelandsecurity.com/story/cfats-can-be-fixed-dhs-officials-tell-skeptical-republicans/2012-02-06

For more stories, see items **9** and **18**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

7. *February 8, Bloomberg* – (International) **Japan to install vent system for reactors after Fukushima crisis.** Japan's power utilities plan to install vent systems with filters for nuclear reactors to reduce radioactive releases in the event of an accident, Bloomberg reported February 8. The system will cut emission of radioactive particles to less than one-thousandth of usual volumes, the Federation of Electric Power Companies, a group of 10 regional utilities, said in presentation materials at a government meeting February 7. The companies will also install equipment to remotely vent steam and gas, it said. The companies are considering details of the plan and have not yet decided when to start building the filter-equipped vent systems. Countries including Sweden and Switzerland have also installed filtered vent systems at their nuclear stations.
Source: http://www.businessweek.com/news/2012-02-08/japan-to-install-vent-system-for-reactors-after-fukushima-crisis.html

8. *February 8, Government Security News* – (National) **Study says nuclear plant designs need stepped-up attention to security.** A report by a group of nuclear scientists said there is room to enhance new reactor and plant designs. The extensive report "The Future of Nuclear Power in the United States," released February 8 by the Federation of American Scientists and Washington and Lee University, said while most safety procedures and precautions at U.S. nuclear plants are geared towards accidents, more attention must be paid to intentional attacks and sabotage. The study's senior researcher noted the terror threat to nuclear plants comes primarily in two types: ground-based armed attacks, and asymmetric attacks using brute force or cyber vulnerabilities. He also said spent fuel pools are generally not protected by a containment dome and are more vulnerable than the reactor to attacks from the ground or air. Ways to manage the spent fuel pools — such as more rapid removal of spent fuel to dry-cask storage, or, by carefully interspersing hotter and cooler spent fuel could reduce the vulnerability.
Source: http://www.gsnmagazine.com/node/25600?c=infrastructure_protection

9. *February 7, Bloomberg* – (Minnesota) **Xcel's Prairie Island nuclear plant in Minnesota vents tritium.** Xcel Energy Inc.'s Prairie Island nuclear plant in Red Wing, Minnesota, released 27 gallons of radioactive water in a leak from its condenser system, according to a filing with the Nuclear Regulatory Commission (NRC) February 7. The 27 gallons of condensate was released from a steam system overflow vent and return pumps failed to operate, causing an overflow onto the ground at the plant, February 3. Despite the incident, the plant's two reactors were operating at full power. The release contained 15,000 picocuries per liter of tritium, a low-level radioactive form of hydrogen. The Environmental Protection Agency's drinking water standard allows 20,000 picocuries per liter, according to the NRC. The leak also included methoxypropylamine, ammonia, and hydrazine, the filing showed.
Source: http://www.bloomberg.com/news/2012-02-07/xcel-s-prairie-island-nuclear-plant-in-minnesota-vents-tritium.html

[Return to top]

Critical Manufacturing Sector

10. *February 8, U.S. Department of Transportation* – (National) **NHTSA recall notice - Ford F-53 and F-59 automatic transmission selector cable.** Ford announced February 8 the recall of 13,239 model year 2011 F-53 and F-59 stripped chassis vehicles manufactured from February 1, 2010 through July 1, 2011, and from May 10, 2011 through October 25, 2011. The ‘PRNDL’ cable may break at the attachment to the transmission control selector arm assembly mounted on the steering column. If the cable breaks, the transmission gear indicator in the ‘PRNDL’ display in the instrument panel will remain in the first gear position regardless of the gear selected. An incorrect gear indication in the instrument panel may prevent the driver from knowing if they are in park or reverse, increasing the risk of a crash. Ford will notify owners, and dealers will replace the transmission selector arm assembly and the ‘PRNDL’ cable assembly. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V035000&summary=true&prod_id=1421768&PrintVersion=YES

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Banking and Finance Sector

11. *February 8, Pittsburgn Post-Gazette* – (Pennsylvania) **Police unsure why driver crashed through doors of PNC’s Firstside Center.** Police in Pittsburgh continued to search for the driver of a stolen sports utility vehicle (SUV) that crashed into a PNC Bank branch February 7, drawing a bomb squad. The man drove the vehicle onto the steps of the building and into its glass front doors about 2 p.m., police said. Witnesses said the suspect ran away, possibly darting into a nearby building. The commotion prompted police to clear and cordon off 3-block stretch for more than 2 hours while a bomb squad examined the vehicle with a robot. Bomb technicians found no explosives. Many people inside the building did not leave, but moved to rooms in the back. Police are still investigating a motive. A police commander said his detectives did not know if the crash was an accident or if the bank was targeted. The SUV was apparently stolen earlier in the day from the Parkway Center Mall in Green Tree, the commander said. Source: http://www.post-gazette.com/pg/12039/1208764-53.stm

12. *February 8, San Francisco Chronicle* – (California) **Plea deals made in Calif. mortgage scheme.** Four defendants have pleaded guilty to charges related to a mortgage loan scheme that involved at least 20 northern Californian properties and lined the defendants’ pockets with more than $20 million, federal investigators announced February 8. Through an arrangement with two real estate agents that lasted

from 2002 to 2007, a couple secured 63 loans on properties purchased through straw buyers, court documents said. The couple also admitted to owning and operating numerous residential care facilities that employed illegal immigrants. The California Department of Social Services barred the couple from operating care facilities in 1998 because of licensing violations, but the couple continued to operate the facilities by using buyers paid to purchase the properties and then sign grant deeds that transferred title to the wife, court documents said. The couple pleaded guilty to charges of bank fraud, tax evasion, and harboring illegal aliens, and are responsible for $5.2 million in restitution. A real estate agent, who pleaded guilty to charges of bank fraud and monetary transactions using criminally derived property, is responsible for $2.8 million of that sum. Prosecutors said the other agent will have to pay about $300,000. The maximum sentence for bank fraud is 30 years in prison and a $1 million fine.
Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2012/02/08/BAEV1N4AJM.DTL

13. *February 7, Detroit Free Press* – (Michigan; International) **Man held on Ponzi scheme charges.** An Iraqi citizen and former Dearborn, Michigan resident is in custody on federal charges he operated a Ponzi scheme that allegedly bilked investors, mostly Iraqi-Americans, out of $58 million, the U.S. attorney's office said February 6. Authorities said the man promised big returns on rebuilding projects in Iraq, but instead used investors' money to repay earlier investors. He fled to the Middle East after investors discovered the scheme. More than 100 sued him in federal court in Detroit in 2010. The U.S. attorney's office said he was arrested at Detroit Metro Airport February 3.
Source: http://www.freep.com/article/20120207/NEWS04/202070344/Man-held-on-Ponzi-scheme-charges

For another story, see item **33**

[Return to top]

Transportation Sector

14. *February 8, CNN* – (Texas) **Suspect, victim die in Texas transit shooting.** A shooting suspect and one of three people he shot at a Dallas Area Rapid Transit (DART) station just north of Dallas have died of their wounds, officials said. The shootings happened February 7 at the Arapaho station in Richardson, Texas, a DART spokesman said. "A DART female officer had been alerted by a bus operator about an issue with a customer, so she went to the station to meet the bus," he said. "Meanwhile, a second bus pulled into the station and that operator also indicated they had someone attempting to board the bus that was being unruly. The suspect got off the bus and started walking towards the train station. When our officer approached him, he started firing." The DART officer received non-life threatening gunshots to her bulletproof vest and her arm. Two male passengers also were shot. One later died. A Richardson police spokesman said during a news conference that it was unclear if the victims were hit by crossfire or were targeted by the gunman. Several dozen people were evacuated from the DART station.

Source: http://www.cnn.com/2012/02/07/us/texas-transit-shootings/index.html?hpt=us_c2

15. *February 7, Associated Press* – (Tennessee) **Small derailment causes propane scare.** A minor train derailment caused operations to be temporarily shut down at a Chattanooga, Tennessee railroad yard. Three empty Norfolk Southern rail cars came off a track at the DeButts Yard February 7 and one of them landed on a propane tank. A Chattanooga Fire Department (CFD) spokesman said in a news release that tank was righted at 9:30 a.m. and the propane was being pumped into another container. The CFD Tactical Services chief said heavy equipment used to right rail cars was used to lift the car so technicians could get to the propane tank.
    Source: http://www.wrcbtv.com/story/16695238/small-derailment-causes-propane-scare

16. *February 6, Associated Press* – (National) **Congress passes bill to speed air traffic control switch to GPS, open skies to drone aircraft.** A bill to speed the nation's switch from radar to an air traffic control system based on GPS technology, and to open U.S. skies to unmanned drone flights within 4 years, received final Congressional approval February 6. The bill, which has been sent to the U.S. President for his signature, authorizes $63.4 billion for the Federal Aviation Administration (FAA) over 4 years, including about $11 billion toward the air traffic system and its modernization. It accelerates the modernization program by setting a deadline of June 2015 for the FAA to develop new arrival procedures at the nation's 35 busiest airports so planes can land using the more-precise GPS navigation.
    Source: http://www.washingtonpost.com/business/technology/senate-passes-faa-bill-that-speeds-switch-to-gps-opens-us-skies-to-unmanned-aircraft/2012/02/06/gIQAvU7vuQ_story.html

For more stories, see items **2** and **5**

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

17. *February 8, Food Safety News* – (Nebraska; North Carolina; South Carolina) **Another recall of salad with hard-cooked eggs.** In another recall related to hard-cooked eggs that may be contaminated with Listeria, Bost Distributing Company of Bear Creek, North Carolina, doing business as Harold Food Company, is withdrawing about 1,200 pounds of chicken salad products, Food Safety News reported February 8. The recall is one of many resulting from a recall by Minnesota-based Michael Foods, which produced the cooked eggs at its Wakefield, Nebraska facility. There have been no

confirmed reports of illnesses associated with the eggs. The products were sent to a distributor in South Carolina for further distribution to retail establishments in North Carolina and South Carolina. The chicken salad products may have been repackaged as sandwiches under a brand other than Harold Food Co. and may no longer bear the original identifying information.
Source: http://www.foodsafetynews.com/2012/02/another-recall-of-salad-with-hard-cooked-eggs/

18. *February 8, KUSA 9 Denver* – (Colorado) **10 homes evacuated in Walsh after tank rupture.** Ten houses in a small southeastern Colorado town were evacuated following an ammonia spill. A Baca County Emergency Management official said the small sealed tank of anhydrous ammonia, which is used as a fertilizer, fell off a grain truck and ruptured February 8 in the town of Walsh. Within a few hours, the tank was empty except for some vapors. A Colorado State Trooper said the tank fell off a vehicle when the vehicle's axle broke and one end of the vehicle fell. The fall broke the tank's valve. He said he thought the tank had a capacity of about 500 gallons. A hazardous material team was on its way to Walsh, home to about 700 people.
Source: http://www.9news.com/news/article/247877/222/Truck-rolls-leaking-chemicals-evacuation-ordered

19. *February 7, Wired* – (International) **Fast-spreading animal virus leaps Europe, UK borders.** A newly identified disease is moving rapidly through livestock in Europe and has authorities worried and puzzled, Wired reported February 7. The disease, dubbed Schmallenberg virus for a town in west-central Germany where one of the first outbreaks occurred, makes adult animals only mildly ill, but causes lambs, kids, and calves to be born dead or deformed. The United Kingdom's Animal Health and Veterinary Laboratories Agency (AVHLA) said February 7 the virus has been found on 29 farms in England; in the past few weeks they found it in sheep, but announced hey have identified it in cattle as well. In mainland Europe, it has been identified on several hundred farms in the Netherlands, Germany, Belgium, and France. The European Center for Disease Prevention and Control said the new virus's closest relatives do not cause disease in humans — but that other more distantly related viruses do. The viral vector is believed to be midges and mosquitoes. The disease does not pass from adult animal to another animal, but apparently does from a mother animal to offspring in utero, and that is why it is showing up now: It is lambing season. With Europe enduring its coldest winter in decades, there are no virus-carrying insects flying around now. Instead, the animals giving birth to deformed and dead offspring were infected last summer and fall. No one has been able to say so far whether the organism can survive in insects over the winter. Agricultural media are starting to record the economic fallout, including a Russian ban on European livestock, and the possibility of a ban on shipping live animals and sales.
Source: http://www.wired.com/wiredscience/2012/02/schmallenberg-virus/

20. *February 7, Washington Post* – (Maryland) **Fire damages Silver Spring grocery store.** A fire caused significant damage late February 7 at a grocery store and forced the evacuations of at least two stores at a Silver Spring, Maryland shopping center, Montgomery County fire officials said. The blaze broke out in an aisle in the middle of

the store, said a fire department spokesman. The store's sprinkler system kept the fire in check and it took firefighters about 10 minutes to extinguish it, he said. Authorities evacuated the store and a Kohl's nearby. The cause of the fire is under investigation. The store will remain closed as fire and health inspectors evaluate the damage, and if food can be handled safely in the store due to the damage.
Source: http://www.washingtonpost.com/blogs/crime-scene/post/fire-damages-silver-spring-grocery-store/2012/02/07/gIQAVFQexQ_blog.html

[Return to top]

Water Sector

21. *February 7, Santa Cruz Sentinel* – (California) **Santa Cruz County offers grants to seal old wells.** Santa Cruz County, California, water officials estimate there are 1,000 unused wells, ranging from dozens to hundreds of feet deep, tucked into backyards and agricultural fields throughout the county. The abandoned wells pose a risk to groundwater, officials said. The county is now encouraging landowners with wells on their property to come forward, offering more than $300,000 in state grants to seal them and ensure they do not turn into environmental hazards. "They become conduits, or straws, which draw down potentially hazardous materials in to the groundwater," said a county land use program manager. County officials suspect most of the wells are located in previously rural areas that are now connected to municipal water, including Live Oak and Scotts Valley. The county's groundwater has long been the source of concern, from agricultural activities in South County to growth that has taxed local aquifers. Eighty percent of the county's potable water comes from those aquifers, and the encroachment of seawater is an escalating concern.
Source: http://www.santacruzsentinel.com/localnews/ci_19914582

For more stories, see items **1** and **9**

[Return to top]

Public Health and Healthcare Sector

22. *February 7, WSAZ 3 Huntington* – (West Virginia) **Man threatens medical staff with gun.** A man was arrested February 7 after deputies said he walked into the Prestera Center, a facility that offers mental health and addiction services, outside of Huntington, West Virginia, pointed a gun at the staff, and threatened to start shooting if he did not receive drugs. Deputies said the weapon used was a BB gun and did not have the CO2 cartridge needed to actually fire a BB. They believe the gun was used more to strike fear in others and posed no real threat. Deputies said the man was passed out in the lobby when they arrived on the scene with the gun in his hand inside a jacket pocket. He is charged with attempted armed robbery and attempting to commit robbery by using the threat of deadly force.
Source: http://www.wsaz.com/news/headlines/138851489.html

23. *February 7, Fox News* – (National) **Lyme disease high-risk areas revealed in new map.** An extensive field study has identified areas of the United States where people have the highest risk of contracting Lyme disease, according to the Centers for Disease Control and Prevention. The study found that high infection risk is mainly confined to the Northeast, Mid-Atlantic and Upper Midwest regions. To collect data for the study, scientists studied 304 sites from Maine to Florida, and across the Midwest, between 2004 and 2007. At each location, "tick hunters" combed for Lyme disease-carrying ticks called black-legged ticks. The findings showed a heightened risk of Lyme disease in large parts of the Northeast, from Maine going as far south as Maryland and northern Virginia. The researchers also identified a separate and distinct Lyme disease risk region in the upper Midwest that includes most of Wisconsin, a large area in northern Minnesota, and a sliver of northern Illinois. The researchers noted the study did not examine risk in the West, where Lyme disease is believed to be confined to areas along the Pacific Coast, and where a different tick species, known as the western black-legged tick, carries the bacteria. The South was rated as having a low infection risk, according to the survey findings. The study is published in the February issue of the American Journal of Tropical Medicine and Hygiene.
Source: http://www.foxnews.com/health/2012/02/07/lyme-disease-high-risk-areas-revealed-in-new-map/

For more stories, see items **12** and **39**

[Return to top]

Government Facilities Sector

24. *February 7, Nextgov* – (International) **Pentagon IG's Website outage blamed on technical problems.** The Pentagon inspector general's (IG) Web site has been inaccessible for days because of technical difficulties within the agency, IG officials said February 7. "Due solely to internal factors, the [Department of Defense] IG Internet Web page has been unavailable over the past several days," a IG spokeswoman said. "The Web page should be available in the near future."
Source: http://www.nextgov.com/nextgov/ng_20120207_1527.php

25. *February 7, Reuters* – (California) **Anonymous targets Oakland officials over handling of Occupy.** The hacker group Anonymous released personal information of officials in Oakland, California, in a leak it said was in retaliation for the city's treatment of Occupy protesters, and officials February 7 decried the move as despicable. The hacker group released the home addresses, phone numbers, and names of relatives of Oakland's top elected officials the week of January 30, accompanied by a statement that they were "shocked and disgusted" by the treatment of protestors. In a press conference February 7, city officials pushed back against the leak. Oakland has been a flashpoint for the national "Occupy" protests against economic inequality that began in 2011 in New York's financial district and spread to dozens of cities.
Source: http://www.chicagotribune.com/news/sns-rt-us-anonymous-oaklandtre8170b3-20120207,0,983012.story

For more stories, see items **28** and **39**

[Return to top]

Emergency Services Sector

26. *February 8, Associated Press; Charleston Gazette* – (West Virginia) **Hackers post W.Va. police officers' personal info.** Hackers affiliated with the Anonymous hacking group obtained more than 150 police officers' personal information from an old Web site for the West Virginia Chiefs of Police Association and posted it online, the Associated Press reported February 8. The association's president told the Charleston Gazette the FBI is investigating. He said a group called CabinCr3w hacked the site February 6 and obtained the home addresses, home phone numbers, and cellphone numbers of current and retired police chiefs. The association has a new Web site, but members' information was stored on the old Web site's database. In an online message by CabinCr3w addressed to "citizens of West Virginia," the group said it has been monitoring cases of police brutality. The chief said CabinCr3W is affiliated with the hacking collective Anonymous, and CabinCr3w's Twitter page is laced with references to the larger hacking group.
Source: http://www.google.com/hostednews/ap/article/ALeqM5il-cj-qXoaurp-tJkbwnw9KgdZgg?docId=be8ecbfc75a34ebda134078c9aa847bc

27. *February 7, Computerworld* – (National) **FBI declares cloud vendors must meet CJIS security rules.** The FBI February 7 reaffirmed its rule that all cloud products sold to to U.S. law enforcement agencies must comply with the FBI's Criminal Justice Information Systems (CJIS) security requirements. While the nation's top law enforcement agency conceded some vendors may have a tough time meeting those rules, it insisted there would be no compromising on security. The CJIS database, maintained by the FBI, is one of the world's largest repositories of criminal history records and fingerprints. The records are available to law enforcement agencies and contractors around the country that comply with the security rules, which include requirements that all data, both in transit and at rest, be encrypted and that anyone who accesses the database pass FBI background checks. A spokesman for the FBI's CJIS division February 7 maintained the CJIS security requirements are compatible with cloud computing.
Source:
http://www.computerworld.com/s/article/9224048/FBI_declares_cloud_vendors_must_meet_CJIS_security_rules?taxonomyId=17

28. *February 7, Lawrenceville Patch* – (New Jersey) **Suspicious powder evacuates Lawrence police station.** A suspicious white powder prompted authorities to order a precautionary evacuation of the Lawrence Township, New Jersey police and court facility February 7. All civilians and nonessential personnel were kept out of the building for almost an hour until hazardous materials personnel from the Trenton Fire Department confirmed the substance was a nonhazardous starch, according to a police department spokesman. The white powder was packed into a spent shotgun shell mailed to a Lawrence Township resident, he said. The 39-year-old man told police he

believes the doctored shotgun shell was sent to him by a former employer who, the man alleged, has been harassing him for some time. He went to the township police station to show police the shotgun shell and other harassing materials he had received, the spokesman said. Those who came in contact with the shell were quarantined inside the building. The building was reopened to the public and normal activity resumed soon after testing by the haz-mat team showed the powder was harmless.
Source: http://lawrenceville.patch.com/articles/suspicious-powder-prompts-evacuation-of-police-station

29. *February 6, Associated Press* – (New York; New Jersey) **NYPD officer pleads guilty in gun smuggling case.** A Brooklyn, New York police officer pleaded guilty February 6 to conspiracy charges, admitting his central role in a smuggling case that involved guns, cigarettes, and slot machines. The officer could face roughly 5 to 6 years in prison at a June 15 sentencing. He was the first among a dozen individuals to enter a plea that negates the need for a trial in the case built over the past 2 years. Others charged include three retired New York City Police Department officers, and a New Jersey corrections officer. The officer's lawyer said he had a sterling record with the police department for nearly 18 years before he met a federal cooperator who recommended a plan to transport cigarettes bought at Indian reservations into New York. He said the FBI developed a sting operation that led to the transport of supposedly stolen slot machines from Atlantic City and weapons from New Jersey across state lines into New York. Authorities said the FBI from September 2010 to last October supplied the officer and others with items that carried a street value of about $1 million. They included three M-16 rifles, a shotgun, 16 handguns, 12 slot machines, and thousands of cartons of cigarettes, along with counterfeit merchandise. The defendants were paid about $100,000 during the scheme, authorities said.
Source:
http://www.boston.com/news/nation/articles/2012/02/06/nypd_officer_pleads_guilty_in_gun_smuggling_case/

For another story, see item **14**

[Return to top]

Information Technology Sector

30. *February 8, Help Net Security* – (International) **More bogus ad-serving Android apps evade Google's Bouncer.** Users searching for games on the official Android Market have been heavily targeted by ad-pushing scammers lately. First it was the fake Temple Run app, and now a string of bogus copies of popular iPhone games supposedly developed by Rovio Mobile Ltd, the developers of the famous Angry Birds game. Some of these games are offered by other developers — mostly on Apple's iPhone Apps Store — and some do not even exist, but the scammers are trying to take advantage of the fact Angry Birds' developer Rovio has become a well known and trusted name. The scammers were able to register their account under Rovio Mobile by using a capital "I" instead of a lowercase "L" in "Mobile," and the result is a legitimate looking account. Once the user tries to install any of the apps, she is faced with an

image taken from the original app and instructions to follow a link to complete the process and to unlock the "full version." However, the link leads to a Web page hosting advertisements for diet pills, and entices the users to sign in to find out how they can get three bottles of pills for free.
Source: http://www.net-security.org/secworld.php?id=12367

31. *February 8, Softpedia* – (International) **Malware steals documents and uploads them to Sendspace.** Security experts came across a piece of malware programmed to steal documents from the infected computer. The malicious element is designed to upload the obtained Microsoft Word and Excel files to the hosting site sendspace.com Trend Micro researchers said Sendspace was used previously to store stolen data because the service allowed crooks to "send, receive, track and share" big files, but the process was never done automatically by malware. The infection begins with an executable file called Fedex_Invoice(dot)exe, identified as TROJ_DOFOIL.GE, the file's name hinting it may be spread with the use of a fake "FedEx failed delivery" spam campaign. Once the file is executed, it downloads and executes TSPY_SPCESEND.A, a trojan that searches the local drive for Word and Excel documents, collecting them in a password-protected archive placed in the user's temporary folder. After the archive is created, it is uploaded to Sendspace, its download link transmitted to the malware's command and control (C&C) server. This way the crooks do not have to store all the files on the C&C, instead they access them from the file hosting service. This discovery means information theft and exfiltration are not specific only for targeted attacks, but they are present in mass campaigns as well.
Source: http://news.softpedia.com/news/Malware-Steals-Documents-and-Uploads-Them-to-Sendspace-251430.shtml

32. *February 8, Threatpost* – (International) **Attackers using fake Google Analytics code to redirect users to Black Hole Exploit Kit.** Injecting malicious code into the HTML used on legitimate Web sites is a key part of the infection lifecycle for many attack crews, and they often disguise and obfuscate their code to make it more difficult to analyze, or so it appears, legitimate code. The latest instance of this technique has seen attackers employing code meant to look like Google Analytics snippets, but instead sends victims off to a remote site hosting the Black Hole Exploit Kit. Researchers at Websense discovered the ongoing attack recently, and found the code being used to hide the fake Google Analytics tags is heavily obfuscated, making analysis quite difficult. The malicious code, which is being injected into benign pages on legitimate sites, is designed to look just like actual Google Analytics code and to appear as though it is referring to common domains.
Source: http://threatpost.com/en_us/blogs/attackers-using-fake-google-analytics-code-redirect-users-black-hole-exploit-kit-020812

33. *February 8, Softpedia* – (International) **Blackhole toolkit served by spam ahead of tax season.** Symantec researchers came across a large number of spam messages that try to trick the recipient into clicking on a link that points to the Blackhole toolkit. More than 200 unique URLs were identified in a series of e-mails that urge users to verify their accounts after some discrepancies were identified by the sender company. The phony e-mails, apparently coming from a legitimate company, read: "With intent

to assure that the exact information is being sustained on our systems, as well as to improve the quality of service we can provide to you; [COMPANY NAME] has participated in the Internal Revenue Service [IRS] Name and TIN Matching Program. We have found out, that your name and/or TIN, that we have on your account is different from the information on file with the Social Security Administration. In order to verify your account, please enter the secure section." Once the link is clicked, the user is taken to a page containing more links that point to a JavaScript file called js.js. This file serves the Blackhole toolkit looking for various vulnerabilities on the victim's computer, the final payload being identified as Trojan.Zbot. The domains that contain the malicious JavaScript file are not only newly registered domains, but also legitimate domains that were hijacked by the cybercriminals that launched the campaign. Users are advised not to click on links that come with a suspicious looking e-mail, but also to avoid opening attachments, especially if they are represented by exe, zip, or pdf files.
Source: http://news.softpedia.com/news/Blackhole-Toolkit-Served-by-Spam-Ahead-of-Tax-Season-251438.shtml

34. *February 7, Computerworld* – (International) **Adobe sets IE as next target in Flash security work.** Adobe plans to tackle Microsoft's Internet Explorer (IE) in its ongoing work to "sandbox" its popular Flash Player within browsers, Adobe's head of security said February 7. On February 6, Adobe released a beta version of a sandboxed Flash Player plug-in for Mozilla's Firefox on Windows Vista and Windows 7 as a follow-up to a similar initiative in 2010 for Google's Chrome. Next on the list is IE. "IE has a big chunk of the user base," said Adobe's senior director of security, products, and services. "We want to do what protects the most users the fastest." According to Web metrics company Net Applications, IE accounted for 53 percent of all browsers used last in January worldwide, or more than double Firefox's 21 percent, and almost triple Chrome's 19 percent. Adobe's head of security declined to set a timetable for putting Flash within a sandbox inside IE.
Source:
http://www.computerworld.com/s/article/9224047/Adobe_sets_IE_as_next_target_in_Flash_security_work?taxonomyId=17

35. *February 7, Computerworld* – (International) **Symantec expects Anonymous to publish more stolen source code.** On February 7, Symantec confirmed the pcAnywhere source code published on the Web February 6 by hackers who tried to extort $50,000 from the company was legitimate. A company spokesman also said Symantec expects the rest of the source code stolen from its network in 2006 will also be made public. Symantec's acknowledgement followed the appearance late February 6 of a 1.3GB file on various file-sharing Web sites that claimed to be the source code of the pcAnywhere remote-access software. The Anonymous hacking group claimed responsibility for posting the pcAnywhere source code. Also February 6, an individual or group going by the name "Yama Tough" published a series of e-mails on Pastebin that detailed an attempt to extort $50,000 from Symantec.
Source:
http://www.computerworld.com/s/article/9224039/Symantec_expects_Anonymous_to_publish_more_stolen_source_code?taxonomyId=17

36. *February 7, H Security* – (International) **Trustwave issued a man-in-the-middle certificate.** Certificate authority Trustwave issued a certificate to a company allowing it to issue valid certificates for any server. This enabled the company to listen in on encrypted traffic sent and received by its staff using services such as Google and Hotmail. Trustwave has since revoked the CA certificate and vowed to refrain from issuing such certificates in the future. According to Trustwave, the CA certificate was used in a data loss prevention (DLP) system, intended to prevent confidential information such as company secrets from escaping. The DLP system monitored encrypted connections by acting as a man-in-the-middle, meaning it tapped into the connection and fooled the browser or e-mail client into thinking it was communicating with the intended server. To prevent certificate errors, the DLP system had to be able to produce a valid certificate for each connection — the Trustwave CA certificate enabled it to issue such certificates itself.
Source: http://www.h-online.com/security/news/item/Trustwave-issued-a-man-in-the-middle-certificate-1429982.html

For more stories, see items **24**, **25**, **26**, and **27**

Internet Alert Dashboard

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

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

[Return to top]

Communications Sector

See items **30** and **36**

[Return to top]

Commercial Facilities Sector

37. *February 8, Associated Press* – (South Dakota) **Tenant has minor injuries in SD apartment blast.** No one was seriously hurt in a Sioux Falls, South Dakota apartment explosion, the Associated Press reported February 8. The blast that produced heavy smoke and triggered the building's sprinkler system prompted the evacuation of the downtown apartment building late February 7. Police said a tenant in the third-floor apartment where the blast occurred told authorities he was cooking french fries at the time. The tenant suffered minor injuries. Damage to the building was not immediately determined.
Source:
http://www.wausaudailyherald.com/usatoday/article/38527151?odyssey=mod|newswell|text|FRONTPAGE|s

38. *February 8, WLNE 6 Providence* – (Rhode Island) **Search on in Johnston for arsonist after apartment fire.** The search is on for an arsonist in Johnston, Rhode Island, after a fire at an apartment complex early February 7. One person was hurt and another 18 people were displaced. Flames burned through the roof of the three-story apartment building just after 4 a.m. "We believe that it did originate outside the building," said the assistant fire chief. While a Johnston police officer suffered smoke inhalation, no one else was hurt.
    Source: http://www.abc6.com/story/16739061/search-on-in-johnston-for-arsonist-after-apartment-fire

39. *February 8, Associated Press* – (Washington) **Many report illness at Washington cheerleading event.** Washington State health officials said February 7 they are investigating reports of intestinal illness affecting at least 19 squads that participated in a weekend state cheerleading tournament at Comcast Arena in Everett, Washington. Reported symptoms include vomiting and diarrhea. KOMO 4 Seattle reported several people were hospitalized but their conditions were unknown. The Washington Interscholastic Activities Association hosted the competition. More than 3,000 people attended, and more than 1,000 people in 52 squads competed in cheerleading, dance and drill events, the group said. The first symptoms developed February 5 and 6, the health department said. State health officials were working with the Snohomish Health District and the association to determine the cause of the illnesses. Surveys were being sent to participants and samples were being collected. There have been reports of students suffering symptoms at Puget Sound-area high schools including Marysville, Ballard, Juanita, Mount Si, and Skyline, KOMO 4 reported. Students from Pierce and Kitsap counties may also have become ill, a Snohomish Health District spokeswoman told The Daily Herald of Everett.
    Source: http://www.suntimes.com/news/nation/10507899-418/many-report-illness-at-washington-cheerleading-event.html

For more stories, see items **3**, **11**, and **20**

[Return to top]

National Monuments and Icons Sector

40. *February 4, KTVU 2 Oakland* – (California) **Copper wire thieves target state parks.** Copper wire thieves are narrowing in on state parks, KTVU 2 Oakland reported February 4. A California state park ranger said thieves damaged one area of a state park in Benicia by digging a hole to rip out buried copper wires. A bathroom at Dillon's Point was left with no electricity because of the vandals. A ranger who patrols the grounds said that in less than a year, thieves have caused $30,000 worth of damage. State park officials have contacted recycling centers and asked them to keep an eye out for the stolen copper.
    Source: http://www.ktvu.com/news/news/copper-wire-thieves-target-state-parks/nHTjx/

[Return to top]

Dams Sector

41. *February 8, Dredging Today* – (Oregon) **Corps awards contract for Bonneville Spillway rock removal.** The U.S. Army Corps of Engineers awarded a contract February 6 to remove large rocks from the base of the spillway at Bonneville Lock and Dam near Portland, Oregon. After the record-breaking water flows at the Corps' Columbia River dams in 2011, engineers found large amounts of rock had accumulated below Bonneville's spillway gates, placed there by the force of the water. The rock moves around during spill operations, which means the large stones can damage the concrete structure below the spillway. The contractor will have rock removal equipment on a barge and will use divers to assist with the underwater work to remove the rocks. The work must be done by March 31 to ensure the Corps is ready to begin spilling water for juvenile fish migration in April.
Source: http://www.dredgingtoday.com/2012/02/08/corps-awards-contract-for-bonneville-spillway-rock-removal-usa/

42. *February 7, Silverton Appeal Tribune* – (Oregon) **Engineers report on dam safety.** The engineering and construction firm that built Silver Creek Dam about 2 miles southeast of Silverton, Oregon, said three out of four previously identified ways the dam could fail are not a threat, the Silverton Statesman Journal reported February 7. In the spring of 2011, the U.S. Army Corps of Engineers completed a "potential failure modes analysis" — an investigation into all the ways the dam could fail. The study was done in preparation for an early-warning and monitoring system that was originally slated for installation this summer. The Corps identified four potential credible failure modes that included spillway jacking; downstream sill and stilling basin scour; upstream scour of spillway sill; and overtopping. Of the four, overtopping is considered to be the only remaining way for the dam to fail. The other three modes are directly related to the spillway. Water was flowing over the spillway when the Corps conducted its inspection. "It was difficult for them to get down and really ascertain what kind of condition the spillway and stilling basin were in," Corps officials said. During a September site visit, the water level at the reservoir had been drawn down, and city staff pumped water out of the basin to provide a clear look at the spillway. The Silverton public works director said the city inspects the dam every 6 months and and collects drain samples quarterly to check for turbidity. It is considered a high-hazard dam because of its proximity to Silverton; if it failed, the consequences would be severe.
Source:
http://www.statesmanjournal.com/article/20120208/COMMUNITIES/202080356/Engineers-report-dam-safety?odyssey=mod|newswell|text||p

[Return to top]

NTAS
National Terrorism Advisory System
NO ACTIVE ALERTS
www.DHS.gov/alerts

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

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

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703)387-2267
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.