Daily Open Source Infrastructure Report
1 March 2012

Top Stories

- In what is being called the largest healthcare fraud case in U.S. history, federal law enforcement officials indicted a Dallas-area physician for allegedly bilking Medicare out of nearly $375 million. – *Los Angeles Times* (See item **24**)
- A U.S. company posted hacking techniques for disabling programmable logic controllers (PLCs) that manage industrial machinery of four energy and manufacturing firms. – *Yomiuri Shimbun* (See item **31**)
- At least nine people were killed and hundreds were injured February 28 and 29 as a line of tornadoes moved across the Midwest, damaging dozens of businesses and apartment buildings. – *Associated Press; MSNBC; NBC News* (See item **39**)

Fast Jump Menu

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 29, Framingham MetroWest Daily News* – (Massachusetts) **Tanker crash and fuel spill closes Rte. 30 in Weston.** An oil tanker rolled onto its side on Rte. 30 in Weston, Massachusetts, February 29, shutting down traffic in both directions, police said. The multi-car crash occurred near the intersection of Pine Street, Weston police said. The town's dispatcher said six officers rushed to the scene. Two engines, a ladder truck and an ambulance also responded, according to the Weston Fire Department. It was not clear how much, if any, fuel spilled.
Source: http://www.metrowestdailynews.com/features/x1640255095/Tanker-crash-and-fuel-spill-in-Weston

2. *February 28, MarketWatch* – (Pennsylvania) **Chevron reports oil spill in Marcellus Shale: Pa.** Chevron Corp. has reported to state regulators that a small oil condensate spill occurred late 2011 at a company's Marcellus Shale well site was greater than anticipated, the Pennsylvania Department of Environmental Protection (DEP) said February 28. On December 20, Chevron reported to regulators that it had discovered a leak from a pipe joint weld buried 4 feet under the well pad in Robinson, Washington County. Initially, the broken pipe was estimated to have spilled 2 barrels of oil condensate, but Chevron reported to regulators by the end of December the spill was greater than anticipated, said the DEP's community relations coordinator. "As of today they believe as much of 80 barrels of condensate were lost between November 8, when they began their fracking operation, and December 18, when they discovered the break in the pipe," he said. The firm is working to determine the extent of contamination of soil at the site, and the DEP has collected soil and water samples, he said.
Source: http://www.marketwatch.com/story/chevron-reports-oil-spill-in-marcellus-shale-pa-2012-02-28

For more stories, see items **31**, **39**,

[Return to top]

Chemical Industry Sector

3. *February 28, U.S. Environmental Protection Agency* – (Oregon) **Oregon lumber mill cited for toxic chemical leaks and violations.** Sanders Wood Products Company in Liberal, Oregon, was found to have a series of polychlorinated biphenyl (PCB) leaks and other violations of federal PCB laws at its lumber mill, according to a settlement reached with the U.S. Environmental Protection Agency (EPA), the agency announced February 28. The company will pay over $108,000 in penalties. During a 2009 inspection, an EPA inspector identified leaks in three PCB-containing transformers. Federal law requires repair, containment, or replacement of leaking transformers containing PCBs. In addition, the transformers were not properly maintained and lacked necessary labels. PCBs are known carcinogens that can harm the immune, reproductive, nervous, and endocrine systems. As part of the settlement, the company confirmed it has removed the leaking transformers from the facility. The areas where the PCBs leaked have also been cleaned up. The company has also certified it is currently in compliance with all applicable requirements under the Toxic Substances Control Act at each of its facilities.

Source: http://yosemite.epa.gov/opa/admpress.nsf/0/68CFF14AAAF2AF0B852579B2006CD60C

For more stories, see items **20** and **22**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

4. *February 29, DeKalb Daily Chronicle* – (Illinois) **Insulator failure to blame for latest Byron plant shutdown.** For the second time in a month, a power interruption caused operators at the Byron Generating Station in Ogle County, Illinois, to declare an "unusual event," officials said in a news release. A failed insulator in the station's switchyard is believed to have caused loss of power to Unit 1 February 28, the release said. One of the station's many redundant power sources kicked in and both of the plant's units were operating at 100 percent power, it said. The insulator was being replaced; the work may continue into February 29, the release said, adding that the facility was "in a safe condition."
Source: http://www.daily-chronicle.com/2012/02/29/insulator-failure-to-blame-for-latest-byron-plant-shutdown/a14z4bq/

5. *February 28, Power Engineering* – (Ohio) **Cracks at nuclear plant caused by 1978 blizzard, report says.** Cracks found in the containment building wall of the Davis-Besse nuclear power plant in Oak Harbor, Ohio, was caused by lack of an exterior weatherproof coating on the shield building, according to a report from plant owner FirstEnergy Nuclear Operating Co. (FENOC), Power Engineering reported February 28. FENOC said in its Root Cause Analysis Report that moisture associated with the blizzard of January 1978 migrated into the concrete, froze, and expanded, causing the tight, subsurface cracks in the containment building. The cracks were found during a reactor head replacement outage in the fall of 2011. The report said the cracking occurred following the blizzard's combination of extreme weather conditions, which included 3 days of driving rain before a drastic temperature drop and intense winds. The report also concluded the structural integrity of the shield building remains intact, and the building is able to perform its safety function. FENOC will apply a weatherproof coating to protect exterior walls, perform additional inspections to verify the cracks have not spread, and develop a long-term building monitoring plan.
Source: http://www.power-eng.com/articles/2012/02/cracks-at-nuclear-plant-caused-by-1978-blizzard-report-says.html

[Return to top]

Critical Manufacturing Sector

6. *February 28, U.S. Department of Labor* – (Florida) **Florida aluminum fabricator cited by U.S. Labor Department's OSHA for combustible dust and other hazards; proposed penalties total nearly $140,000.** Fritz Aluminum Services Inc. was cited by

the U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) February 28 for 37 violations for exposing workers to a variety of safety and health hazards, including combustible dust accumulations, at the company's Eustis, Florida facility. The OSHA opened an inspection in September 2011 after receiving a complaint. Three willful violations involved failing to provide workers with an abrasive blasting suit or apron during sandblasting operations, replace missing and clogged filters in the powder coating booth, and implement a housekeeping program and provide proper ventilation to keep combustible dust accumulations at a minimal level. Twenty-eight serious violations were also cited.
Source: http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=21891

7. *February 28, U.S. Department of Labor* – (Wisconsin) **U.S. Department of Labor's OSHA cites Yaskawa America in Oak Creek, Wis., after worker suffers burns from electrical shock at manufacturing plant.** The U.S. Department of Labor's Occupational Safety and Health Administration February 28 cited Yaskawa America Inc. with six safety — including one willful — violations, after a worker suffered burns from an electrical shock September 15, 2011 at the company's Oak Creek, Wisconsin manufacturing facility. The Waukegan, Illinois-based company produces drives and motion control components for heating, ventilation, and air conditioning systems. The worker suffered second- and third-degree burns on his hand after receiving an electrical shock from exposed parts that had the potential to be energized to 480 volts. The willful violation was allowing the worker to come in contact with exposed energized parts on testing equipment. Additionally, three serious safety violations include using unapproved electrical equipment, failing to provide personal protective equipment to employees working on energized parts, and failing to implement electrical safe work practices.
Source: http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=21897

8. *February 28, U.S. Consumer Product Safety Commission; Health Canada* – (National; International) **American Honda recalls trimmers due to laceration hazard.** The U.S. Consumer Product Safety Commission and Health Canada, in cooperation with American Honda Motor Company announced a voluntary recall of about 17,600 Honda Grass Trimmers February 28. Consumers should stop using recalled products immediately unless otherwise instructed. The shaft can crack and cause the lower gear case and cutting attachment to detach, posing a laceration hazard to the operator and bystanders. Honda is aware of 11 incidents of broken or cracked shafts. No injuries were reported.
Source: http://www.cpsc.gov/cpscpub/prerel/prhtml12/12121.html

For another story, see item **31**

[Return to top]

Defense Industrial Base Sector

9. *February 28, ABC News* – (Alaska; Virginia) **Air Force base quietly pauses F-22 fighter missions after more air problems.** ABC News reported February 28 that pilots at Joint Base Elmendorf-Richardson in Anchorage, Alaska, reported a sudden spike of incidents in which they experienced an apparent lack of oxygen while flying the F-22 Raptor fighter jet — a mysterious, recurring problem that already caused the fleet to sit idle on the tarmac for months in 2011. In at least three incidents in the last 2 weeks, pilots at the base reported the "hypoxia-like" symptoms, leading officials to ground their F-22s for a day for "review," a U.S. Air Force spokeswoman told ABC News. "In each case, appropriate procedures were applied," she said, and the planes went back in the air the day after the temporary halt. An additional case of a pilot experiencing hypoxia-like symptoms also popped up at Virginia's Joint Base Langley-Eustis earlier in February, another Air Force spokesman said.
   Source: http://abcnews.go.com/Blotter/22-raptor-air-force-base-quietly-pauses-fighter/story?id=15807740#.T05AwHn3J2m

10. *February 28, DoD Buzz* – (National) **F-22 Raptor 'smoking gun' not found.** U.S. Air Force (USAF) leaders still do not know for sure why the F-22 Raptor keeps experiencing oxygen problems after the service completed a fleet-wide study of its aircraft oxygen generation systems, DoD Buzz reported February 28. USAF engineers did not find a "smoking gun" during the Air Force Scientific Advisory Board's quick-look study, the Air Force deputy chief of staff for Operations, Plans and Requirements said. The Air Force secretary ordered the study after the service grounded its F-22 fleet when multiple pilots experienced "hypoxia-like" symptoms in flight. An F-22 pilot crashed and died in November 2010. An Accident Investigation Board (AIB) found the fighter jet's bleed air intakes malfunctioned and the pilot "most likely experienced a sense similar to suffocation." However, the AIB's report blamed the pilot, not the aircraft for the crash. The Defense Department's Inspector General is completing an assessment of that report. The scientific advisory board found a few contributing factors, including that a leaky cooling system restricted oxygen reaching pilots, the service's deputy chief of staff for Operations, Plans, and Requirements said February 29. He did not want to list it as the "smoking gun" because service engineers do not know for sure how the fluid from the cooling system got into the F-22's On Board Oxygen Generating System (OBOGS). Engineers also found problems with the F-22's breathing regulator/anti-G (BRAG) valve, he said. The BRAG valve connects the OBOGS to the pilot's oxygen mask.
    Source: http://www.dodbuzz.com/2012/02/28/f-22-raptor-smoking-gun-not-found/

[Return to top]

Banking and Finance Sector

11. *February 28, CBC News* – (International) **Toronto police charge 7 in ATM skimming fraud.** Police in Toronto, Canada, said they have laid 357 charges against seven people accused of skimming ATM and credit card data and using it in several countries.

Private information of at least 1,500 cardholders was compromised by the international ring, police told a news conference February 28. The loss to Canadian financial institutions was more than $360,000, a detective said. Police allege Canadian credit card data, obtained with ATM tamper devices in southern Ontario, was used fraudulently in Bulgaria, the United States, Chile, South Africa, the Dominican Republic, and Mexico. In December, Toronto police executed two search warrants at Toronto homes and allegedly uncovered a facility that manufactured and distributed the tamper devices. Police allege the devices have been used in Ontario, the United States, Australia, and Indonesia. The police service's financial crimes unit worked with U.S. Secret Service and the Canada Border Services Agency on the case. The charges against the 7 men include 33 counts of possessing a credit-card forgery device, 14 counts of fraudulent possession of credit-card data, and 2 counts of making or repairing a credit-card forgery device. Four of the seven have also been charged with participating in a criminal organization.
Source: http://www.cbc.ca/news/canada/toronto/story/2012/02/28/toronto-fraud-atm-skimming.html

12. *February 28, Bloomberg* – (Massachusetts) **State Street fined $5 million by regulator over CDO influenced by Magnetar.** State Street Corp., the third-largest custody bank, was fined $5 million February 28 by Massachusetts' top securities regulator for failing to disclose the role of a hedge fund in structuring an investment vehicle that the fund was betting against. State Street, acting as investment manager of Carina CDO Ltd. allowed Magnetar Capital LLC to influence the composition of the vehicle even though it knew the hedge fund was betting on the failure of some or all of the portfolio, according to a statement from the Massachusetts Secretary of the Commonwealth. Carina subsequently defaulted. Magnetar has been linked to 26 collateralized debt obligation (CDO) transactions, according to the statement.
Source: http://www.bloomberg.com/news/2012-02-28/state-street-is-fined-5-million-over-cdo-influenced-by-magnetar-capital.html

13. *February 28, Reuters* – (National) **Americans lost $1.52 bln to identity theft, scams in 2011.** Identity theft and other scams cost Americans $1.52 billion in 2011, the Federal Trade Commission (FTC) said February 28. In a nationwide sampling of consumer complaints, law enforcement, and other agencies received 1.8 million complaints in 2011, up from 1.4 million in 2010 and double the level in 2006, the FTC said in a statement. Identity theft remained the top category. The increase reflects the growing number of agencies that contributed to the Consumer Sentinel Network, a database that is the basis of the report, rather than an upturn in fraud, the head of the FTC's planning and communications unit told Reuters. Identity theft "has been our No. 1 complaint generator for the past 5 years, and that seems to be consistent" at 15 percent of complaints in 2011, he said. Fraudsters increasingly are using the Internet and e-mail to carry out scams or identity theft rather than by telephone or mail, he said.
Source: http://www.chicagotribune.com/sns-rt-usa-consumerfraudl2e8dsbi3-20120228,0,2334070.story

14. *February 28, AccessNorthGa.com* – (Florida) **Fed suit alleges negligence in Cornelia bank failure.** Two former bank officials with the Community Bank and Trust (CBT) of

Cornelia were listed as defendants in a lawsuit filed in federal court in Gainesville, Florida, February 28. CBT's former president and chief executive officer (CEO) and CBT's retail banking group vice president (VP) were listed as defendants in the suit filed by the Federal Deposit Insurance Corporation (FDIC). The FDIC alleges their negligence resulted in an $11 million loss when they ignored bank policy in issuing Home Funding Loan Program (HFLP) loans. The FDIC wants to recover the money on behalf of the bank's depositors and creditors. CBT closed in January 2010. According to the complaint, the VP breached his fiduciary duties and was negligent in approving HFLP loans, violating bank policy. The president and CEO's alleged negligence stems from his failure to supervise the VP and implement corrective measures.
Source: http://www.accessnorthga.com/detail.php?n=246129

15. *February 28, Associated Press* – (National) **Jury convicts 2 in $50M bank fraud conspiracy.** A federal jury in Minneapolis, Minnesota, convicted two people February 28 for their roles in a $50 million bank fraud conspiracy that authorities said depended on identity theft by employees of some of America's largest banks. The two were found guilty of multiple counts, including bank fraud conspiracy and aggravated identity theft. So far, 27 people have either pleaded guilty or been convicted in the scheme, in which customer identities were stolen, then bought and sold, and used to create phony bank and credit card accounts, apply for loans, or get cash. Prosecutors said the conspiracy was carried out from 2006 through 2011 in Minnesota, California, Massachusetts, Arizona, New York, and Texas. According to evidence at trial, one of the defendants possessed and trafficked more than 8,700 stolen identification documents between March 2006 and December 2010. Prosecutors said the other defendant used fraudulent credit cards to obtain cash from banks and buy merchandise from the Mall of America in Bloomington, Minnesota, and Southdale Mall in Edina, Minnesota. Victims included American Express, Associated Bank, Bank of America, Capital One, Guaranty Bank, JP Morgan Chase Bank, TCF Bank, US Bank, Wachovia Bank, Washington Mutual, and Wells Fargo.
Source: http://www.foxreno.com/news/ap/crime/jury-convicts-2-in-50m-bank-fraud-conspiracy/nK7X6/

16. *February 28, Bloomberg* – (Florida) **TD Bank settles lawsuit with Razorback over fraud in Florida.** Toronto Dominion Bank (TD) agreed February 28 to settle a lawsuit with investors who claimed it aided a $1.2 billion Ponzi scheme run by an imprisoned confidence man, a lawyer said in a Fort Lauderdale, Florida court. Barron's and the Miami Herald reported TD Bank would pay $170 million. A bank attorney told a judge in state court that a draft settlement was reached and is confidential. The accord is with investors known as the Razorback Group. The investors claimed losses of $188 million. The case was scheduled for trial the week of March 5. Razorback's suit against Gibraltar Private Bank & Trust is still set to go to trial the week of March 5. Gibraltar's attorney argued February 28the terms of the TD settlement should be made public, including a disbarred attorney serving 50 years in prison for a scheme he ran out of his Fort Lauderdale law firm. He sold stakes to investors in fictitious employment- and sex-discrimination cases. Seven other people have been criminally charged.
Source: http://www.bloomberg.com/news/2012-02-28/td-bank-settles-lawsuit-with-razorback-over-rothstein-fraud-in-florida.html

17. *February 28, The Register* – (International) **Banking trojan hijacks live chat to run real-time fraud.** A new strain of financial malware is hijacking live chat sessions in a bid to hoodwink business banking customers into handing over their banking log-in credentials or into authorizing fraudulent transactions. The attack is being carried out using the Shylock malware platform, using a configuration that runs a browser-based man-in-the-middle attack. The assault –- which targets business banking customers rather than consumers –- kicks in when a victim logs into their online banking application. Sessions are suspended, supposedly to run security checks (on the pretext the "system couldn't identify your PC"), before a Web-chat screen under the control of hackers is presented to victims. But instead of talking to a customer service rep., the mark is actually chatting to cybercrooks, who will attempt to hoodwink victims into handing over log-in credentials or other data needed to authorize fraudulent transactions. Unbeknownst to the victims, the fraudsters are relaying authorization data to the victim's bank during their conversation, carrying out a concurrent fraud in real time.
Source: http://www.theregister.co.uk/2012/02/28/banking_trojan_hijack_live_chat/

For more stories, see items **32** and **40**

[Return to top]

Transportation Sector

See items **1**, **21**, **25**, **26**, and **39**

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

18. *February 29, Pittsburgh Tribune-Review* – (Pennsylvania) **Brunton Dairy to resume bottling milk.** A Beaver County, Pennsylvania dairy that voluntarily ceased production twice so state regulators could determine whether its products were contaminated will resume bottling operations and sales March 1. The dairy voluntarily ceased milk production July 29, 2011. Sixteen people reported symptoms including abdominal pain, nausea, and diarrhea after drinking pasteurized milk from the dairy that was packaged in glass bottles, according to the state health department. The outbreak was traced to the bacteria Yersinia enterocolitica, but inspectors could never determine its source. The dairy resumed bottling milk October 1, 2011. State inspectors collected random samples over several days and sent them to a lab for testing. The dairy voluntarily stopped bottling milk at the end of October after one sample came back positive for

Yersinia. The state department of agriculture recently acknowledged a lab error caused a reading that led to the second shutdown. A dairy spokesman said distribution of milk initially will be limited to the dairy's store. He did not know when delivery would resume for about 1,000 customers and 25 retail outlets in western Pennsylvania.
Source: http://www.pittsburghlive.com/x/pittsburghtrib/news/breaking/s_783961.html

19. *February 28, Gainesville Sun* – (Florida) **Kitchen fire could close Satchel's for 6 weeks.** A February 28 fire in the kitchen ceiling damaged Satchel's Pizza, a popular Gainesville, Florida restaurant. The owner said smoke was spotted in a corner of the kitchen, and the restaurant was evacuated. He estimated the needed repairs could shut the restaurant for about 6 weeks. Gainesville Fire Rescue crews said they found smoke coming out from an eave, and the fire appeared to be getting worse when they arrived. The roof over the kitchen area has multiple layers, which posed some difficulties for firefighters, the fire chief said.
Source: http://www.gainesville.com/article/20120228/ARTICLES/120229496/-1/entertainment?p=1&tc=pg

[Return to top]

Water Sector

20. *February 29, Associated Press* – (Louisiana) **Man pleads guilty to discharging pollutants.** Federal prosecutors said the son of a father-son team running the Arkla Disposal Services Inc. wastewater treatment facility in Shreveport, Louisiana, pleaded guilty to illegally discharging pollutants into the Red River without a permit. A U.S. attorney said the son pleaded guilty February 28 to discharging untreated wastewater into river in violation of the Clean Water Act. Federal prosecutors said the father still faces charges of violations of the Clean Water Act, conspiracy, and obstruction of justice. His trial has been set for March 12. The facility treated industrial and oilfield wastewater. The son faces a year in prison or a fine of not more than $100,000. Sentencing has been set for June 20.
Source: http://www.dailycomet.com/article/20120229/APN/1202290601?Title=Man-pleads-guilty-to-discharging-pollutants

21. *February 29, Associated Press* – (Maryland) **Broken water main causes sinkhole in Bladensburg on Md. commuter route, closing Annapolis Road.** A sinkhole caused by a water main break closed westbound lanes of Route 450 in Bladensburg, Maryland, February 29. Police said the sinkhole that formed overnight on Annapolis Road is about 8 feet wide and 10 inches deep. Repairs are expected to start immediately. It was unclear how long the road would be closed. A Washington Suburban Sanitary Commission spokesman said the sinkhole is the result of a 12-inch water main break February 16. He said a patch was made to the broken main, and a contractor was supposed to come out the next day to repair the pipe. That apparently did not happen and the patch failed overnight February 29.
Source: http://www.washingtonpost.com/local/broken-water-main-causes-sinkhole-in-bladensburg-on-md-commuter-route-closing-annapolis-road/2012/02/29/gIQAcVemhR_story.html

22. *February 28, Associated Press* – (Iowa) **Antifreeze spilled at Fort Dodge company.** Hundreds of gallons of antifreeze leaked into a Fort Dodge, Iowa storm sewer and ended up in the Des Moines River. The Iowa Department of Natural Resources (DNR) said a contractor hit and broke a chilled water line February 28 at Boehringer Ingelheim Vetmedica, a company that makes drugs for animals. Between 350 and 750 gallons of 12 percent propylene glycol was released onto the ground. Since it was raining at the time, the solution was washed into a Fort Dodge storm sewer and was later discharged into the Des Moines River. The DNR said antifreeze mixes easily with water and it had no impact on the river.
Source: http://www.chicagotribune.com/news/chi-ap-ia-antifreezespill,0,5133864.story

For another story, see item **47**

[Return to top]

Public Health and Healthcare Sector

23. *February 29, Associated Press* – (Colorado) **Man holding hostages dies in Colorado standoff.** A man pulled out a gun at a Colorado Springs, Colorado medical building February 28, and held two people hostage before a police officer shot him; he died hours later. Police said the man showed up with a gun at the Urological Associates office angry at a medical office employee and took her and another person hostage. He released the hostages, but three other people remained in the building, hiding from the gunman. Negotiators tried to get the man to surrender peacefully before officers moved in to try to rescue the people who were still hiding in the building. Police said an officer shot the suspect during an "armed confrontation" after a 3-hour standoff. Dozens of people from several offices in the building were evacuated safely, and nearby schools were locked down during the standoff. More than a dozen police and fire department vehicles and ambulances lined the street near the office during the incident.
Source: http://www.officer.com/news/10635089/man-holding-hostages-dies-in-colo-standoff

24. *February 28, Los Angeles Times* – (Texas) **$375-million Medicare fraud: Dallas doctor accused in record case.** February 28, federal law enforcement officials announced what they called the largest healthcare fraud case in the nation's history, indicting a Dallas area physician for allegedly bilking Medicare for nearly $375 million in billings for nonexistent home healthcare services. Under the alleged fraud scheme, the doctor and his office manager allegedly sent healthcare "recruiters" door-to-door asking residents to sign forms that had the doctor's electronic signature and stated he had seen the residents professionally for medical services he never provided. They also allegedly dispatched more "recruiters" to a homeless shelter in Dallas, paying $50 to every street person they coaxed from a nearby parking lot and signed him up on the bogus forms. The long-running ruse allegedly began in 2006 and over 5 years collected more Medicare beneficiaries than any other medical practice in the United States. Top Justice Department officials, working for several years to stem a rampant rise in healthcare fraud around the country, also revealed that 78 home health agencies that were working with the physician will be suspended from the Medicare program for up

to 18 months.
Source: http://www.latimes.com/news/nation/nationnow/la-na-nn-medicare-fraud-20120228,0,6359381.story

[Return to top]

Government Facilities Sector

25. *February 28, Reuters* – (Washington) **Students in Washington state town evacuated over threat.** Authorities evacuated 900 students from a three-school compound in Cle Elum, Washington, and shut down a highway February 28 after a bomb threat was found on a computer at the high school. Police used bomb dogs to search the high school, middle-school, and elementary school but found no explosives, officials said. The three schools are located in a single complex along state route 903, which was shut down for several hours by the Washington State Patrol between Cle Elum and Roslyn.
Source: http://www.reuters.com/article/2012/02/29/us-washington-school-threat-idUSTRE81S05520120229

26. *February 28, Fort Lauderdale Sun Sentinel* – (Florida) **Explosives removed from charter school in Boynton Beach.** Bomb squad investigators removed explosives from South Tech Academy in Boynton Beach, Florida, that were found February 28. The school was on a nearly 3-hour lockdown. The explosives were found on a bus. The driver that found the explosive device gave it to a school employee, who then left it at the school police officer's desk. When the officer found it, he ordered the school on lockdown and called the Palm Beach County Sheriff's Office bomb squad. School officials evacuated about 35 students and staff members and placed the rest of the school on lockdown shortly after school dismissed for the day. After-school tutoring and sports activities had just started.
Source: http://www.orlandosentinel.com/news/local/fl-south-tech-evacuated-20120228,0,7503424.story

27. *February 28, Arizona Republic* – (Arizona) **Audit: Retired O-6 took $2.7M from Guard fund.** A retired colonel was ultimately responsible for embezzling more than $2.7 million from an emergency fund for Arizona National Guard members during an 8-year period. However, an inattentive supervisor and inadequate oversight played a role in allowing him to carry on his scheme, according to a report from the Arizona auditor general, the Arizona Republic reported February 28. A department employee raised concerns to a supervisor in February 2011 about the colonel's handling of money, but the supervisor failed to take any action for 5 months, the report said. During that time, he steered an additional $140,000 away from a fund to help high-school dropouts and into an account to which he had almost unfettered access. The colonel pleaded guilty to theft and fraud charges in Maricopa County Superior Court and is scheduled to be sentenced March 28.
Source: http://www.militarytimes.com/news/2012/02/gannett-retired-colonel-took-2-million-from-guard-fund-022812/

28. *February 28, Boulder Daily Camera* – (Colorado) **Boulder officials: Toxins found in South Boulder rec center's floors.** Boulder, Colorado officials acknowledged February 28 that potentially toxic materials line the floors of three rooms at the South Boulder Recreation Center and will have to be removed at an unknown cost. A spokeswoman for Boulder's Parks and Recreation Department said city officials have known since late January that a rubberized layer of flooring in the center's main gymnasium, racquetball, and Pilates rooms contain "elevated levels of mercury and lead." She said there is "no immediate danger to the public or employees" because the rubber floor is covered by wood in the gym and on the racquetball courts, and by layers of carpet and vinyl tile in the Pilates studio. According to the Northeast Waste Management Officials' Association, rubber gym floors that were installed prior to 1985 frequently contain high levels of mercury and lead. The flooring was used widely in public buildings, schools, and gymnasiums throughout the early 1970s and 1980s.
Source: http://www.dailycamera.com/boulder-county-news/ci_20061787

For more stories, see items **23**, **33**,

[Return to top]

Emergency Services Sector

29. *February 29, Associated Press* – (Alabama) **1 dead, 3 missing after Coast Guard chopper crashes.** One crew member died and rescuers were searching February 29 for three others missing after a U.S. Coast Guard (USCG) helicopter crashed in Alabama's Mobile Bay during a training mission, USCG officials said. Divers planned to return to the sunken wreckage after daylight February 29. Overnight fog had hampered searches from the air, the chief petty officer said. The MH-65C helicopter crashed February 28 near Point Clear, Alabama. One crew member was found unresponsive and later declared dead, the USCG said in a news release February 29. The aircraft had departed the Aviation Training Center in Mobile, Alabama, on a training mission February 28, an official said. The three missing are all USCG members. The cause of the crash remains under investigation.
Source: http://www.orlandosentinel.com/news/local/breakingnews/os-helicopter-crash-coast-guard-20120229,0,5867153.story

30. *February 28, WTSP 10 ST. Petersburg* – (Florida) **'SWATing' hoax triggers emergency response.** Sheriff's investigators are trying to track down who made a hoax call to emergency operators in Sarasota, Florida, over the weekend of February 25. The caller who identified himself as a 15-year-old, claimed he shot his parents and was armed with a gun. He also claimed to have a bomb strapped to himself, set to detonate within 10 to 15 minutes. "Ultimately there were almost three dozen law enforcement officers dispatched, hostage negotiators, SWAT team, and every available deputy," said a Sarasota County Sheriff's Office spokeswoman. But when deputies arrived, they found an unsuspecting family, no one shot, and no guns. In fact, investigators said the call did not even come from the home. It is part of a troubling trend called "SWATing." The prankster obtains information about their intended target then call in posing as that person with a story that triggers a SWAT-style response. If caught, the prankster could

potentially face federal charges punishable by decades behind bars.
Source: http://www.wtsp.com/news/article/241436/8/SWATing-hoax-triggers-emergency-response-

[Return to top]

Information Technology Sector

31. *February 29, Yomiuri Shimbun* – (International) **U.S. firm posts PLC hacking methods online.** A U.S. information security company posted hacking techniques for disabling programmable logic controllers (PLCs) on the Internet, the Yomiuri Shimbun learned. A PLC is an electronic control system that enables machinery to work as programmed and is widely used in production systems at factories and in critical infrastructure. Alarmed by the hacking method released online by U.S. firm Digital Bond, Inc., DHS's Industrial Control Systems Cyber Emergency Response Team issued a warning stating cyberattacks against PLCs could cause a major systemic breakdown. Four companies in the United States, Japan, and France produce PLC control systems for automakers, electric power substations, and others. Digital Bond stated it posted the hacking method to "inform the public of the risks" of PLC breakdowns, arguing companies and governments have been slow to cope with PLCs' vulnerabilities. About 2 million PLC units per year are manufactured in Japan, approximately 1.4 million of which were exported. While cyberattacks targeting computer control systems have sharply increased overseas, this is the first time a Japanese PLC maker was revealed to be exposed to the risk of a cyberattack. The firms put at risk by Digital Bond's post are: Japan's Koyo Electronics Industries Co.; the United States' General Electric Co. and Rockwell Automation, Inc.; and France's Schneider Electric SA. After figuring out the design flaws of the companies' PLCs, Digital Bond posted programs attacking them on the firms' Web sites February 14, according to the U.S. network security company. Koyo Electronics said it sells several thousands of its PLCs domestically, as well as in the United States and other countries every year. The control systems are mainly used at automobile, semiconductor, and machine tool plants. Should the disclosed hacking techniques be abused, there is a danger the systems involved could be illegally controlled by a remote party. The PLCs made by the remaining three manufacturers feature designs that are different from each other, and are also used at a wide range of factories and transformer stations. Should these systems be hacked using Digital Bond's methods or other tricks, production and other systems would break down or develop anomalies such as abnormal restarts. However, no direct links to Digital Bond's post have been confirmed, industry sources said.
Source: http://www.yomiuri.co.jp/dy/national/T120228005028.htm

32. *February 29, Softpedia* – (International) **Attack can circumvent OpenSSL protection, researchers say.** A collaborative team of researchers at the RSA conference in San Francisco planned to reveal an attack method that can be used to bypass the security measures offered by OpenSSL, allowing an attacker to recover the cryptographic key that ensures data is transferred in an encrypted form between users and secure Web servers. According to Quantum Day, a senior lecturer in computer

science in the department of computer science at the University of Bristol, one of the members of the collective, will present the findings and show how their attack works. By triggering a bug in the software with the aid of cleverly designed messages sent to the Web servers, the experts managed to recover part of the cryptographic key. If a large number of messages are used, the entire key could be obtained. The approach proposed by the team only works on the 0.9.8g version of OpenSSL and only on certain configurations, but if it works it can represent yet another threat to the integrity of the SSL protocol on which so many businesses rely. In the case of the e-commerce Web sites, whose popularity is constantly growing among Internet users, the exposure of the cryptography key can make the difference between credit card numbers being safe, or ending up in the hands of a profit-driven hacker.
Source: http://news.softpedia.com/news/Attack-Can-Circumvent-OpenSSL-Protection-Researchers-Say-255711.shtml

33. *February 29, Softpedia* – (International) **UN.org, Skype.com, and Oracle.com hacked by D35m0nd142.** Grey hat hacker D35m0nd142 managed to gain unauthorized access to the sites of the United Nations, Skype, and Oracle. On the official Skype site, the hacker found Blind SQL injection vulnerabilities that allowed him to access their Web server. A similar vulnerability was discovered on Oracle's community site, which can allow hackers to cause serious damage. By leveraging an MSSQL injection flaw, he managed to bypass the security protocols implemented by the United Nations site administrators. In each scenario, the hacker ensured the data he accessed remained unharmed and contacted the ones responsible for the sites to notify them of the presence of the issues.
Source: http://news.softpedia.com/news/UN-org-Skype-com-and-Oracle-com-Hacked-by-D35m0nd142-255812.shtml

34. *February 28, Government Computer News* – (International) **Researchers: How 'leaky' smart phones give up their crypto keys.** Smart phones being used for sensitive transactions leak data that can be used to recover the cryptographic keys securing connections, according to researchers presenting at the RSA Conference. Tests using about $1,000 worth of off-the-shelf equipment were able to pick up power usage information from phones' CPUs from as far away as 30 feet, said the vice president of technology at Cryptography Research Inc. By analyzing power consumption in the CPU during cryptographic processes, data — including crypto keys — could be extracted.
Source: http://gcn.com/Articles/2012/02/28/RSA-6-crypto-keys-extracted-from-leaky-smart-phones.aspx?Page=1

For another story, see item **17**

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

35. *February 29, IDG News Service* – (International) **Malware increasingly uses DNS to avoid detection, experts say.** The number of malware threats that receive instructions from attackers through domain name system (DNS) is expected to increase, and most companies are not currently scanning for such activity on their networks, security experts said February 28 at the RSA Conference 2012. There are many channels attackers use for communicating with their botnets, ranging from traditional ones such as TCP, IRC, and HTTP to more unusual ones such as Twitter feeds, Facebook walls, and even YouTube comments. Most malware-generated traffic that passes through these channels can be detected and blocked at the network level by firewalls or intrusion prevention systems. However, that is not the case for DNS and attackers are taking advantage of it, said the founder of Counter Hack Challenges and SANS fellow during a presentation on new attack techniques. The DNS protocol is normally used for a precise critical function — the translation of host names into IP addresses and vice-versa. Because of this, DNS traffic does not get filtered or inspected by traffic monitoring solutions and is allowed to flow freely through most networks. As DNS queries gets passed from one DNS server to another until they reach the authoritative servers for the respective domains, network-level IP blocklists are useless at blocking them.
    Source:
    http://www.computerworld.com/s/article/9224743/Malware_increasingly_uses_DNS_to_avoid_detection_experts_say?taxonomyId=17

36. *February 29, WHIZ 40 Zanesville* – (Ohio) **Power restored-WHIZ stations back on-air.** The early morning storms that rumbled through Zanesville and other parts of southeastern Ohio caused some power outages February 29. The power disruption also knocked WHIZ TV, AM 1240 Radio, Z-92, and Highway 103 off air. American Electric Power told WHIZ News that it was a transmission problem with two sub-stations. After about 3 hours February 29, power was restored to all customers.
    Source: http://www.whiznews.com/content/news/local/2012/02/29/power-restored-whiz-stations-back-on-air

37. *February 28, Arizona Republic* – (Arizona) **Cox Communications voice mail is down for some.** Cox Communications landline phone customers in metro Phoenix said February 28 they had been without voice-mail service for more than a week. A Cox spokeswoman acknowledged the problem in an e-mail and said the company was working hard to fix it. She would not disclose how many customers were affected by the outage, nor could she give an estimate of when the voice mail service would be restored. Only residential telephone customers were affected, she said, adding that they were still able to make and receive calls. She said customers had the option of setting up call-forwarding service to another phone number. The service would be offered free to affected customers, she said.
    Source:

http://www.azcentral.com/arizonarepublic/business/articles/2012/02/28/20120228cox-communications-voice-mail-down-for-some.html

For more stories, see items **33** and **34**

[Return to top]

Commercial Facilities Sector

38. *February 29, Florida Times-Union* – (Florida) **Suspicious powder delivered to Jacksonville Girl Scouts office tested harmless.** A state laboratory determined that a suspicious white powder in a package opened February 28 at the Girl Scouts of Gateway Council office in Jacksonville, Florida, contained no harmful agents. However, the package's contents resulted in an evacuation of two facilities. Since the package was specifically addressed to an employee, Girl Scouts officials also evacuated their office in Gainesville as a safety precaution. Fire officials cleared the scene at 2 p.m., although the 40 Jacksonville employees and those in the Gainesville office would not return to work until February 29.
Source: http://jacksonville.com/news/crime/2012-02-28/story/suspicious-powder-delivered-jacksonville-girl-scouts-office-tested

39. *February 29, Associated Press; MSNBC; NBC News* – (National) **'Devastation ... like we've never seen' in twister-hit town.** At least 9 people were killed February 28-29 as a line of tornadoes marched across the Midwest. Forecasters warned more twisters could strike the Tennessee Valley and southern Appalachians through February 29. Six of the deaths and nearly 100 injuries occurred in Harrisburg, Illinois, after an EF-4 tornado swept through, destroying at least 200 homes and more than 25 businesses. Three other deaths were reported in Missouri, where storms included a suspected tornado that hit a mobile home park outside the town of Buffalo. One person died in the mobile home park and around a dozen people were injured. Two others died in the Cassville and Puxico areas of Missouri. In Harrisburg, police issued a curfew overnight and the area most impacted was evacuated as a precaution. Some 3,300 customers were without power in the town of about 10,000. About 12 people were injured when an EF-2 tornado ripped through Harveyville, Kansas. At least three of the injured are in critical condition, according to Weather.com, and 40 percent of the town suffered damage. KSHB 41 Kansas City reported an apartment complex and a church were among the damaged buildings A tornado with a preliminary rating of EF-2 moved through Branson, Missouri, injuring 32 people and heavily damaging the city's famous theaters and moving up Highway 76, uprooting road signs and scattering debris. The assistant general manager for the 530-room Hilton and adjacent Branson Convention Center, noted windows were shattered and some rooms had furniture sucked away by high winds. Hotel workers were able to get all guests to safety as the storm raged. The owner of the damaged Cakes-n-Creams '50s Diner said the theater next to his business "kind of exploded", and the hotels "on the two sides of me lost their roofs." Newburgh, Indiana, and Kingsport, Tennessee, also reported storm damage.
Source: http://usnews.msnbc.msn.com/_news/2012/02/29/10536654-4-killed-as-tornadoes-rake-midwest-states

40. *February 28, U.S. Federal Trade Commission* – (National) **FTC action leads to court orders banning marketers from selling vacation packages.** The operators behind a vacation prize scheme have been banned from selling vacation packages under settlements with the U.S. Federal Trade Commission (FTC) and the Florida Attorney's General Office, which charged the defendants with tricking consumers into believing they had won a vacation package as a prize, and then failing to provide the package as promised, according to a February 28 release. According to the complaint, the defendants advertised a vacation package worth thousands of dollars as a prize to consumers who called a toll-free number and answered a trivia question. Callers were told they had won, and that if they paid up to $400 in "taxes" or "fees" they would receive their prize. The complaint alleged callers did not receive the vacation packages as promised. The defendants are VGC Corporation of America, also doing business as All Dream(s) Vacations, All Dreams Travel, Five Star(s) Vacations, 5 Star(s) Vacations, Total Tours, and Travel & Tours Corp.; All Dream Vacations Corp., also doing business as All Dreams Vacations; and three individuals. The orders also impose a judgment of more than $14 million, which will be suspended on the satisfaction of numerous terms and conditions designed to ensure that the defendants will be stripped of all of their assets of value.
Source: http://www.ftc.gov/opa/2012/02/vgc.shtm

41. *February 28, KRLD 1080 AM Dallas* – (Texas) **3-alarm fire guts east Dallas business.** Fifty-four firefighters battled intense smoke from a laundromat fire in Dallas, February 28. Due to the extremely thick smoke, firefighters attacked the blaze defensively for more than 2 hours before they could go inside the building to fight the flames. Three fire companies fought the blaze. No one was seriously hurt and only one person suffered some minor smoke inhalation and was treated at the scene. The cause of the fire was still under investigation.
Source: http://dfw.cbslocal.com/2012/02/28/3-alarm-fire-guts-south-dallas-business/

42. *February 28, San Francisco Bay City News* – (California) **Three busted for allegedly robbing shipyard by boat.** Two men and a woman were arrested for allegedly burglarizing San Francisco's Hunters Point Shipyard after traveling there by boat February 27, police said. The individuals were arrested as part of a sting at the shipyard, where tools, wires, pipes and other equipment had recently been stolen, then recycled for cash, according to police. San Francisco police conducted the operation in coordination with University of California police and federal authorities. Investigators believed the thieves were using boats to enter nearby Islais Creek and began surveillance there the night before, according to police.
Source: http://sfappeal.com/news/2012/02/three-busted-for-allegedly-robbing-shipyard-by-boat.php

For another story, see item **32**

[Return to top]

National Monuments and Icons Sector

43. *February 29, TriCities.com* – (Virginia) **Cause of Lee County wildfire unknown.** An 800-acre wildfire was reported in Lee County, Virginia, and firefighters were working February 28 to save the 34 homes and other buildings in its path. Emergency personnel were called to the blaze, which was burning southeast of the Blackwater community, near state Routes 600 and 602, February 27, the Virginia Department of Forestry's director of public information said. A combined crew of 8 firefighters from the department of forestry and Blackwater Volunteer Fire Department set up a containment line around the whole fire, and no homes were evacuated. No injuries or structural damage was reported from the fire, which is burning about 200 acres of forest and 600 acres of 8-foot-tall buffalo grass. The cause of the fire is still unknown.
Source: http://www2.tricities.com/news/2012/feb/29/cause-lee-county-wildfire-unknown-ar-1727911/

44. *February 28, Cherokee Scout* – (North Carolina) **Wildfire still burning in national forest.** A fire in the Nantahala National Forest in Cherokee County, North Carolina was expected to burn 750 acres by February 29. More than 40 firefighters from the U.S. Forest Service and other agencies were fighting the fire about 14 miles northwest of Murphy near Turner Top Mountain, said a spokeswoman for national forests in North Carolina. The fire was reported February 26. Ninety percent of the fire is on national forest service land, and no structures are threatened.
Source:
http://cherokeescout.com/articles/2012/02/28/news/doc4f4d32cc62d4c328094578.txt

[Return to top]

Dams Sector

45. *February 29, Wilkes-Barre Times Leader* – (Pennsylvania) **Levee repair completion expected this summer.** The U.S. Army Corps of Engineers expects to finish design and engineering for repairs to the Wyoming Valley levee system in Luzerne County, Pennsylvania, during spring 2012 and work to be completed this summer, all paid for with federal funds, the Wilkes-Barre Times Leader reported February 29. According to a spokesman for the Corps' Baltimore District, the system will be restored to its condition prior to last summer's record flooding. In September 2011, boils threatened to compromise the levee system near the county recreation fields in Forty Fort when the Susquehanna River swelled to a record level of more than 42 feet. The spokesman said the damage varied along the length of the system. Some included debris obstruction in culverts, damage to outfall pipes, and damage near and around the floodwall.
Source:
http://www.timesleader.com/news/Levee_repair_completion_expected_this_summer_02-29-2012.html

46. *February 29, Omaha World-Herald* – (Midwest) **Flooding costs top $1 billion.** Costs revealed February 28 continue to push the bill for 2011 Missouri River flooding over

$1 billion in the states of Nebraska, Iowa, Missouri, and Kansas. Early estimates indicate the U.S. Army Corps of Engineers' six big upriver dams prevented at least $7.6 billion in damage last year, said a spokesman who manages river programs for the Corps. He said the reservoir system provides an average $1.8 billion in annual benefits. The commander of the Omaha District said the $7.6 billion prevented-damage estimate is a "low-ball number" because it is based on 1970s-era information of which businesses, homes, crops, and developments exist in the river floodplain. However, the cost of flooding continues to climb, officials said. Nearly 1,100 Nebraskans and 1,300 Iowans have sought individual assistance from the Federal Emergency Management Agency. Officials said the cost of repairs to dams and levees will climb as engineers continue inspections and find soft spots in levees, for example. Seepage is a primary concern in 2012 because floodwater was on the levees for a long time and could have created a capillary effect through the earthen structures. Repairs to five holes in levees protecting the Hamburg, Iowa, and Rockport, Missouri, areas now are substantially complete, officials reported. Crews worked through the night February 27 to finish closing the third and final breach in the Hamburg area before a rainstorm February 28. The levees have been rebuilt to original height and width. Officials said the five projects represented the most critical repairs in the levee system damaged during 2011's flood.
Source: http://www.omaha.com/article/20120228/NEWS01/702289888

47. *February 28, U.S. Army Corps of Engineers* – (Washington) **Oil leak reported at Ice Harbor Lock and Dam.** About 44 gallons of new transformer oil leaked into the Snake River during an oil transfer operation at Ice Harbor Lock and Dam in Washington February 27, according to U.S. Army Corps of Engineers Walla Walla District officials. The leak occurred while maintenance staff was replacing the oil in three of the dam's six power transformer heat exchangers or "cooling units" — these cooling units had been traced as the likely source of an oil sheen observed by Corps staff and reported to state officials in December and January. The transformers and cooling units are being repaired; part of the repair process is to replace clean oil into the transformers and cooling units. During a nonroutine oil-flushing operation, oil escaped from an open transfer connection onto a concrete floor in the powerhouse and into a drain running to the powerhouse drainage sump. Maintenance crews shut down oil-transfer operations and used absorbent pads to recover oil on floor. Of the 64 gallons of oil that leaked from the open transfer connection, about 15 gallons were recovered in the dam during Ice Harbor staffs' spill-response actions, 5 gallons remained in the oil transfer hoses, leaving 44 gallons of oil unaccounted for and assumed to have been discharged to the river.
Source: http://www.keprtv.com/news/local/Oil-leak-reported-at-Ice-Harbor-Lock-and-Dam-140803743.html

[Return to top]

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

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