Daily Open Source Infrastructure Report
23 February 2012

Top Stories

- An international phone scam where callers in India posed as debt collectors bilked millions of dollars out of more than 10,000 U.S. residents by using threats of arrest or the loss of their jobs, authorities said. – *Associated Press* (See item **16**)
- Code was published that attackers could use to crash fully patched versions of pcAnywhere on any Windows PC, without first having to authenticate to the PC. – *InformationWeek* (See item **34**)

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 21, U.S. Department of Labor* – (Texas) **US Department of Labor's OSHA cites Precision Drilling for exposing workers to safety hazards at drilling site near Pecos, Texas.** The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) cited Precision Drilling Co. L.P. with two serious and two

repeat safety violations following a November inspection of the company's work site, which is located 18 miles northeast of Pecos, Texas. Proposed penalties total $69,300. The inspection was conducted as part of OSHA's oil and gas regional emphasis program, which is designed to prevent fatalities and catastrophic events at oil drilling and gas wells. The serious violations included failing to ensure portable fire extinguishers were kept in their designated places and to remove or repair damaged electrical cords.
Source:
http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=21855

2. *February 21, Aberdeen News* – (South Dakota) **Diesel leak cleanup continues near Aberdeen.** It could take up to 10 days to clean up diesel after a pipeline leak from the NuStar Energy pipeline about 2 miles north of Aberdeen, South Dakota, a company spokesman said February 21. The firm initially estimated that around 500 barrels spilled from the February 20 leak. NuStar's continuous self-monitoring system on its pipeline system discovered a leak in a small section of the petroleum products pipeline. The 6-inch pipeline, which carries diesel, was shut down and NuStar and third-party response teams were mobilized. To clean the area, the affected soil will e excavated, removed, and taken for disposal. Shutting down the line will not affect the diesel supply in the region because there is an abundant supply of diesel in NuStar's other terminals, including Aberdeen. The leak is under investigation.
Source: http://www.aberdeennews.com/news/aan-crews-cleaning-up-diesel-spill-this-morning-near-aberdeen-20120221,0,5404243.story

3. *February 21, U.S. Department of Labor* – (Florida) **2 Florida companies cited by US Department of Labor's OSHA after worker injured by explosion at gas station.** The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) cited Coomes Oil & Supply Inc., doing business as the 5th Wheel BP gas station in St. Augustine, Florida, and Florida Rock & Tank Lines Inc. for safety hazards after an employee of the latter company was burned in an explosion at the station in August. A Florida Rock & Tank Lines delivery driver was refilling an above-ground gasoline storage tank with a broken gauge. The tank overflowed, and the combination of vapors and heat from the running delivery truck caused an explosion. The OSHA's inspection found the gas station and Florida Rock & Tank Lines decided to refill the storage tank even though the liquid level gauging system was inoperable. Florida Rock & Tank Lines has been cited for one willful violation with a proposed penalty of $70,000 for failing to provide a means for the delivery driver to determine if the storage tank had enough capacity for additional gasoline.
Source:
http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=21849

4. *February 21, Demopolis Times* – (Alabama) **Corrosion cited in pipeline explosion.** A corroded pipe has been blamed for a massive natural gasoline explosion in Sweet Water, Alabama, December 2011, the Demopolis Times reported February 21. A Transco natural gas pipeline ruptured December 3 with an explosion that could be

heard for more than 30 miles while shooting flames nearly 100 feet in the air for more than an hour. The pipeline was shut down immediately after the failure as firefighters battled the blaze for the next 90 minutes. "Although we have systems and processes in place to prevent and identify corrosion, our investigation indicated there were multiple factors working in conjunction that led to this problem not being recognized," a Transco spokesman said. "Extremely corrosive soil conditions, combined with failures in the pipeline's protective coating and cathodic protection system ultimately weakened the pipe, causing it to rupture." The rupture forced the company to make several changes in its corrosion control program.
Source: http://www.demopolistimes.com/2012/02/21/corrosion-cited-in-pipeline-explosion/

For more stories, see items **6** and **17**

[Return to top]

Chemical Industry Sector

5. *February 22, Easton Express-Times* – (Pennsylvania) **Essroc Cement Corp. agrees to pay $82,000 for alleged toxic chemical reporting violations.** Essroc Cement Corp. agreed to pay $82,000 to settle alleged violations of toxic chemical reporting requirements at its manufacturing facility in Nazareth, Pennsylvania, the Easton Express-Times reported February 22. The U.S. Environmental Protection Agency (EPA) cited the cement company for violating the Emergency Planning and Community Right-to-Know Act and said Essroc failed to submit 3 years of required reports on lead, a regulated toxic chemical. The years spanned 2006 to 2008 when the site processed lead in amounts in excess of 130,000 pounds annually — significantly exceeding the law's 100-pound reporting threshold, the EPA's June 2011 investigation found. As part of the settlement, Essroc did not admit liability, but now complies with federal law, the EPA said. Essroc in December agreed to pay $33 million for pollution control technology to resolve alleged violations of the Clean Air Act at five of its plants. Essroc also promised to pay a $1.7 million fine under the agreement, which settled a clean air investigation by the EPA.
Source:
http://www.lehighvalleylive.com/nazareth/index.ssf/2012/02/essroc_cement_corp_agrees_to_p.html

6. *February 22, KARK 4 Little Rock* – (Arkansas) **Tanker containing 3,000 gallons of hydrochloric acid overturns in White County.** HAZMAT crews worked into February 22 cleaning up after a tanker containing 3,000 gallons of hydrochloric acid overturned in White County, Arkansas. The accident happened late February 21 at the intersection of Peanut Ridge and Shiloh Road in the community of Coffey near Searcy. White County deputies evacuated one house and blocked off a 2-mile radius around the accident. Deputies said less than 100 gallons actually leaked. The driver was said to be in the area delivering the acid for fracking.
Source: http://arkansasmatters.com/fulltext?nxd_id=511972

7. *February 21, NorthJersey.com* – (New Jersey) **DuPont cleanup put off for a year.** The federal Environmental Protection Agency (EPA) is delaying DuPont's cleanup of Pompton Lake in Pompton Lakes, New Jersey, for a year after residents and another government agency complained the chemical giant's proposed dredging was not enough. The cleanup, which had been planned for the spring, will not happen until 2013, the EPA announced February 21. The move comes after the U.S. Fish and Wildlife Service said the proposed dredging of 26 acres at the mouth of Acid Brook would not be enough to protect wildlife from contamination. Many residents were also skeptical cleaning just a small portion of the 200-acre lake could solve 100 years of mercury contamination from DuPont's factory. A DuPont spokesman said the firm targeted the delta because its studies showed that was where most of the mercury accumulated. Both the EPA and DuPont had expected to start the project around March. But an EPA spokeswoman said the agency was delaying the work so it could address the concerns.
   Source:
   http://www.northjersey.com/news/139944213_DuPont_cleanup_put_off_for_a_year.html

For more stories, see items **17**, **23**, and **26**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

8. *February 22, Richmond Times-Dispatch* – (Virginia) **Elevated radioactivity levels found in North Anna well.** February 17, Dominion Virginia Power was notified by its laboratory contractor that water taken from an on-site groundwater sampling point at its North Anna nuclear power station near Mineral, Virginia contained an unusually high level of tritium — more than twice the U.S. Environmental Protection Agency's standard for drinking water. "At this point, I don't think there's any concern on the NRC's [Nuclear Regulatory Commission] part that it would affect (nearby Lake Anna) or drinking water supplies," said a spokesman for the agency's Atlanta office. Dominion is not sure where the radioactivity is leaking from, but the two reactors at the plant are not the source, a company spokesman said. Dominion said it has been working to find and fix potential sources of the escaping tritium, and that the contaminated water is not leaking off-site.
   Source: http://www2.timesdispatch.com/business/2012/feb/22/tdmain01-elevated-levels-of-a-weak-form-of-radioac-ar-1706167/

9. *February 22, CNN* – (International) **NRC examines U.S. response to Fukushima.** February 21, the Nuclear Regulatory Commission (NRC) released about 3,000 pages of transcripts of conversations recorded in its operations center after the Fukushima Daiichi nuclear disaster, conversations that underscore the difficulty the agency had in responding to the crisis unfolding halfway around the world. The transcripts, released in response to Freedom of Information Act requests, show agency officials struggling to get information about the disaster and trying to ascertain its potential impact on U.S. citizens in Japan, on potential fallout victims in the United

States, and on operators of U.S. nuclear reactors of similar design. The transcripts are of conversations and phone calls at the NRC's operations center in Rockville, Maryland. Agency officials said the Fukushima experience demonstrated the "significant limitation" the United States had on getting data about an incident "halfway around the world." Officials also said previous exercises in the command center had not fully prepared them for what turned out to be a months-long event that required teams of people working round-the-clock for months. They said they did not communicate as fully as they should have with state officials seeking information about the potential for fallout and the safety of their own nuclear plants.
Source: http://www.krcrtv.com/news/30511475/detail.html

10. *February 21, Reuters* – (National) **U.S. nuclear plants to buy more safety equipment.** Operators of the 104 nuclear reactors in the United States have agreed to purchase additional equipment to respond to emergencies that interrupt off-site power, the Nuclear Energy Institute (NEI) said February 21. The equipment will help ensure that every U.S. commercial nuclear energy facility can respond safely to extreme events. NEI said U.S. companies have ordered more than 300 pieces of equipment, ranging from diesel-driven pumps and generators, fans, hoses and communication gear. "The additional portable equipment will provide power and water to maintain three key safety functions in the absence of AC power and heat transfer capability from permanently installed safety systems," said the NEI's chief nuclear officer. The three functions are reactor core cooling, used fuel pool cooling, and containment integrity. The Nuclear Regulatory Commission is working through a sweeping set of reforms to ensure a Fukushima disaster does not occur at any of the nuclear stations located in 31 states.
Source: http://www.foxbusiness.com/industries/2012/02/21/us-nuclear-plants-to-buy-more-safety-equipment/

[Return to top]

Critical Manufacturing Sector

Nothing to report

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Banking and Finance Sector

11. *February 22, Orange County Register* – (California) **Authorities: 'Snowboarder Bandit' robs Laguna Niguel bank.** Deputies in Laguna Niguel, California, are investigating a bank robbery that occurred at 1:30 p.m. February 21 at a Chase Bank,

with authorities briefly blocking off a parking structure at a busy Irvine shopping center to search for a suspect. Authorities believe the incident is tied to a serial robber known as the "Snowboarder Bandit," suspected of carrying out at least seven Orange County holdups in Irvine, Laguna Hills, Anaheim Hills, Ladera Ranch, and Corona del Mar. In the latest robbery, the man handed the teller a note, then left with an unknown amount of cash, an Orange County Sheriff's Department spokesman said. The "Snowboarder Bandit" earned his nickname due to his youthful appearance and the ski-type clothes he wears during robberies.
Source: http://www.ocregister.com/news/bank-341291-chacon-niguel.html

12. *February 22, U.S. Securities and Exchange Commission* – (New York; International) **SEC charges China-based executives with securities fraud.** February 22, the U.S. Securities and Exchange Commission (SEC) charged two China-based executives with defrauding U.S. investors into believing they were investing in a Chinese coal business when in fact they were investing in an empty shell company. The SEC alleges Puda Coal Inc.'s chairman embarked on a scheme with its former chief executive officer (CEO) to steal and sell Puda's sole revenue-producing asset, a coal-mining company named Shanxi Puda Coal Group. Just weeks before Puda Coal announced Shanxi Coal received a highly lucrative mandate from provincial government authorities, the chairman quietly transferred Puda's 90 percent stake in Shanxi Coal to himself. In July 2010, he transferred a 49 percent equity interest in Shanxi Coal to CITIC Trust Co Ltd., a Chinese private equity fund. CITIC placed its 49 percent stake in Shanxi Coal in a trust and then sold interests in the trust to Chinese investors. The chairman caused Shanxi Coal to pledge 51 percent of its assets to CITIC as collateral for a $516 million loan from the trust to Shanxi Coal. In exchange, CITIC gave the chaurman 1.212 billion preferred shares in the trust. According to the SEC's complaint, the transactions were not approved by Puda's board or shareholders and not disclosed in SEC filings, which the chairman and CEO knew were materially false and misleading. During two Puda Coal public offerings in 2010, CITIC was separately selling interests in Shanxi Coal to Chinese investors while the chairman and CEO were still telling U.S. investors Puda Coal owned a 90 percent stake in that company. Puda Coal's common stock was listed and traded on the New York Stock Exchange from September 2009 to August 2011.
Source: http://www.sec.gov/news/press/2012/2012-31.htm

13. *February 21, Gaithersburg Gazette* – (Maryland; Virginia) **Beltway bank bandit pleads guilty last week, faces life in prison.** A Beltsville, Maryland man connected to at least 20 robberies in Maryland and Virginia pleaded guilty February 17 to bank robbery and handgun charges in federal court. He was originally facing 14 charges in a Montgomery County, Maryland court following his arrest by police September 16, 2011. A felony information filing January 31 ultimately charged the man with one count each of bank robbery, the possession of a firearm by a previously convicted felon, and the use of a handgun in a violent crime. Police in Montgomery County and Arlington and Alexandria, Virginia, said they linked the man to as many as 13 bank jobs in Montgomery and at least 10 in Virginia from July 2, 2010, to September 6, 2011. He faces a maximum sentence of life in prison and a $750,000 fine, according to his plea agreement. Police estimate he made off with at least $108,706 in total from his

robberies.
Source: http://www.gazette.net/article/20120221/NEWS/702219964/1022/beltway-bank-bandit-pleads-guilty-last-week-faces-life-in-prison&template=gazette

14. *February 21, Atlanta Journal-Constitution* – (Georgia) **Sandy Springs police arrest suspects in credit fraud case.** Authorities arrested a Sandy Springs, Georgia couple in connection with the theft of possibly hundreds of credit card numbers, the Atlanta Journal-Constitution reported February 21. The wife faces 29 charges of financial identity fraud. Her husband was arrested February 14 and faces a charge of financial identity fraud and possession of tools for the commission of a crime. According to Sandy Springs Police, managers at a Taco Mac restaurant suspected the woman of stealing credit card numbers while working as a server. In December 2011, her managers saw her remove a portable skimmer from her apron pocket. Police said the managers later found the skimmer in the woman's coat pocket and notified authorities. Information retrieved from the device indicated 29 credit card numbers were illegally obtained while the device was in the woman's possession, police said. Detectives executed another search warrant at her home February 14, where they recovered three commercial credit card reading and writing devices, along with dozens of prepaid gift cards containing information allegedly gleaned from customers.
Source: http://www.ajc.com/news/north-fulton/sandy-springs-police-arrest-1357688.html

15. *February 21, Escondido North County Times* – (California) **Local couple accused in mortgage fraud scheme.** An Escondido, California real estate agent and his wife pleaded not guilty February 21 to conspiracy and other charges related to what federal prosecutors said was a $50 million mortgage fraud. The couple and seven others were named in an indictment unsealed February 21. They all face multiple counts of conspiracy, wire fraud, money laundering, and criminal forfeiture. The U.S. attorney's office accused the defendants of taking part in a multimillion-dollar mortgage fraud scheme that targeted low-income immigrants in San Diego. According to the indictment, the husband owned and operated real estate and mortgage brokerage businesses in San Diego and employed the other seven named in the indictment. Prosecutors said he and his employees conspired to get mortgage loans for unqualified buyers by lying to lenders about their job and salary information. According to the indictment, the loans were processed by the man's wife, who worked at a subprime lender. Prosecutors also accused the defendants of conspiring to create false financial records for the purpose of verifying the income listed on applications. Lenders supplied more than $50 million in loans based on the false documents, losing more than $15 million, according to the indictment.
Source: http://www.nctimes.com/news/local/escondido/escondido-local-couple-accused-in-mortgage-fraud-scheme/article_612f2bd3-0d00-5fda-a8c2-c1552e89965d.html

16. *February 21, Associated Press* – (California; International) **Authorities say debt-collector scam bilked millions.** An international phone scam where callers in India posed as debt collectors bilked millions of dollars out of more than 10,000 U.S. residents by using threats of arrest or the loss of their jobs, U.S. authorities said

February 21. The callers, who apparently coordinated with someone in the United States, drew on personal data snatched from payday loan Web sites, a Federal Trade Commission (FTC) official said. Over a 2-year period, at least 20 million calls may have been placed, with phony collectors typically demanding around $500, but sometimes asking for as much as $2,000. The investigation of a scam with so many millions of calls flooding in from India was a first of its kind, the FTC's Midwest director said. From 2010 to 2012, $5 million was paid in 17,000 transactions to accounts controlled by the alleged fraudsters, the FTC said. No criminal charges have been filed, but the FTC charged Villa Park, California-based American Credit Crunchers LLC, Ebeeze, LLC, and their owner with violating the FTC Act and the Fair Debt Collection Practices Act in connection to the alleged scheme. The owner allegedly withdrew thousands of dollars paid by victims that ended up in his company accounts, though the FTC said it was not clear if the scheme was directed primarily from California or India.
Source: http://www.foxnews.com/us/2012/02/21/authorities-say-debt-collector-scam-bilked-millions/

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

[Return to top]

Transportation Sector

17. *February 22, Reuters* – (Texas) **Fog halts ships overnight on Houston Channel-Coast Guard.** Ships were halted overnight February 21 along the Houston Ship Channel as dense sea fog impaired visibility along the 53-mile waterway to the busiest U.S. petrochemical port, the U.S. Coast Guard said February 22. In Houston, 42 ships were waiting to transit the ship channel, according to the Coast Guard. The pilots were preparing to resume guiding ships along the waterway February 22.
Source: http://www.reuters.com/article/2012/02/22/transport-shipping-houston-channel-idUSH5E8D900N20120222

For more stories, see items **2**, **4**, **6**, **22**, and **29**

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

18. *February 22, Food Safety News* – (National) **CDC: Raw milk much more likely to cause illness.** Raw milk and raw milk products are 150 times more likely than their pasteurized counterparts to sicken those who consume them, according to a 13-year

review published by the Centers for Disease Control and Prevention (CDC) February 21. States that permit raw milk sales also have more than twice as many illness outbreaks as states where raw milk is not sold. The CDC study, published online in Emerging Infectious Diseases, reviewed dairy-related outbreaks between 1993 and 2006 in all 50 states, during which time the authors counted 121 outbreaks resulting in 4,413 illnesses, 239 hospitalizations, and 3 deaths. Despite raw milk products accounting for about1 percent of dairy production in the United States, raw milk dairies were linked to 60 percent of dairy-related outbreaks. In addition, 202 of the 239 hospitalizations (85 percent) resulted from raw milk outbreaks. Thirteen percent of patients from raw milk outbreaks were hospitalized, versus 1 percent of patients from pasteurized milk outbreaks. Currently, 30 states permit the sale of raw milk, while another 7 are considering raw milk legislation changes in 2012.
Source: http://www.foodsafetynews.com/2012/02/cdc-raw-milk-much-more-likely-to-cause-illness/

19. *February 21, Associated Press* – (California) **$100K reward in arson attack at CA beef processor.** Fresno County, California authorities are offering $100,000 for information leading to an arrest in an arson attack in January at the state's biggest beef processor. Sheriff's officials announced the reward February 21. The January 8 fire destroyed 14 big-rig tractors and several trailers at Harris Ranch near Coalinga. Harris Ranch estimated the loss in excess of $2 million. Animal rights activists claimed responsibility for the fire through an anonymous e-mail released by the North American Animal Liberation press office. The e-mail included a description of the containers of accelerant and kerosene-soaked rope apparently used to set the fire. Sheriff's investigators declined to comment on whether the group's description matches details from the investigation.
Source: http://www.mynews4.com/news/story/100K-reward-in-arson-attack-at-CA-beef-processor/iG6AELMs_EWI-jfZUVvYsQ.cspx

20. *February 21, Associated Press* – (Pennsylvania) **US labor agency cites Hershey distribution plant.** Federal labor officials said they found nine workplace violations at a candy repackaging and distribution facility in Palmyra, Pennsylvania, owned by The Hershey Co. and operated by Exel Inc. where foreign student workers protested the summer of 2011. The Occupational Safety and Health Administration said February 21 it has proposed penalties of $283,000 after inspections prompted by a complaint by the National Guestworker Alliance on the students' behalf. An Exel spokeswoman said the company plans to fight the findings. She said they involve only the co-packing area within the plant, and they mostly involve record-keeping.
Source: http://facilities.broadcastnewsroom.com/article/US-labor-agency-cites-Hershey-distribution-plant-1891039

21. *February 17, Food Safety News* – (California) **Raw milk dairy under investigation for Campylobacter outbreak.** Campylobacter may have struck yet another raw-milk dairy, Food Safety News reported February 17. Claravale Farm, one of the two state-licensed commercial raw milk dairies in California, is being investigated for the possibility that some of its milk was contaminated with Campylobacter, an infectious disease that can cause serious gastric problems and in some cases can be life-

threatening. An ongoing Campylobacter outbreak involving product from a Pennsylvania raw milk dairy has so far sickened at least 77. Claravale Dairy the week of February 20 voluntarily stopped distributing to the many stores that sell its products, which include cream and raw cow and goat milk. Its distribution area ranges from the Bay Area to San Diego. However, as of February 17, the dairy had not yet informed its customers, either through its Web site or its Facebook page, that it had stopped production. A spokesman for the state's public health department said the agency is working with local health departments on reported illnesses where raw milk was consumed. A spokesman for the state's agriculture department said the agency is aware of the action taken by Claravale and that tests of its products are pending. The department is also taking samples from the dairy itself. Results were still several days away, and the department had not taken any regulatory action.
Source: http://www.foodsafetynews.com/2012/02/campylobacter-investigation-at-cas-oldest-raw-milk-dairy/

For more stories, see items **7** and **14**

[Return to top]

Water Sector

22. *February 22, WABC 7 New York* – (New Jersey) **Boil water advisory in NJ after water main break.** A water main break in Woodbridge, New Jersey, February 22 prompted a boil water advisory for parts of the state. Middlesex Water Company issued the advisory for residents of the Fords, Avenel, and Woodbridge Proper sections of Woodbridge Township, and the Clara Barton section of Edison Township due to the broken 16-inch water main on Route 35, which caused service interruptions and loss of water pressure. Middlesex Water crews were working to restore water service to the area, however in the interim, customers may experience lower than normal water pressures.
Source:
http://abclocal.go.com/wabc/story?section=news/local/new_jersey&id=8553379

For more stories, see items **7** and **8**

[Return to top]

Public Health and Healthcare Sector

23. *February 22, Associated Press* – (California; Virginia) **Health officials warn of mercury in skin cream.** California health officials sent out a medical alert earlier this month after tracing the mercury poisoning of a 39-year-old Alameda County woman to an illegal skin-lightening cream smuggled in from Mexico, the Associated Press reported February 22. Health investigators are currently going undercover in some San Francisco Bay Area ethnic communities to root out the foreign-made products whose pigment-busting ingredient can have damaging health effects. The unlabeled jars of mercury-laced cream are typically used to lighten skin or fade freckles and age spots.

California officials worked with the U.S. Centers for Disease Control and Prevention in reporting last month that at least 22 people in five households in California and Virginia had shared skin-lightening creams made in Mexico. Twelve people in California and 10 in Virginia had elevated levels of mercury in their bloodstream.
Source: http://news.yahoo.com/health-officials-warn-mercury-skin-cream-081952327.html;_ylt=Al0WDyLfHQQ8cgAj2t74T4G3scB_;_ylu=X3oDMTQybjhyN2JuBG1pdANMYXRlc3ROZXdzIExpc3RpbmcEcGtnA2M4MmVmOGJhLThmMTMtMzVlNy1iZTIwLWQyYjczODhhNGVkOARwb3MDNjMEc2VjA01lZGlhU3RvcnlMaXN0BH

24. *February 21, Chinook Observer* – (Washington) **Hospital records burn in storage bldg fire.** An Ocean Beach Hospital storage site for old medical files in Ilwaco, Washington, caught fire February 15 causing an estimated $125,000 in damages, likely a total loss. The Ilwaco fire chief said the fire was fueled by the former residence's all-wood interior, as well as "the files stored floor to ceiling with old medical records in corrugated cardboard boxes." He added that he was unable to find any smoke alarms in the building. The chief believed the cause of the fire could have either been "... an electrical problem due to either some wires that are from the subpanel — in that house that was an old fuse box type panel," or "... that it was something that had to do with a baseboard heater that they claimed wasn't in use. But there was a lot of combustibles nearby."
Source: http://www.chinookobserver.com/news/hospital-records-burn-in-storage-bldg-fire/article_c52c99fa-5ce9-11e1-9617-0019bb2963f4.html

25. *February 18, Consumer Affairs* – (National) **Johnson & Johnson recalls Infants' Tylenol.** Johnson & Johnson's McNeil Consumer Healthcare is recalling about 574,000 bottles, of Infants' Tylenol Oral Suspension, 1-ounce Grape distributed nationwide in the United States, Consumer Affairs reported February 18. The company said it had received a "small number" of complaints from consumers who reported difficulty using a new dosing system. Called SimpleMeasure, the new system includes a dosing syringe, which a parent or caregiver inserts into a protective cover, or "flow restrictor," at the top of the bottle to measure the proper dose. In some cases, the flow restrictor was pushed into the bottle when inserting the syringe. No adverse events associated with this action have been reported to date and the risk of a serious adverse medical event is remote, the company said. Consumers can continue to use Infants' Tylenol provided the flow restrictor at the top of the bottle remains in place.
Source: http://www.consumeraffairs.com/recalls04/2012/johnson-johnson-recalls-infants-tylenol.html

For another story, see item **27**

[Return to top]

Government Facilities Sector

26. *February 22, Softpedia* – (International) **TeamHav0k finds XSS in British, French, and US government sites.** As Operation XSS, the operation launched by the grey hats

from TeamHav0k, continues, the hackers managed to identify cross-site scripting vulnerabilities in the official Web sites of governments from all over the world. Those countries included the United Kingdom, France, Brazil, and the United States in a statement by TeamHav0k, Softpedia reported February 22. Besides their statement, the post also contains a proof-of-concept to show that the site of France's Ministry of Agriculture, Food, Fishing, Rural, and Regional Development contains a major XSS flaw that can be utilized by an attacker to take over an unsuspecting user's session. A similar vulnerability was identified on the official site dedicated by the French government to outdoor sports. The domains owned by the Newport City Council and the Marine Accident Investigation Branch from Great Britain are on the list of potential victims. Finally, the U.S. site noted as being insecure belongs to the California Department of Pesticide Regulation, the organization that is in charge of monitoring the use of pesticide and its effects on public safety.
Source: http://news.softpedia.com/news/TeamHav0k-Finds-XSS-in-British-French-and-US-Government-Sites-254306.shtml

27. *February 21, Federal Computer Week* – (National) **VA performance dashboard failed to protect personal data, OIG says.** The Veterans Affairs Department wrongly allowed more than 20 employees and contractors access to veterans' sensitive personal and financial data in a recent information technology dashboard project, according to a new report from the Office of Inspector General. The security violation occurred in the VA's Systems to Drive Performance Dashboard while it was in development last year, the assistant inspector general for audits and evaluations wrote in the February 13 report. The VA dashboard was being created to track cost accounting data. In March 2011, the development team populated the dashboard with veterans' personally identifiable information, including birth date, age, sex, race, ethnicity, county of residence, zip code, and financial data. For the next 35 days, "more than 20 system users had inappropriate access to the sensitive data hosted in the Systems to Drive Performance development environment," the assistant inspector general wrote. In mid-April, access was terminated for most dashboard users. In addition to allowing inappropriate access, the VA did not handle user access requests consistently, and did not report the unauthorized access as a security violation as required. The problems were attributed to lack of awareness, failure to implement existing policies, and poor oversight.
Source: http://fcw.com/articles/2012/02/21/va-performance-dashboard-failed-to-protect-veterans-personal-data-oig-says.aspx

28. *February 17, WRAL 5 Raleigh* – (New York) **Ex-Bragg soldier arrested with 'arsenal' of stolen weapons.** A former soldier from the Fort Bragg U.S. Army base in Cumberland County, North Carolina, was arrested in the Bronx borough of New York City February 16, on charges he stole a cache of weapons from the military, authorities said. He was charged with one count each of theft of government property and unlicensed transportation of explosives. New York police searched an apartment in December 2011 and seized two grenades, six M-16 30-round magazines, two improvised explosive devices, four firearms, and other ammunition. Federal authorities said the man, who served in Iraq in 2006 and 2008, admitted to smuggling the weapons back to Fort Bragg in a shipping container after his last deployment. When he was

discharged in 2010, he arranged to transport them to New York.
Source: http://www.wral.com/news/news_briefs/story/10746165/

For another story, see item **39**

[Return to top]

Emergency Services Sector

29. *February 22, Macon Telegraph* – (Georgia) **Hospital patient steals ambulance, crashes into PTAP on 13th street.** A hospital patient accused of taking an ambulance from The Medical Center and crashing it into a 13th Street business February 20 did it because "the voices inside his head told him to steal the ambulance and wreck it," Columbus, Georgia police reports state. Police said the patient dragged a paramedic some 20 feet before he fled the hospital. The patient wrecked the ambulance moments later at an automobile accessory store. The crash did $115,000 in damage to the ambulance, $35,000 in damage to the building, and $80,000 in damage to a BMW on display in the showcase window. The suspect was arrested at the scene and is at the Muscogee County Jail pending a February 22 court hearing. He is charged with aggravated assault, theft by taking motor vehicle, second-degree criminal damage to property, and traffic violations, a police lieutenant said. He is being held without bond, jail officials stated.
Source: http://www.macon.com/2012/02/22/1914843/the-medical-center-hospital-patient.html

30. *February 21, CNET* – (California) **Hackers nip at LA police canine group.** Hackers February 21 released names, addresses, and phone numbers of more than 100 officers whose information was pilfered from the Web site of the Los Angeles County Police Canine Association (LACPCA). The LACPCA president confirmed to CNET the group's site was hacked and said that the FBI had notified him of the breach. The hackers did not identify themselves but referred to the "cabin," and the Twitter account of the hacker group CabinCrew publicized the data leak in a post February 21.
Source: http://news.cnet.com/8301-27080_3-57381992-245/hackers-nip-at-la-police-canine-group/?tag=mncol

[Return to top]

Information Technology Sector

31. *February 22, Softpedia* – (International) **XSS flaw in Skype Shop may allow hackers to steal user accounts.** A Georgian security researcher has identified major cross-site scripting (XSS) vulnerabilities on the Skype Shop Web site and in the Skype Application Programming Interface (API) site. The first site is the official Skype store where customers can purchase items including: headsets, phones, webcams, mobiles, and microphones. According to a blog post on the researcher's personal site, the XSS flaw discovered on these sites could allow an attacker to hijack cookies if she manages to convince the potential victim to click on a specially designed link. If exploited

successfully, a hacker could hijack the user's session and even steal his account. Given the large number of visitors the site has, the vulnerability can be cataloged as being a "high risk" issue. The vulnerabilities were reported to Skype and the company's representatives redirected it to Microsoft's Security Response Center, which now handles certain problems found in Skype.
Source: http://news.softpedia.com/news/XSS-Flaw-in-Skype-Shop-May-Allow-Hackers-to-Steal-User-Accounts-254437.shtml

32. *February 22, Help Net Security* – (International) **New Zeus/SpyEye makes bots function as C&C servers.** The latest build of the Zeus/SpyEye malware shows a change that could hamper security researchers' ability to take down the botnets using it and to track the criminals behind them. According to Symantec researchers, a previous build already moved towards replacing the bot-to-command and control (C&C) system with peer-to-peer capabilities so the bots receive configuration files from other bots, and this new one has finalized the transition. "This means that every peer in the botnet can act as a C&C server, while none of them really are one," said the researchers. "Bots are now capable of downloading commands, configuration files, and executables from other bots — every compromised computer is capable of providing data to the other bots." Apart from making such a botnet practically immune to a takedown, the move also has the added benefit of making the tracking and blocking of IP addresses of the C&C servers obsolete.
Source: http://www.net-security.org/malware_news.php?id=2009

33. *February 22, Softpedia* – (International) **'Dropper' trojan hijacks critical DLL file to avoid detection.** According to Bitdefender experts, the latest piece of malware, Trojan.Dropper.UAJ, hijacks a library file called comres.dll, and alters it to ensure that the malware steps into play each time it is being used. The dynamic link library (DLL) is utilized by many popular applications, including Web browsers, networking tools, and other apps that communicate online. Known as DLL load hijacking, this technique relies on the fact that many application are not programmed to use a certain library file, instead they utilize the one that is most accessible or placed in system folders. To ensure the success of this mechanism, Dropper makes a copy of the genuine comres.dll file, alters it, and then saves it in the Windows directory from where the operating system usually accesses it when needed. The trojan then drops a backdoor, identified by Bitdefender as Backdoor.Zxshell.B, which contains the code compromising the system. Once this is accomplished, cybercriminals can add and remove user files and rights, change passwords, and execute files with elevated privileges.
Source: http://news.softpedia.com/news/Dropper-Trojan-Hijacks-Critical-DLL-File-to-Avoid-Detection-254324.shtml

34. *February 21, InformationWeek* – (International) **Symantec pcAnywhere remote attack code surfaces.** Code has been published that attackers could use to crash fully patched versions of pcAnywhere on any Windows PC, without first having to authenticate to the PC. The exploit details were made public February 17 in a Pastebin post from Alert Logic's director of security research. Advertised as a "PCAnywhere Nuke," the Python code can be used to create a denial of service by crashing "the ashost32 service," he said. "It'll be respawned so if you want to be a real pain you'll

need to loop this ... my initial impressions are that controlling execution will be a pain." He said the exploit works even against the most recent, fully patched version of pcAnywhere (version 12.5.0 build 463 and earlier). "Symantec is aware of the posting and is investigating the claims," said a Symantec spokeswoman.
Source: http://www.informationweek.com/news/security/vulnerabilities/232601182

35. *February 20, Help Net Security* – (International) **Researchers break video CAPTCHAs, offer solutions.** After creating the "Decaptcha" software to solve audio CAPTCHAs, Standford University's researchers modified it and turned it against text and, more recently, video CAPTCHAs with considerable success. Video CAPTCHAs are touted by its developer, NuCaptcha, as the best and most secure method of spotting bots trying to pass themselves off as human users. Unfortunately for the company, the researchers managed to prove that more than 90 percent of the company's video CAPTCHAs can be decoded by using their Decaptcha software in conjunction with optical flow algorithms created by researchers in the computer vision field of study. One of the researchers shared the team's results and many details about their findings February 17, saying that while discussing ongoing research is unorthodox in the security community, the numerous interactions he had with various companies over the last 3 years made him realize many people rely on research results to design CAPTCHAs.
Source: http://www.net-security.org/secworld.php?id=12433

For more stories, see items **16**, **26**, **27**, **30**, **38**, and **40**

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

36. *February 22, Tallahassee Democrat* – (Florida) **Bird leads to cable outage.** Almost 3,000 Tallahassee, Florida residents were without cable February 22 after a bird interfered with a switch on a utility pole. At about 12 a.m., a bird interfered with a utility pole in the Buck Lake area of Tallahassee, an assistant to the city manager said. A Comcast representative said the city cleared the area at 5 a.m., which allowed Comcast to repair damage to the cable. She said Comcast originally believed the outage was caused by a squirrel's nest igniting. The fiber was cut when the pole was burned down, which led to a cable outage. The Comcast spokeswoman said it would be between 2 to 3 hours before the fiber was repaired due to the size of the cable.
Source: http://www.tallahassee.com/article/20120222/NEWS/120222003/Bird-leads-cable-outage

37. *February 22, CNET News* – (National) **Verizon customers hit by another 4G LTE outage.** Verizon's 4G services continue to suffer growing pains with another outage being reported February 22 by users in several different states. A few customers in Michigan, Arizona, and Virginia posted messages about outages via the Verizon discussion forums, while Engadget received reports of data coverage being down in Indianapolis, Milwaukee, Phoenix, Pennsylvania, and Ohio. A tweet from the company highlighted this latest issue: "VZW is investigating customer issues in connecting to the 4GLTE data network. 3G data, voice and text services are operating reliably." A Verizon spokesperson also confirmed the outage but said he had no further details. Though Verizon is claiming 3G data is unaffected, some commenters said otherwise. Engadget also said it heard from 3G customers reporting their service was down.
Source: http://news.cnet.com/8301-1023_3-57382686-93/verizon-customers-hit-by-another-4g-lte-outage/

38. *February 22, H Security* – (International) **Report: IPv6 sees first DDoS attacks.** Calling it a "milestone in IPv6 deployment," Arbor Networks noted respondents in its seventh annual Worldwide Infrastructure Security Report said they observed distributed distributed denial of service (DDoS) attacks on their IPv6 networks. The network monitoring and security provider said there are now enough IPv6 end-points to make launching a DDoS over IPv6 possible. Although the IPv6 DDoS attacks "in the wild" were a milestone, the report does note their rarity points to low IPv6 market penetration.
Source: http://www.h-online.com/security/news/item/Report-IPv6-sees-first-DDoS-attacks-1440502.html

39. *February 21, Daily North Salem* – (New York) **Phone service down in Somers, North Salem, Bedford.** Telephone service provided by LightPath, a division of Optimum, failed in some sections of Somers, North Salem, and Bedford, New York, February 21. In Somers, offices without telephone service include the town's offices, the parks and recreation department, and the Somers Library. As of 2:30 p.m., e-mail access was available and highway telephones were working. There was no indication of when power would be restored to the Lightpath phone lines. Meanwhile, in North Salem, phone service was also interrupted throughout the day February 21, according to a supervisor. The outage is due to a cut cable belonging to Optimum LightPath, a Bedford town clerk said. The company services the Westchester Telecom Network that manages communication in numerous Westchester County municipalities, including Bedford, North Salem, and Somers.
Source: http://www.thedailynorthsalem.com/news/phone-service-down-somers-north-salem-bedford

For another story, see item **31**

[Return to top]

Commercial Facilities Sector

40. *February 22, H Security* – (International) **Porn portal's user database open and accessible on the net.** Apparently, the user database of the videosz.com porn portal was openly available on the Internet. The VideosZ site offers adult customers the ability to download any available porn DVD for a fee of about $30. But a security hole allowed several hundred thousand data records of customers and affiliate partners, including such information as addresses, passwords, credit card details, and downloaded movies, to be accessed without password authentication. An anonymous reader of heise Security, The H's associate in Germany, had stumbled across an IP address that gave access to a server with an unprotected phpMyAdmin interface. Such servers are usually protected by a log-in procedure and can normally only be accessed from specific computers. In addition to customer data, the database also exposed the business data of VideosZ affiliates, and information on paid premiums. Heise Security informed the server operators of the problem, and access protection was implemented as a result.
Source: http://www.h-online.com/security/news/item/Porn-portal-s-user-database-open-and-accessible-on-the-net-1440233.html

41. *February 22, Associated Press* – (Georgia) **Police: Ga. victims related in Korean spa shooting.** A gunman shot two of his sisters and their husbands inside a Korean health spa in an Atlanta suburb and then killed himself, police said February 22. Surveillance video showed a man walking into the Su Jung Health Sauna February 21 and getting into an argument with someone, then opening fire, police said. The shootings happened in the salon area at the front of the building, the Norcross police chief said. Police recovered a .45-caliber gun at the salon. Four people were found dead inside, and another was taken to a hospital before being pronounced dead, investigators said. Investigators said they believe about 20 people were inside the spa when the gunfire began.
Source: http://www.statesman.com/news/nation/police-ga-victims-related-in-korean-spa-shooting-2192171.html

For more stories, see items **29** and **45**

[Return to top]

National Monuments and Icons Sector

42. *February 21, Associated Press* – (Arizona) **Grass fire burning in Arizona's Kaibab National Forest.** Crews from the U.S. Forest Service and the Ponderosa Fire Department were battling a grass fire about 3 miles northeast of Parks on the Williams District of the Kaibab National Forest in northern Arizona February 21. Forest Service officials said the so-called Rabbit Fire is approximately 90 acres and burning in the grass on the south side of Klostermeyer Hill in Government Prairie. Authorities said the cause of the fire is under investigation.

Source: http://www.abc15.com/dpp/news/region_northern_az/other/grass-fire-burning-in-arizonas-kaibab-national-forest

[Return to top]

Dams Sector

43. *February 22, KXXV 25 Waco* – (Texas) **Corps preparing safety program for Waco Dam.** A recent study by the U.S. Army Corps of Engineers classified the Waco Dam in Texas as having Moderate to High Risk characteristics, but said it is not in imminent danger of failing and is currently performing its intended function, according to KXXV 25 Waco February 22. Engineers from the Fort Worth District recently met with local cities and water utilities to discuss the Corps plan to improve safety at the dam. The risk informed screening process considers current dam behavior, how well the dam meets current design criteria, and the potential consequences of dam failure. Waco Dam's classification was a result of potential issues of seepage, piping, and erosion, according to the Corps.
Source: http://www.kxxv.com/story/16987966/corps-preparing-safety-program-for-waco-dam

44. *February 21, Stevens Point Journal* – (Wisconsin) **McDill Dam order ignored.** The village of Whiting, Wisconsin president knew about a 1999 letter that shows the McDill Pond Dam was built incorrectly but forged ahead with plans to get the structure repaired and ownership transferred from the village. In that letter, the Wisconsin Department of Natural Resources approved the permit for construction, but said concrete — not sand — had to be used under the box culvert. An inspection in September 2011 showed sand was used. The dam started leaking in June 2010, and McDill Pond remains drawn down as a result. The village president said he saw the letter but decided to ignore it to get the dam repaired and its ownership transferred.
Source: http://centralwisconsinhub.wausaudailyherald.com/article/20120221/SPJ0101/202210537/McDill-Dam-order-ignored?odyssey=tab|mostpopular|text|FRONTPAGE

45. *February 21, Gilroy Dispatch* – (California) **$75M shake-up, Anderson Dam fixes shoots up.** Although still in the planning stages, the potential price tag for the retrofit of Anderson Dam in Santa Clara County, California, was bumped up from $110 million to an estimated $185 million, the Gilroy Dispatch reported February 21. According to a seismic study completed in July 2011, Anderson Dam — which holds up to 90,373 acre-feet of water — was deemed unsafe, with the possibility that if a large earthquake struck within 1.25 miles of the dam, a 35-foot wall of water would rush to Morgan Hill and put it under water in 15 minutes, and flood Gilroy, San Martin, and the valley floor up to San Jose within a few hours. A Santa Clara Valley Water District spokesman said one factor in the higher estimate is outlet work not originally included. It will be done where the water is released from the dam, he said. During a preliminary study, four fault lines were found under the dam, said the acting senior engineer for the project.
Source: http://www.gilroydispatch.com/news/san_martin_county/m-shake-up-anderson-dam-fixes-shoots-up/article_0b0ca516-4c47-5f35-b94e-e87a14c716bd.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