Daily Open Source Infrastructure Report
20 March 2012

Top Stories

- Eight people were questioned on counterfeiting charges March 19 after they were found with $100 million in fake U.S. treasury bonds in Poland, authorities said. – *Associated Press* (See item **8**)
- A winter storm packing heavy snow and gusty winds forced authorities to close 180 miles of Interstate 40 in Arizona. The storm also closed schools and canceled flights in Arizona and New Mexico. – *CNN* (See items **18**, **2**)
- A report found the Washington, D.C. agency responsible for providing clean drinking water rigged lead-monitoring test results by not conducting tests in known problem areas. – *Washington Examiner* (See item **26**)
- Authorities in Johnston City, Illinois, issued a boil water order after two teenagers were arrested for climbing a water tower March 16. – *Associated Press* (See item **27**)
- The Los Angeles Fire Commission allocated emergency funds to fix glitches in the city's emergency response system that are delaying the dispatch of firefighters and paramedics. – *Associated Press* (See item **39**)
- A security researcher identified approximately 5 million Internet-accessible Remote Desktop Protocol (RDP) endpoints that are potentially vulnerable to a network worm exploiting a critical Microsoft vulnerability. – *Threatpost* (See item **45**)

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. *March 19, Skowhegan Morning Sentinel* – (Maine) **Powder blast sends woman to hospital.** One person was taken to a local hospital and several others were examined at the scene after a giant cloud of fire-suppression powder was released without warning at a gas station in Skowhegan, Maine, March 18. The powerful plume, emitted from about 50 hoses installed in the roof of the fuel-pumping area, covered vehicles, people, and the parking lot with a coating of white powder. The white-out obscured the busy station from view and briefly closed the road to motor vehicle traffic. The Skowhegan fire chief said the chemical was a nontoxic compound that can cause mild eye and throat irritation but is not life threatening. One woman was taken to the hospital by ambulance and two others went by private vehicle, all with respiratory complaints. The pump areas of the service station were closed after the incident.
Source: http://www.onlinesentinel.com/news/powder-blast-sends-woman-to-hospital_2012-03-18.html

2. *March 19, Associated Press* – (Arizona; New Mexico) **Winter storm, strong winds strike NM, Ariz.** A winter storm and high winds struck parts of Arizona and New Mexico March 18, causing hazardous driving conditions, power outages, and school cancellations. The fast moving storm forced the National Weather Service to place parts of northern New Mexico under a winter storm warning March 19 as heavy snow and wind from Arizona was expected to quickly blanket the area. The company PNM reported that 33,000 customers were out of power at one point March 19 in the Albuquerque area due to high winds. A spokesman for PNM said emergency crews were working to restore power, and by 9 p.m. the number without electricity was down to 4,500. Heavy winds and blowing dust forced the closure of parts of Interstate 10 in southern New Mexico due to low visibility, but the road was back open later in the day.

Source: http://www.lcsun-news.com/las_cruces-news/ci_20204901/winter-storm-strong-winds-strike-nm-ariz

3. *March 16, Houston Chronicle* – (Texas) **Regulators say Citgo plant leak ran for 5 months.** An alkylation unit at Citgo Petroleum Corp.'s refinery in Corpus Christi, Texas, was leaking for 5 months before spilling as much as 500 pounds of the hydrofluoric acid March 5, the U.S. Chemical Safety Board said March 16. Leaks from a flange on the unit occurred as early as September 2011, according to the statement from the board's lead investigator. The release persisted after maintenance and the unit was kept online while a clamp was redesigned. Water cannons were automatically activated to contain the chemical release, Citgo said March 6.
Source: http://www.chron.com/business/article/Regulators-say-Citgo-plant-leak-ran-for-5-months-3413966.php

For another story, see item **17**

[Return to top]

Chemical Industry Sector

4. *March 18, Arlington Heights Daily Herald* – (Illinois) **Pesticide spills when truck on Route 53 tips.** The ramp from westbound Lake-Cook Road to southbound Route 53 near Arlington Heights, Illinois, was closed for many hours after a truck carrying 36,000 pounds of pesticides overturned early March 18. "It is a hazardous material scene until they determine that nothing has been ruptured or leaked," said an Illinois State Police master sergeant. The semi rolled over in the left ditch along the ramp. The accident is under investigation.
Source: http://www.dailyherald.com/article/20120318/news/703189878/

For another story, see item **3**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

See item **33**

[Return to top]

Critical Manufacturing Sector

5. *March 19, KCPQ 13 Tacoma* – (Washington) **Everett dry dock sinks, causing 140-foot tug to capsize.** A 200-foot dry dock in Everett, Washington's Vigor Marine Shipyard sunk, causing a 140-foot tug boat to capsize March 18. The ship, Invader, had an estimated 50,000 to 60,000 of diesel fuel on board, according to the U.S. Coast Guard. The Coast Guard and department of ecology responded to monitor the salvage operation. The dry dock began sinking March 17 and continued to sink until it struck

the sea floor March 18. Both the dry dock and the Invader were partially submerged. The cause of the dry dock sinking was yet to be determined. In addition to the Invader, which was docked on the starboard side, the dry dock held paint, scissor lifts and a propane fork lift. A boom was deployed around the perimeter of the dry dock and tug to prevent leakage. A light sheen was reported on the surface of the water.
Source: http://www.q13fox.com/news/kcpq-everett-dry-dock-sinks-causing-140foot-tug-to-capsize-20120318,0,1601269.story

6. *March 19, U.S. Department of Labor* – (Louisiana) **U.S. Labor Department's OSHA fines Bradken Inc. for exposing workers to numerous safety and health hazards at Amite, La., foundry.** The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) March 19 cited Bradken Inc. with 27 serious and 7 other-than-serious violations for exposing workers to safety and health violations at the company's steel alloy casting facility in Amite, Louisiana. Inspectors found that workers melting and pouring casts were exposed to mechanical, welding, electrical, and confined space hazards, as well as a lack of machine guarding. Bradken, a global supplier headquartered in Australia, employs about 270 workers at the Amite facility who produce large steel alloy castings for the mining, freight rail, and steel industries worldwide.
Source:
http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=22011

7. *March 18, WRBL 3 Columbus* – (Georgia) **Fire at Kia supplier plant causes Kia Motors to halt production for two days.** A March 17 fire at a Kia supplier plant in West Point, Georgia, caused the car company to halt local production for 2 days. The Daehan facility makes insulation and noise reduction products for a nearby Kia plant. It took about 5 hours to contain the fire at the facility, which suffered a partial roof collapse and smoke damage. Five fire agencies and about 50 firefighters responded. While authorities were investigating the cause, some workers said they thought the fire was started by hot carpet, which is made at the plant and reaches over 100 degrees, that was not cooled off before it was thrown into a bin.
Source: http://www2.wrbl.com/news/2012/mar/18/fire-kia-supplier-plant-causes-kia-motors-halt-pro-ar-3435344/

[Return to top]

Defense Industrial Base Sector

See items **31** and **32**

[Return to top]

Banking and Finance Sector

8. *March 19, Associated Press* – (International) **Polish authorities seize $100 million in fake US treasury bonds, arrest 8 people.** Eight people are to be questioned on

counterfeiting charges March 19 after they were found with $100 million in fake U.S. treasury bonds in their possession, Polish authorities said. The central anti-corruption bureau, a state agency, said the suspects — three Poles, two Italians, two Ukrainians, and a Moldovan woman — were arrested March 18 in regions around Krakow and Lublin, in southern and eastern Poland. A bureau spokesman said the value of the fake bonds was a record seizure for the bureau. No other details were immediately available, and it was not clear if any fake bonds in the scam made it to the market.
Source: http://www.washingtonpost.com/world/europe/polish-authorities-seize-100-million-in-fake-us-treasury-bonds-arrest-8-people/2012/03/19/gIQA3gybMS_story.html

9. *March 19, Warren Tribune Chronicle* – (Florida; National) **Man to plead guilty in $14M Ponzi scheme.** A Florida man who founded a company that allegedly ran a $14.8 million Ponzi scheme that defrauded 100 investors in 9 states will plead guilty April 5, the Warren Tribune Chronicle reported March 19. He faces up to 20 years in prison and a $5 million fine on 30 counts of conspiracy, mail fraud, wire fraud, securities fraud, and money laundering. According to court records, he created and was the president of A&O Companies. The company's chief executive officer is facing similar charges and penalties. The indictment alleges that between 2006 and January 20, 2009, the two solicited investors to buy into their real estate ventures. Prosecutors claim they then used the money to pay for employees' salaries, personal expenses, and to pay off other investors, whom they promised between 20 and 45 percent interest. The men lied to investors, telling them their investment was secured through promissory notes and guaranteed through a lakefront Florida property, the indictment says. The property, however, was promised as collateral on more than $8 million in promissory notes, while the property was purchased for only $425,000. Once they issued the fraudulent notes, they paid some investors the promised interest payments "to give the false impression that there were actual investments," the charges state.
Source: http://www.tribtoday.com/page/content.detail/id/569420/Man-to-plead--guilty-in--14M--Ponzi-scheme.html?nav=5021

10. *March 19, Associated Press* – (Georgia; National) **FDIC sues ex-directors of troubled failed Ga. bank.** Federal bank regulators filed a lawsuit March 16 against 10 former directors and officers of a failed Georgia bank that collapsed and led to a wide-ranging criminal investigation and prison time for two of its top officials. The Federal Deposit Insurance Corporation's complaint accuses the former Omni National Bank officials of negligence and loose lending policies that led to the bank's March 2009 collapse. It seeks to recover more than $37 million in losses that included loans targeting low-income properties. It names several defendants who have already been charged criminally with their role in the bank's collapse. The bank's former vice president (VP) was sentenced to 5 years in prison in 2011 after pleading guilty to cooking the bank's books. Another Omni executive was sentenced to almost 2 years in prison on charges of taking bribes. The lawsuit claims the VP, executive, and five others approved loans for low-income properties despite "numerous, repeated, and obvious violations" of the bank's loan policies and procedures. It said the lenders allowed the use of straw borrowers, did not get proper appraisals, and did not make sure the borrowers had proper credit scores or the ability to repay the loans. It accused Omni's president and its

former chief executive of failing to supervise loan officers despite numerous "red flags," such as reports of prior misconduct by the VP. Between 2003 and 2008, the Atlanta-based bank expanded into seven states and its assets quadrupled to almost $1 billion, fueled mostly by a surge in real estate lending.
Source:
http://www.thenorthwestern.com/usatoday/article/38820037?odyssey=mod|newswell|text|FRONTPAGE|s

11. *March 19, Financial Industry Regulatory Authority* – (National) **FINRA fines Citi Financial $600,000 and orders restitution of $648,000 for excessive markups and markdowns.** The Financial Industry Regulatory Authority (FINRA) announced March 19 that it has fined Citi International Financial Services LLC, a subsidiary of Citigroup, Inc., $600,000 and ordered more than $648,000 in restitution and interest to more than 3,600 customers for charging excessive markups and markdowns on corporate and agency bond transactions, and for related supervisory violations. FINRA found that the markups and markdowns occurred from July 2007 through September 2010. They ranged from 2.73 percent to more than 10 percent, and were excessive given market conditions, the cost of executing the transactions, and the value of the services rendered to customers. In addition, from April 2009 through June 2009, Citi International failed to use reasonable diligence to buy or sell corporate bonds so that the resulting price to its customers was as favorable as possible. During the relevant period, Citi International's supervisory system regarding fixed income transactions contained significant deficiencies. Citi International was also ordered to revise its written supervisory procedures regarding review of markups and markdowns, and best execution in fixed income transactions.
Source:
http://www.finra.org/Newsroom/NewsReleases/2012/P125821?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+FINRANews+(FINRA+News)&utm_content=Google+Reader

12. *March 19, Associated Press* – (New York; National) **NY Mets owners settle in Ponzi-related case.** The owners of the New York Mets agreed to pay up to $162 million in a settlement announced March 19 with the trustee for fraud victims of a Ponzi scheme. The agreement was announced just as a civil trial was set to begin in a federal court in New York City to determine if the team's owners might owe as much as $386 million because they were among those who made significantly more than their original investment in the investment company linked to the scheme. The settlement does not require any money to be paid for at least 3 years. It also created the possibility the owners could owe nothing if they can secure $162 million of the $178 million they are seeking in claims of their own against the Ponzi schemer's estate. The trial was set to showcase what the trustee said was a conscious decision by the Mets owners to ignore warnings the head of the fund was operating a multibillion-dollar fraud over several decades, costing thousands of investors about $20 billion. A trustee originally sought $1 billion from the owners. The judges already had ruled the team's owners must pay up to $83.3 million in profits they received. That amount would now be included in the $162 million. There remain another 800 lawsuits pending against those who profited from their investments in the fraudulent scheme.

Source: http://www.google.com/hostednews/ap/article/ALeqM5hGeLVQ4bQAfa-HtH-JdPSB7T5N4A?docId=f2133627756b4a588af49bed7493437e

13. *March 19, PC Magazine* – (International) **Linkedin e-mail scam deposits banking trojan.** GFI Labs recently discovered a LinkedIn e-mail phishing scam that installs the Cridex banking Trojan. The fake LinkedIn e-mail looks like an authentic e-mail reminder about pending invitations. The phishing scam shares the same IP address (41.64.21.71) as several recent Better Business Bureau and Intuit spam runs. The Cridex bot, also known as Cardep or Dapato, was discovered in the wild in August 2011. It spreads through e-mailed or shared attachments. Once installed, the trojan connects to a remote command and control (C&C) server. Then it injects itself into the target's Internet Explorer process, where it steals online banking credentials, e-mail accounts, cookies, and FTP credentials, and sends them back to the C&C server. Earlier this month, M86 Labs reported that Cridex currently infects 25,000 machines.
Source: http://securitywatch.pcmag.com/security/295538-linkedin-email-scam-deposits-banking-trojan

14. *March 17, Associated Press* – (Nevada; National; International) **Feds say 19 arrested in 9 states in ID theft ring.** Nineteen people were arrested in Nevada and eight other states in a Las Vegas-based identity theft and trafficking ring that a federal prosecutor characterized as a sophisticated racketeering organization involving 50 people nationwide. The scheme revolved around the buying and selling of pilfered debit and credit card information on an Internet site called "Carder.su," a U.S. attorney said March 16. The Secret Service and U.S. Immigration and Customs Enforcement homeland security agents arrested five people March 15 in Las Vegas and 14 more in California, Florida, New York, Georgia, Michigan, New Jersey, Ohio, and West Virginia, according to the statement. The attorney said more arrests were expected as federal agents locate defendants named in three sealed indictments handed up by a federal grand jury in Las Vegas January 10 and March 13. The statement said charges include conspiracy, racketeering, and production and trafficking in false identification documents and access device cards. Members of the ring allegedly traded counterfeit documents and stolen bank account information on organization Web sites. Leaders of the organization allegedly tested and provided reviews of services, including money laundering, and products such as fake identification documents and stolen credit card account data lists from Europe, the Middle East, Asia, and the United States.
Source: http://www.foxnews.com/us/2012/03/17/feds-say-1-arrested-in-states-in-id-theft-ring/

15. *March 16, U.S. Government Accountability Office* – (National) **IRS needs to further enhance internal control over financial reporting and taxpayer data.** The Internal Revenue Service (IRS) implemented many controls and procedures intended to protect key financial and tax-processing systems; nevertheless, control weaknesses continue to jeopardize the confidentiality, integrity, and availability of financial and sensitive taxpayer data processed by agency systems, according to a Government Accountability Office statement March 16. Specifically, the IRS continues to face challenges in controlling access to its information resources. For example, it had not always (1) implemented controls for identifying and authenticating users, such as requiring users

to set new passwords after a prescribed period of time; (2) appropriately restricted access to certain servers; (3) ensured that sensitive data were encrypted when transmitted; (4) audited and monitored systems to ensure that unauthorized activities would be detected; or (5) ensured management validation of access to restricted areas. In addition, unpatched and outdated software exposed the agency to known vulnerabilities, and the IRS had not enforced backup procedures for a key system. Source: http://www.gao.gov/assets/590/589399.pdf

16. *March 16, WTVT 13 Tampa Bay* – (Florida; International) **Credit card fraud ring busted in Pinellas.** Authorities busted an international crime ring that had its headquarters in Pinellas County, Florida, WTVT 13 Tampa Bay reported March 16. The crimes involved luxury cars and credit cards. Authorities targeted 10 men, including the ring leader. The 3-year long joint operation involved the Pinellas County Sheriff's Office, the U.S. Secret Service, and the Florida Attorney General's Office.The alleged fraud totaled more than $3 million. Most of the suspects are originally from Bulgaria and Lithuania. The suspects were also accused of setting up phony corporations in Florida to run the cards and keep cash. The Pinellas County Sheriff said the men also made millions by taking out big dollar car loans to buy expensive vehicles with no intention of paying back the money. The cars were allegedly retailed in the state of Illinois and then shipped overseas and sold for double the price. Source: http://www.myfoxtampabay.com/dpp/news/local/pinellas/credit-card-fraud-ring-busted-in-pinellas-03162012

For another story, see item **43**

[Return to top]

Transportation Sector

17. *March 19, North Platte Telegraph* – (Nebraska) **Tornadoes hit Lincoln County; at least 2 injured.** At least two tornadoes hit the North Platte, Nebraska area March 18, injuring at least two people and damaging homes and power lines in its path. The Red Cross and Salvation Army opened an emergency shelter at the North Platte Recreation Center. Emergency management officials were searching for people who could have been injured. Some Dawson Public Power and Nebraska Public Power customers in and around North Platte were without power due to the damaged power lines. Union Pacific Railroad reported at least 15 train cars turned over by the storm, as well as damage to vehicles. Various reports indicated roads with downed power lines. Source: http://www.nptelegraph.com/breaking_news/article_0a0bdbe8-7181-11e1-96df-0019bb2963f4.html

18. *March 18, CNN* – (Arizona) **Winter storm closes 180 miles of AZ interstate.** A winter storm packing heavy snow and gusty winds forced authorities to close 180 miles of Interstate 40 in northern Arizona for many hours, March 18. The road was closed in both directions, said a dispatch supervisor for the Arizona Highway Patrol. The closure stretched roughly from Kingman in western Arizona to eastward to Winslow, including the city of Flagstaff, he said. Portions of Interstate 17 south of Flagstaff were also

closed, according to the Arizona Department of Transportation's Web site, as were several state roads. Flagstaff received 10 to 14 inches of snow, according to the National Weather Service. The city of Prescott had received 8 to 12 inches. Several crashes and reports of stuck vehicles had been reported as of March 18, with one person sustaining minor injuries on I-40. The Flagstaff Unified School District, Northern Arizona University Flagstaff campus, and Coconino Community College Flagstaff and Page campuses announced they would be closed March 19.
Source: http://fox8.com/2012/03/18/winter-storm-closes-180-miles-of-arizona-interstate/

19. *March 17, Los Angeles Times* – (California) **Gas thieves allegedly spark bus fire at Fontana day-care center.** Suspected gasoline thieves were believed to be responsible for a March 16 fire outside a San Bernardino County, California day-care facility that engulfed two school buses, the Los Angeles Times reported March 17. Investigators found a small pump and hoses near the scene in Fontana, said a statement from the San Bernardino County Fire Department. The equipment was probably intended to extract fuel from the tank of a vehicle, authorities said. Firefighters arrived and found the two small buses burning and threatening to spread to a third bus and the day-care center. The blaze was contained to the buses but caused minor damage to some playground equipment, said the news release. Investigators said the culprit was probably pumping fuel from one of the buses when a spark from the pump or the vehicle caused gasoline fumes to ignite. The fire caused about $80,000 in damage, authorities said.
Source: http://latimesblogs.latimes.com/lanow/2012/03/fontana-day-care-fire.html

20. *March 16, KDAF 33 Dallas* – (Texas) **Plane makes emergency landing at DFW airport after bomb threat.** The FBI is investigating a bomb threat on a United Express flight that landed at Dallas/Fort Worth International Airport (DFW) in Texas, March 16. United Express flight 5394 departed from Los Angeles International Airport carrying 66 passengers and crew. The Embraer ERJ 145 landed safely. The FBI said so far they did not have any suspects. The incident shut down one runway at DFW Airport, however, no other flights were affected.
Source: http://www.the33tv.com/news/kdaf-plane-makes-emergency-landing-at-dfw-airport-after-bomb-threat-20120316,0,2152847.story

21. *March 16, KIVI 6 Boise* – (Idaho) **Numerous reports of flooding across the state, as governor declares this Flood Awareness Week.** Reports of flooding were all across Idaho, KIVI 6 Boise reported March 16. The Weiser River was close to flood level. Valley County experienced significant flooding of roads and homes in low lying areas. There was significant flooding on Highway 55. Areas affected included Donnelly, McCall, New Meadows, Weiser, and Cascade.
Source: http://www.kivitv.com/news/local/142961175.html

For more stories, see items **1**, **2**, and **4**

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

22. *March 18, Bloomberg* – (International) **Fukushima farmers face decades of tainted crops as fears linger.** Farmers in Japan's Fukushima face years of additional losses as consumers continue to doubt the safety of produce from the region devastated a year ago by the tsunami and nuclear fallout, which may taint crops for decades. Almost 100,000 farmers lost about 58 billion yen ($694 million) by March 1, or 25 percent of production, according to JA, the country's biggest agricultural group. Imports of farm products jumped 16 percent to 5.58 trillion yen in 2011, according to the agriculture ministry. Inadequate testing by the government of rice, milk and fish from the region has prompted consumers to leave them on supermarket shelves and instead select produce from other regions or from overseas. Checks conducted nationwide so far are only 1 percent of what Belarus checked in the past year, a quarter century after the Chernobyl disaster, according to a researcher at Norinchukin Research Institute.
Source: http://www.bloomberg.com/news/2012-03-19/fukushima-farmers-face-decades-of-tainted-crops-as-fears-linger.html

23. *March 18, KWTX 10 Waco* – (Texas; Oklahoma) **Cattle rustling on the rise in Central Texas.** A spike in beef prices along with a smaller supply of cattle because of the drought is leading to an increase in cattle theft across much of central Texas, KWTX 10 Waco reported March 18. One bull can now go for close to $2,000 at auction, some of the highest prices ranchers have seen in years. "Cattle's one of the few items you can steal and get the same cash value for the next day," said a special ranger with the Texas and Southwestern Cattle Raisers Association. In the last year alone, special rangers tackled more than 1,000 cases in Texas and Oklahoma, a number that is expected to grow. Ranchers are taking extra precautions to make sure they do not become victims of cattle thieves, including old fashioned branding, liquid nitrogen branding, and microchipping to track livestock. "We have a 90 percent recovery rate on these cattle if they're branded," said a special ranger.
Source:
http://www.kwtx.com/home/headlines/Cattle_Rustling_on_the_Rise_in_Central_Texas_143274716.html

24. *March 17, United Press International* – (National) **Stink bugs threaten crops in U.S. South.** Two Mid-Atlantic hurricanes last year had the effect of pushing that region's invasive stink bug infestation into the deep south, U.S. Department of Agriculture scientists say. The Washington Post reported March 16 the brown marmorated stink bugs have headed south from Pennsylvania, Maryland, and West Virginia into South Carolina, Georgia, and Florida, putting vegetable and citrus crops at risk. Another type of stink bug is damaging soybeans and other legumes in Georgia. In 2010, they caused about $37 million in damage to mid-atlantic apple crops alone. Peach and raspberry

crops also took heavy hits in some parts of Maryland. Agriculture officials worry it could get worse once the bugs become established in Florida.
Source: http://www.upi.com/Science_News/2012/03/17/Stink-bugs-threaten-crops-in-US-South/UPI-74531332034124/

25. *March 16, KOIN 6 Portland* – (Oregon) **FBI investigating Ore. bird-farm vandalism.** The FBI is looking into the release of dozens of birds at an Oregon pheasant farm. The activist animal-rights group Animal Liberation Front (ALF) — a group that in the past took credit for the arson of an Oregon horse slaughterhouse — claims it is responsible for cutting the fence at the Queener Ridge Pheasant Co. in Scio the night of March 15. The ALF claimed responsibility in a message sent via North American Animal Liberation in Los Angeles. The Linn County Sheriff's Office released a statement saying deputies are investigating what it called "the illegal release of [Chinese Ring-Neck] pheasants from a local hunting ranch," March 16. It reports a holding pen was damaged and 75 to 100 birds escaped. The sheriff's office puts the initial damages at $4,000, including property damage and loss of its game fowls. An FBI spokeswoman said federal agents are looking into the incident.
Source: http://www.koinlocal6.com/news/local/story/FBI-investigating-Ore-bird-farm-vandalism/Oa65rKr-iEOw2o-FdTB-5w.cspx

For another story, see item **54**

[Return to top]

Water Sector

26. *March 19, Washington Examiner* – (Washington, D.C.) **D.C. covered up bad water quality tests, report says.** The Washington, D.C. agency responsible for providing clean drinking water throughout the city rigged its monitoring of lead in water by not conducting tests in parts of the city known for having higher lead levels, the District of Columbia inspector general (IG) found. The Washington Examiner reported March 19 that for a 26-month span beginning in July 2001, investigators found the D.C. Water and Sewer Authority (DCWASA) knew lead levels were elevated in the water system. Although it notified the Environmental Protection Administration (EPA) and began trying to remove excessive lead, the DCWASA also tried to cover up the extent of the crisis. "DCWASA sought to minimize the problem by sampling water from residences that were unlikely to have elevated lead levels, avoiding additional testing in areas of the District known to have elevated water lead test results," the IG wrote. Investigators also found that the DCWASA did not use approved testing methods throughout the city and that officials "provided misleading information" during hearings before the city council about lead levels. The EPA required the agency to test more residences to meet federal guidelines that mandated the city have 1,615 acceptable tests. It took the agency about 6,000 tests to meet that standard. A spokesman for the DCWASA said the agency had a leadership overhaul in 2009 and that past problems are not reflective of the agency's current performance. Scientists are not sure whether lead-laden water is to blame for the diagnoses of lead poisoning in some children in Washington, D.C.

Source: http://washingtonexaminer.com/local/dc/2012/03/dc-covered-bad-water-quality-tests-report-says/379566

27. *March 18, Associated Press* – (Illinois) **2 teenagers arrested in southern Illinois for climbing water tower, boil order issued.** Authorities in southern Illinois said two teenagers were arrested for allegedly climbing a water tower March 16. The Johnston City police chief said officers received a call around 11:45 p.m. with a report of a man on the tower. After authorities arrived and tried to get the teenagers down, a large glass alcohol bottle was thrown from the top of the tower. Authorities said emergency responders went up the tower and retrieved both teenagers with harnesses. Charges are pending. Officials in Johnston City issued a precautionary boil order after the incident since there was a possible breach of the water tank.
Source: http://www.therepublic.com/view/story/18df6358a1784217b0fa75d6824de0e9/IL--Water-Tower-Arrests/

28. *March 16, KPIC 19 Roseburg* – (Oregon) **Sewage again spilling into Cow Creek.** Recent heavy rainfall caused the Glendale Wastewater Plant to be inundated with a surge of storm water, KPIC 19 Roseburg reported March 16. The facility was bypassing 208 gallons a minute of raw sewage and storm water into Cow Creek. The spill began around 2 a.m., and the Glendale Public Works superintendent expected it to end by March 17. The facility has bypassed unsanitary water at least once every year for the past decade. Residents were urged not to drink, bathe or swim in Cow Creek below the plant.
Source: http://www.kpic.com/news/health/Sewage-again-spilling-into-Cow-Creek-142960215.html

For another story, see item **5**

[Return to top]

Public Health and Healthcare Sector

29. *March 18, Petersburg Progress-Index* – (Virginia) **Adult care center evacuated after bomb scare.** A Petersburg, Virginia assisted living facility was evacuated as Virginia State Police responded to a bomb scare March 17. An employee reported a suspicious looking package and called 911. Petersburg police requested assistance from the Virginia State Police Bureau of Criminal Investigation Richmond Field Office Bomb Unit. Police roped off and evacuated the building. Staff and about 50 residents spent hours waiting outside in a nearby parking lot, while members of the bomb squad swept the facility. Six hours later police detonated the package. Following an investigation of the pieces, it was determined that the package did not contain any explosives.
Source: http://progress-index.com/news/adult-care-center-evacuated-after-bomb-scare-1.1287351#axzz1pZPHY3E3

30. *March 16, WEAR 3 Pensacola* – (Florida) **Navy hospital evacuated early Friday.** There was a Freon leak at the naval hospital in Pensacola, Florida, March 16,

prompting dozens of people to be evacuated. It was caused when crews, working on wiring beneath the floor in a computer room, nicked a copper wire for the air conditioning system. About 60 people in the immediate area were evacuated. Thirteen people were treated for exposure, and two of them were admitted for further evaluation. The leak was contained to staff areas only and no patients were impacted.
Source: http://www.weartv.com/newsroom/top_stories/videos/wear_vid_21219.shtml

[Return to top]

Government Facilities Sector

31. *March 19, Help Net Security* – (National) **US govt. and military e-mail addresses offered for sale.** Webroot recently unearthed an offer for sale of millions of e-mail addresses harvested by a cybercrime underground service, which has cleverly segmented the database based on country or generic top-level domains, Help Net Security reported March 19. "Next to mass marketing campaigns, the segmented databases could be used for launching targeted attacks against a particular country, which in combination with localization — translating the spam message into the native language of the prospective recipient — and event-based social engineering attacks, could increase the probability of successful interaction with the malicious e-mails," a security expert at Webroot said. He also advised U.S. government and military users to be especially careful when considering the legitimacy of received e-mails, as among the e-mail addresses offered for sale are over 2 million on .gov and .mil domains.
Source: http://www.net-security.org/secworld.php?id=12611

32. *March 19, Associated Press* – (International) **AF's delicate rescue saves stranded $1.7B satellite.** U.S. Air Force ground controllers rescued a $1.7 billion military communications satellite last year that had been stranded in the wrong orbit and at risk of blowing up — possibly because a piece of cloth had been left in a critical fuel line during manufacture, the Associated Press reported March 19. During the 14-month effort, the satellite had to battle gravity and dodge space junk while controllers improvised ways to coax it more than 21,000 miles higher to its planned orbit. "This rescue effort was definitely a very sophisticated and highly technical masterpiece," said the chief of the Military Satellite Communications Division at Peterson Air Force Base, Colorado. The Advanced Extremely High Frequency (AEHF) satellite is the first of six in a $14 billion communications system. Lockheed Martin, expected to build all six AEHF satellites, said the probable cause was a foreign object that got into the system during manufacture. The Air Force said the next two AEHF satellites have been inspected and additional checks have been added to the manufacturing process for the remaining versions.
Source: http://www.military.com/news/article/af-delicate-rescue-saves-stranded-17-billion-satellite.html

33. *March 19, Global Security Newswire* – (Washington, D.C.) **'Small' nuclear blast would devastate downtown D.C., FEMA says.** The U.S. Federal Emergency Management Agency concluded that a 10-kiloton nuclear blast 3 blocks north of the White House in Washington, D.C. would wipe out the Presidential complex as well as

the U.S. Capitol, National Mall, and other structures within one half of a mile, the Washington Post reported March 16. The potential for terrorists to acquire and use a nuclear weapon has been identified as a major threat facing the United States and its partners. A relatively "small" nuclear explosion would eliminate most life and generate harsh radioactivity within that "severe damage zone," the newspaper quoted the November 2011 assessment as saying. The bomb would produce more limited physical effects — such as insubstantial wounds and compromised windows — in an area starting no less than 3 miles from the blast point, according to the document, which is located at http://www.fas.org/irp/agency/dhs/fema/ncr.pdf
Source: http://www.nti.org/gsn/article/small-nuclear-blast-would-devastate-downtown-dc-report/

34. *March 16, Associated Press* – (National) **FBI says retaliation attacks possible in US.** An FBI spokeswoman in Seattle said the agency and the DHS issued a bulletin March 15 to raise awareness about the possibility of homegrown extremist retaliation in response to the killings of civilians in Afghanistan. A soldier from Joint Base Lewis-McChord near Tacoma, Washington, was accused of the shootings. The spokeswoman said there was no specific target or credible information about an imminent attack. However, she said the FBI has previously seen extremists plot attacks in retaliation for the actions of soldiers. They include a plot last year to attack a military recruit processing station in Seattle.
Source:
http://seattletimes.nwsource.com/html/localnews/2017762767_apwaafghanistanretaliation.html

35. *March 16, NextGov* – (National) **OMB: Growth in federal cyberattacks slows.** NextGov reported March 16 that cyberattacks on the U.S. government continue to increase, but most were "phishing" attempts and reports of threats largely leveled out in the past year, according to the Office of Management and Budget (OMB). OMB reported a 5 percent increase in cyberattacks on federal networks in 2011, based on reports to the U.S. Computer Emergency Readiness Team. That is compared to a 39 percent spike in such attacks the previous fiscal year. "Threats to this IT infrastructure — whether from insider threat, criminal elements, or nation-states — continue to grow in number and sophistication, creating risks to the reliable functioning of our government," the report concluded. Of the total 107,655 attacks reported in 2011, 43,889 were aimed at federal departments and agencies.
Source: http://www.nextgov.com/nextgov/ng_20120316_7803.php

36. *March 16, Government Computer News* – (National) **Agencies way behind in using DNSSEC to secure .gov domains.** More than 2 years after the deadline for deploying the DNS Security Extensions in .gov domains, fewer than 60 percent of agencies have digitally signed their records in the Domain Name System, according to a study by Secure64 Software Corp. The company queried Web sites for 359 agencies and found that 205 of them, about 57 percent, had implemented the signatures. The marketing vice president for the security company said it is primarily smaller agencies that are not yet using DNSSEC, and that the delay could be caused by a combination of lack of awareness and lack of resources.

Source: http://gcn.com/articles/2012/03/16/agencies-lag-in-dnssec-security-deployment.aspx

For more stories, see items **2** and **18**

[Return to top]

Emergency Services Sector

37. *March 19, WJXT 4 Jacksonville* – (Florida) **Correctional officer killed by inmate.** A department of corrections officer was stabbed to death by an inmate March 18 at a state prison near Lake City, Florida. The secretary of the department of corrections told WJXT 4 Jacksonville, the sergeant was attacked by an inmate at the Columbia Correctional Institute annex. The secretary said the sergeant was in one of the wings of a dorm checking on an inmate when a control room officer saw the inmate chase and then stab the sergeant several times in the neck with a handmade weapon. He was taken to a nearby hospital where he died. The secretary also said a second officer was trying to lock down inmates when the inmate swung something heavy in a sock, striking him in the eye. The officer was also taken to a hospital, where he was treated and released. The inmate will be transferred to a maximum security prison and the incident will be investigated by the Florida Department of Law Enforcement.
Source: http://www.news4jax.com/news/Correctional-officer-killed-by-inmate/-/475880/9516006/-/11lp7xa/-/index.html?hpt=ju_bn4

38. *March 18, Rapid City Journal* – (South Dakota) **Three injured after police cars collide.** Two patrol cars collided in Aberdeen, South Dakota March 18, injuring three people, according to the South Dakota Department of Public Safety. The Aberdeen Police Department patrol vehicles crashed at an intersection while responding to assist another officer with a fleeing suspect. One officer and his passenger were taken to a nearby hospital with serious injuries. The other officer also went to the hospital to be treated for minor injuries. The South Dakota Highway Patrol is investigating. Brown County Sheriff's Office and the Aberdeen Police Department assisted. The accident remains under investigation.
Source: http://rapidcityjournal.com/news/three-injured-after-police-cars-collide/article_f0baa5dc-715a-11e1-b17e-001871e3ce6c.html

39. *March 18, Associated Press* – (California) **LA fire agency to fix emergency dispatch glitches.** The Los Angeles Fire Commission allocated emergency funds to fix glitches in the city's emergency response system that are delaying the dispatch of firefighters and paramedics, the Associated Press reported March 18. The Los Angeles Times reported March 18 that a woman bled profusely for 45 minutes March 7, while waiting for paramedics after a factory machine sliced off one finger and mangled the others. The delay was caused by a brief failure in the fire department's dispatching system. Firefighters said the system problems are recurring and have created confusion at fire stations, forcing dispatchers to deploy old backup plans. The fire commission president said the panel planned to address equipment breakdowns and response times at its meeting March 20. Officials said the dispatching system is aging and was recently

moved.
Source: http://www.fresnobee.com/2012/03/18/2766001/la-fire-agency-to-fix-emergency.html

40. *March 17, Dearborn Press & Guide* – (Michigan) **Sentences reduced for 227 inmates in overcrowded Oakland County Jail.** A state of emergency regarding overcrowding at Oakland County Jail in Pontiac, Michigan, was declared by the Oakland County sheriff. This prompted the a chief circuit judge to order sentence reductions for 227 inmates to alleviate the situation, officials announced March 16. The sheriff declared the state of emergency March 2. By law, the declaration meant mandatory sentence reductions for inmates who would not present a high risk to public safety, a press release from the Oakland County Circuit Court stated. Both misdemeanor and felony sentences were reduced, but inmates sentenced on assaults or drunk driving charges did not have their sentences reduced, the release stated. Inmates were also screened for pending warrants from other counties and parole violations in other jurisdictions. The sentence reductions were handed down March 16, and many inmates were scheduled to be released as early as March 17. A spokesman from the Oakland County Circuit Court estimated that more than 100 inmates would be released the weekend of March 17.
Source: http://www.pressandguide.com/articles/2012/03/17/news/doc4f649c3f8bef0009286665.txt?viewmode=fullstory

41. *March 15, ABC News* – (California; International) **Car blows up after Border Patrol chase near Mexican border.** The driver has died and a Border Patrol agent has been airlifted to the hospital after a car being chased by the Border Patrol near the Mexican border exploded when it was forced to stop. Early March 15 in eastern San Diego County, Customs and Border Patrol (CBP) agents spotted a car with Texas plates driving the wrong way down the highway. Police sources said the vehicle blew through a checkpoint and agents gave chase. Agents used a spike strip to deflate the vehicle's tires, and the driver came to a stop 10 miles north of the border and 40 miles east of San Diego. When one of the agents approached the car, the driver refused to open the door or the driver's side window. The agent then attempted to break the window, at which point the vehicle exploded and was engulfed in flames. The agent was knocked to the ground and received lacerations and burns to the face and body. The sole occupant of the vehicle died in the fire. Authorities have not yet determined what caused the fire, and whether explosives were involved. The San Diego Sheriff's Department bomb and arson team is investigating.
Source: http://abcnews.go.com/Blotter/car-blows-border-patrol-chase-mexican-border/story?id=15927662#.T2c7t3keheY

For another story, see item **54**

[Return to top]

Information Technology Sector

42. *March 19, IDG News Service* – (International) **New iPad model has already been jailbroken.** Hackers claimed to have figured out a way to bypass Apple's technical restrictions and install unauthorized applications on the company's latest iPad upon its release March 16. Apple forbids installing applications it has not approved, but hackers have found ways to "jailbreak" devices, or modify the code to allow unauthorized programs from alternative application stores.
Source:
http://www.computerworld.com/s/article/9225306/New_iPad_model_has_already_been_jailbroken?taxonomyId=17

43. *March 19, IDG News Service* – (International) **Java-based Web attack installs hard-to-detect malware in RAM.** Malware that does not create any files on the affected systems was installed onto the computers of visitors to news sites in Russia in a drive-by download attack, according to Kaspersky Lab. The attack code loaded an exploit for a known Java vulnerability, but it was not hosted on the affected Web sites themselves. Instead, it was served to their visitors through banners displayed by a third-party advertising service. The Java exploit's payload consisted of a rogue dynamic-link library (DLL) loaded and attached on the fly to the legitimate Java process. This type of malware is rare, because it dies when the system is rebooted and the memory is cleared. The malicious DLL loaded into memory acted as a bot, sending data to and receiving instructions from a command and control server over HTTP. In some cases, the instructions given out by attackers were to install an online banking trojan on the compromised computers. "This attack targeted Russian users. However, we cannot rule out that the same exploit and the same fileless bot will be used against people in other parts of the world: They can be distributed via similar banner or teaser networks in other countries," the researcher said.
Source:
http://www.computerworld.com/s/article/9225300/Java_based_Web_attack_installs_hard_to_detect_malware_in_RAM?taxonomyId=17

44. *March 19, H Security* – (International) **VLC Media Player 2.0.1 closes security holes.** Version 2.0.1 of the open source VLC Media Player has been released, H Security reported March 19. According to a VideoLAN developer, the maintenance update to VLC 2.0 "Twoflower" includes fixes for more than 110 bugs and closes 2 security holes that could be exploited by an attacker to compromise a victim's system. The update addresses a stack overflow in MMS support as well as a heap-based buffer overflow in Real RTSP support which, its developers say, could lead to arbitrary code execution on most systems. For an attack to be successful, a user must first open a specially crafted file or a malicious Web site. All VLC versions up to and including 2.0.0 are affected; upgrading to 2.0.1 fixes these issues.
Source: http://www.h-online.com/security/news/item/VLC-Media-Player-2-0-1-closes-security-holes-1474770.html

45. *March 19, Threatpost* – (International) **Researcher says 5 million machines exposing RDP service online.** A network security researcher scanned a large part of the Internet

in the wake of the release of the patch for the Remote Desktop Protocol (RDP) bug and the publication of exploit code. He started the scan March 16 and hit 300 million IP addresses. He found there were about 415,000 machines communicating using part of the RDP protocol. "Extrapolating from this sample, we can see that there's approximately 5 million RDP endpoints on the Internet today ... it's pretty clear that, yes, RDP is actually an enormously deployed service, across most networks in the world," he said. "There's something larger going on, and it's the relevance of a bug on what can be possibly called the Critical Server Attack Surface. Not all bugs are equally dangerous ... but some flaws are simply more accessible, and RDP — as the primary mechanism by which Windows systems are remotely administered — is a lot more accessible than a lot of people were aware of." RDP is used widely in enterprise networks and small business environments for remote management of machines. In larger networks that have tight administration and regular patching programs and schedules, the bug likely will be addressed quickly, whether through patching or by disabling RDP on machines if it is unnecessary. Some percentage of those machines were already patched, as the fix has been out now for almost a week. However, in smaller networks that may not have a full-time administrator or IT staff, the problem is more problematic. If the business owners do not even know RDP is enabled or what it is for, they may also not realize the importance of patching the vulnerability. That leaves a large potential target base for attackers, even if the majority of enterprise administrators patch their vulnerable machines.
Source: http://threatpost.com/en_us/blogs/researcher-says-5-million-machines-exposing-rdp-service-online-031912

46. *March 18, Computerworld* – (International) **Microsoft blames security info-sharing program for attack code leak.** March 16, Microsoft confirmed sample attack code created by the company likely leaked to hackers from a program it runs with antivirus vendors. "Details of the proof-of-concept code appear to match the vulnerability information shared with Microsoft Active Protection Program (MAPP) partners," a director with Microsoft's Trustworthy Computing group said in a statement. "Microsoft is actively investigating the disclosure of these details and will take the necessary actions to protect customers and ensure that confidential information we share is protected pursuant to our contracts and program requirements," he added. Under the MAPP, Microsoft provides select antivirus companies with technical information about bugs before Microsoft patches the flaws. It is meant to give third-party security vendors advance warning so they can craft detection signatures. Among the things Microsoft shares with MAPP members, according to a program FAQ, are "proof-of-concept or repro tools that further illuminate the issue and help with additional protection enhancement." The acknowledgment by Microsoft was prompted by claims earlier in the day by the Italian researcher who reported the vulnerability in Windows Remote Desktop Protocol in May 2011.
Source:
http://www.computerworld.com/s/article/9225293/Microsoft_blames_security_info_sharing_program_for_attack_code_leak?taxonomyId=17

47. *March 16, Infosecurity* – (International) **New Imuler trojan variant for the Mac disguises itself as image file.** A new version of the Imuler trojan is disguising itself as

image files, according to Intego, which first discovered the Trojan September 2011. Intego found two samples of the new version, designated as Imuler.C, on the VirusTotal Web site, which is used by security companies to share malware samples. In both samples, an application was included with an icon making it look like an image. Intego said the technique "takes advantage of a default setting in the Mac OS X Finder, whereby file extensions are not displayed. Users double-clicking on the application launch the malware, which quickly deletes itself, replacing the original application with a real JPEG image corresponding to the one that was an application, and displays this image in the user's default image viewer. There is no visible trace of the application after this point." The malware then installs a backdoor. "This malware searches for user data, and attempts to upload it. It also takes screenshots and sends them to the server. It creates a unique identifier for the specific Mac to be able to link the Mac and the data it collects. We have seen this malware is active, as it connects to a remote server and downloads new executables," Intego related.
Source: http://www.infosecurity-magazine.com/view/24606/

48. *March 15, V3.co.uk* – (International) **Symantec warns of 64-bit Windows trojans.** Symantec warned of a new Windows 7 trojan that can elevate the privileges of any restricted process to administrator level, without the user's permission or knowledge. The latest fully patched versions of Windows 7 are vulnerable to the backdoor.Conpee trojan, warned a security response engineer at Symantec. The new trojan targets 32-bit and 64-bit versions of Windows 7, adding to the growing weight of evidence that malware writers are redesigning their software to bypass security features in 64-bit Windows, he said. The 64-bit version of Windows 7 and Vista included Kernel Mode Code Signing and Kernel Patch Protection, intended to make them less vulnerable to malware. But backdoor.Conpee and the recently-discovered Backdoor.Hackersdoor trojan have both been shown to infect 64-bit operating systems, the researcher said. "What was just a theory not so long ago is now being used in-the-wild by [these] threats," he warned. The Hackersdoor trojan is able to bypass the driver signing system used in 64-bit Windows using stolen certificates. Symantec first detected this type of infection in December 2011, and while the number of infections seen in the wild since then have been modest, it appears the malware writers have been using it as a test case, the researcher added.
Source: http://www.v3.co.uk/v3-uk/news/2159725/symantec-warns-bit-windows-trojans

For more stories, see items **13**, **14**, **15**, **31**, **35**, **36**, and **39**

Internet Alert Dashboard

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

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

[Return to top]

Communications Sector

See items **31** and **42**

[Return to top]

Commercial Facilities Sector

49. *March 19, Anderson Herald-Bulletin* – (Indiana) **Two injured in meth lab explosion at Days Inn.** A man was critically injured in a methamphetamine explosion March 17 at an Anderson, Indiana hotel. Police were continuing to investigate the incident that also injured a woman. Firefighters quickly extinguished the blaze and, along with the help of hotel staff, evacuated the Days Inn. Police found the injured man in a nearby parking lot. He told officers he was cooking meth when it exploded causing a "red-hot glowing fire." He suffered severe burns to his arms, hands, and neck. The injured woman was found nearby with burns to her arm. Both were transported to a hospital. The incident was being investigated by the Madison County Drug Task Force. Members of the task force decontaminated the room where the meth was being made. Fire damage was limited to that one room, and no one else was injured. The remainder of the hotel was unaffected by the fire, and guests were allowed to return to their rooms, a hotel employee said.
Source: http://www.firefightingnews.com/article-us.cfm?articleID=103768

50. *March 19, WLS-TV 7 Chicago* – (Illinois) **Fire takes over North Chicago buildings.** Nearly a dozen people were left homeless after a major fire in North Chicago, Illinois, March 18. Two auto body shops and an apartment building were involved. One of the auto body shop buildings collapsed. The apartment building also collapsed partially, but no one was hurt. There was no word March 19 on what caused the fire.
Source: http://abclocal.go.com/wls/story?section=news/local&id=8586243

51. *March 18, KTRK 13 Houston* – (Texas) **ATF agents investigating flea market fire.** Federal investigators are now part of the effort to find out what led to a flea market fire in the Channelview section of Harris County, Texas, the week of March 12. The White Elephant Flea Market burned to the ground March 16. Agents with the Bureau of Alcohol, Tobacco, Firearms and Explosives National Response Team were at the scene to investigate. Authorities called the three-alarm fire suspicious because someone broke into two adjacent buildings, and three people were seen leaving the area when it started. About 100 booths were damaged in the blaze. Investigators estimated the fire caused $750,000 worth of damage.
Source: http://abclocal.go.com/ktrk/story?section=news/local&id=8585522

52. *March 18, Reuters* – (New York) **Dozens arrested at Occupy's 6-month anniversary rally.** Dozens of Occupy Wall Street protesters were arrested during the weekend of March 17 as police cleared New York City's Zuccotti Park, where demonstrators had gathered for the movement's 6-month anniversary. The park remained closed March 18 with a sprinkling of police surrounding it, keeping the area clear while crews cleaned

up following the March 17 protests. A sweep just before midnight, when roughly 300 demonstrators had gathered in the park, capped a day of protests and marching in lower Manhattan. The New York City Police Department said it arrested 73 protesters during the weekend.
Source: http://www.reuters.com/article/2012/03/18/us-usa-occupy-wallstreet-idUSBRE82G0FC20120318

53. *March 16, KOTV 6 Tulsa* – (Oklahoma) **TFD: Tulsa hardware store fire set to steal meth-making chemicals.** Tulsa, Oklahoma arson investigators are looking for two people who may have started a bathroom fire as a distraction to steal meth making chemicals from an Ace Hardware store March 16. Fire crews responded and quickly extinguished the fire before it spread to the rest of the store. The fire department released surveillance images of two people they believe may be involved with the fire.
Source: http://www.newson6.com/story/17179307/bathroom-fire-used-to-steal-meth-making-chemicals

For more stories, see items **19** and **33**

[Return to top]

National Monuments and Icons Sector

54. *March 19, KUSA 9 Denver* – (Colorado) **Yuma County fire: Fire in Yuma County contained.** The Heartstrong Fire that burned in Yuma County, Colorado since the afternoon of March 18, was completely contained by the afternoon of March 19, KUSA 9 Denver reported. Some residents of Eckley were allowed to return home late March 18. The rest of the residents living in the 224-square-mile area were allowed to return home early March 19. The Yuma County sheriff said the fire scorced 2,400 acres. He said there was no estimate on how many livestock were lost or the cost of the damage. Two homes were destroyed, and three firefighters from Yuma County were injured. Two of the firefighters were hospitalized overnight. The Yuma Pioneer newspaper said a downed power line caused the blaze.
Source: http://www.9news.com/news/article/257294/222/Fire-in-Yuma-County-now-90-percent-contained

[Return to top]

Dams Sector

55. *March 18, Hudson Valley Your News Now* – (New York) **Asher Dam repairs.** Repairs on the Asher Dam in the village of Rhinebeck, New York, is expected to fix damage from the summer of 2011 storms. The mayor said March 18 there was significant damage to the valves at the dam after tropical storms Irene and Lee, and they could only be accessed by going into the lake. With the repairs and redesign there will be no further risk of damage. The mayor said the project will take about a week to complete, and when finished, they will be able to manage the water level and see improvements

in the drainage issues upstream.
Source: http://hudsonvalley.ynn.com/content/top_stories/577485/asher-dam-repairs/

56. *March 17, Omaha World-Herald* – (South Dakota; Midwest) **Repairs needed on river dams.** Among the estimated $10.5 million in repairs planned for Gavins Point Dam near Yanton, South Dakota, is replacing broken or missing cast-iron spillway grates. Twenty are known to be broken or missing and more than 200 others are under water and will be inspected in March. Corps officials have identified 122 repairs to be done in 2012 following the 2011 flooding. The cost is estimated at more than $186.3 million — plus approximately $54.5 million the following 2 years — at Fort Peck, Garrison, Oahe, Big Bend, Fort Randall, and Gavins Point Dams. Officials primary concerns at Gavins Point include the condition of the spillway's concrete slabs, bank degradation, and restricted flows through the power plant. Peak releases at Gavins Point during the summer-long flood reached 160,000 cubic feet per second — more than twice the previous record, in 1997. High flows scoured away 12 feet of river bottom along a 1,200-yard stretch of the north bank downstream from the dam. That piece of shoreline functions as a dike separating the dam's outflows from Lake Yankton. The lost rock and soil is significant because it could allow seepage from the lake into the river and threaten the dike's integrity. The river side of the dike will be armored with rock the summer of 2012 to prevent future erosion and degradation. Trees and marsh debris coming down Lewis and Clark Lake will plague the Gavins Point power plant for 2 or 3 more years, officials said. Cleanup of the debris is scheduled to begin the week of March 19.
Source: http://www.omaha.com/article/20120317/NEWS01/703179897

57. *March 16, St. Joseph News Press* – (Missouri) **Berm project aims to help flood control.** A $ 1 million-plus project will move about 175,000 cubic yards of dirt and sand to build five berms to ensure the Elwood Gladden and Lake Contrary levees can withstand the next Missouri River flood, a senior project engineer for the project said. The St. Joseph New-Press reported March 16 that the five sand berms are based on flood-fight lessons learned from flooding in 2011. In all five areas, there was an aggressive fight against sand boils, some of which were 6 feet in diameter and were moving a lot of levee material during the summer of 2011. Employees were collecting dirt along drainage ditches and other areas on the outside of the levee to provide the materials needed to build the berms. Removing dirt from drainage ditches will improve the future flow of water. The Corps plans to sew native grasses into the scour hole area after it is filled. Removed rocks will be used to armor the levee's river side. It will also reduce the incidents of wildlife using the levee for burrows. The Corps announced March 16 that a contractor completed work on the Rushville-Sugar Lake Levee, located between southwestern Buchanan and northwestern Platte counties in Missouri. The $1.3 million project began January 30.
Source: http://www.newspressnow.com/localnews/30699025/detail.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