Homeland Security

Daily Open Source Infrastructure Report for 19 May 2011

Top Stories

- Associated Press reports the U.S. Coast Guard May 17 shut down for many hours a 15-mile stretch of the swollen Mississippi River near Natchez, Mississippi, idling barges carrying everything from coal and steel to half of America's grain exports. (See item **16**)
- According to WCHM, the U.S. Drug Enforcement Administration suspended the prescription-dispensing licenses of four physicians and a pharmacy because of the large volume of controlled substances they dispensed. (See item **32**)

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. *May 18, Los Angeles Times* – (California) **Electrical explosion jolts Westwood.** An underground electrical transformer vault exploded May 17 in the Westwood section of Los Angeles, California, near the University of California, Los Angeles (UCLA), sending smoke and a plume of flame shooting up from the street and propelling a manhole cover into the back of a Metro bus, Los Angeles city fire officials said. The bus driver was taken to Ronald Reagan UCLA Medical Center and treated for a "stress reaction," a Metropolitan Transportation Authority (MTA) spokesman said. None of

the 25 passengers on board were injured, even though the back of the bus was passing over the manhole when the cover blew, shattering the vehicle's rear windows. The blast, which occurred near Westwood Boulevard and Weyburn Avenue about 9:30 a.m., temporarily halted traffic. The department of water and power said a junction box failure triggered the explosion, and that an investigation is being conducted into what caused the failure. Windows at the Bank of America branch on Westwood were blown out, said a spokesman, whose office is in the building that houses the bank. UCLA officials said the blast interrupted power at the campus for a short time, and that emergency generators took over until power was restored.
Source: http://www.latimes.com/news/local/la-me-westwood-explosion-20110518,0,5831729.story

2. *May 18, Dow Jones Newswires* – (Pennsylvania) **Chesapeake fined $1.09 million In Pa. natural-gas contamination, explosion cases.** The Pennsylvania Department of Environmental Protection (DEP) fined Chesapeake Energy Corp. nearly $1.09 million for contaminating the drinking water of 16 families with natural gas, and, separately, for an explosion at a condensate storage tank. The state agency said that throughout 2010, it investigated complaints of methane contamination in the drinking water of several residential water wells in northeastern Pennsylvania's Bradford County. Investigators determined "improper well casing and cementing in shallow zones" allowed gas from deep basins to seep into drinking water aquifers, the agency said May 17. Chesapeake has agreed to pay the state $900,000 for the contamination, including $200,000 that will go to a state fund that pays for abandoned wells to be plugged. The Oklahoma energy producer also has agreed to set aside an unspecified amount of money to cover the cost of water-treatment equipment at some water wells near its drilling activity. Chesapeake also was fined $188,000 for a February 23 fire at a liquid-natural-gas storage facility in Avella, in southwestern Pennsylvania. That fire injured three workers. "The water well contamination fine is the largest single penalty DEP has ever assessed against an oil and gas operator, and the Avella tank fire penalty is the highest we could assess under the Oil and Gas Act," DEP's head said.
Source: http://www.nasdaq.com/aspx/stock-market-news-story.aspx?storyid=201105171509dowjonesdjonline000362&title=chesapeake-fined-109-million-in-panatural-gas-contaminationexplosion-cases

3. *May 17, Greeley Tribune* – (Colorado) **OSHA cites Vestas Pueblo plant for safety violations.** The federal Occupational Safety and Health Administration (OSHA) has cited Vestas Towers America Inc. in Pueblo, Colorado for 1 willful and 23 serious safety and health violations after a comprehensive inspection of the turbine-making plant. The inspection came after an employee suffered a partial amputation of two fingers and a broken wrist last November. "Vestas Towers America failed to provide its employees with a safe and healthful workplace," the area office director of OSHA, said in a release. "The numerous hazards uncovered during this investigation are totally unacceptable." A spokeswoman for Vestas — American Wind Technology, Inc., responded that safety is a primary concern at Vestas, which also has plants in Windsor and Brighton. OSHA has proposed $164,000 in fines against Vestas. A willful violation is one committed with intentional knowing or voluntary disregard for the law's

requirements, or with plain indifference to worker safety and health. A serious violation occurs when there is substantial probability that death or serious physical harm could result from a hazard about which the employer knew or should have known.
Source:
http://www.greeleytribune.com/article/20110517/BUSINESS/705179976/1002&parentprofile=1001

4. *May 17, Associated Press* – (West Virginia) **Mine security chief charged with 3rd crime stemming from W.Va. explosion investigation.** The head of security at Massey Energy Co.'s Upper Big Branch mine in Montcoal, West Virginia is facing a third federal criminal charge stemming from the nation's deadliest coal mine explosion in decades. A superseding indictment unsealed May 17 accuses the 59-year-old head of security of lying to federal officials investigating the explosion. The man was indicted in February 2010 on charges of lying to agents from the FBI and federal Mine Safety and Health Administration (MSHA) and obstruction of justice. Prosecutors said the man ordered a subordinate to throw away thousands of pages of security documents from the mine. The superseding indictment accuses the man of lying when he told the MSHA and U.S. Labor Department investigators that security guards were forbidden from warning workers underground when government safety inspectors arrived.
Source:
http://www.therepublic.com/view/story/4d7d55534839453ba1717bd772de048f/WV--Mine-Explosion-Superseding-Indictment/

5. *May 17, Charlestown Patch* – (Massachusetts) **Crews still cleaning oil from sunken barge in Navy Yard.** Officials said about 120 gallons of diesel fuel and hydraulic fluid spilled into Boston Harbor in Boston, Massachusetts, off Constitution Road, where a small barge sunk early May 17, according to an official at the Massachusetts Department of Environmental Protection (DEP). Boston fire, police, DEP, and U.S. Coast Guard crews responded. Environmental officials are tried to contain the oil spill on the surface. They have surrounded most of it with a "boom," which floats and prevents oil from migrating, explained a DEP spokesman. A boom has also been placed around the USS Constitution, which is anchored about 200 yards away from the spill. It should protect the historic ship from contact with the fuel. Police said it appears the boat was submerged by a wake.
Source: http://charlestown.patch.com/articles/submerged-boat-in-navy-yard-leaking-oil-in-harbor

For more stories, see items **6** and **52**

[Return to top]

Chemical Industry Sector

6. *May 18, Erie Times-News* – (Pennsylvania) **Fire departments seek answers to dangers faced in Harborcreek industrial blaze.** While investigators continue to search for the cause of a fire that heavily damaged a Harborcreek Township biofuels

plant over the weekend of May 14 and 15, firefighters who answered the call say they want to know what hazards they came in contact with while dousing the flames. The Fairfield Hose Co. fire chief said he will meet with other fire chiefs, county and local officials, and agency representatives at his department's station to discuss the May 14 fire. "I want to go over all of the risks and concerns of all the chemicals in there, to make sure the equipment is safe," he said May 17. "There are a lot of unanswered questions." The 56,000-square-foot plant is home to American Biodiesel Energy Inc. and North American Powder Coatings. Firefighters who were called to the building at 8:18 p.m. May 14 initially fought the fire from outside because of uncertainty about what was stored inside, fire officials said. Three firefighters who responded suffered injuries, including one who received a chemical burn to the foot, officials said. Fire crews have returned to the plant several times since May 14, including three times May 16, to put out hot spots that flared up. Officials with the state department of environmental protection toured the site May 16 and found no clear evidence of any hazardous materials creating an environmental impact, an agency spokeswoman said afterward. Several other firefighters have been sent to receive medical attention for "minor issues," and a lot of firefighting equipment has been damaged, the fire chief said May 17.
Source:
http://www.goerie.com/apps/pbcs.dll/article?AID=/20110518/NEWS02/305179911/-1/NEWSSITEMAP

7. *May 16, Safety.BLR.com* – (National) **Polyurethane foam not a hazmat.** The Pipeline and Hazardous Materials Safety Administration (PHMSA) has denied a petition to regulate polyurethane (PU) foam and certain finished products containing PU foam as hazardous materials for purposes of transportation in commerce. The petition was submitted in October 2006 by the National Association of State Fire Marshals (NASFM). The association stated that regulation of PU foam was essential to the safety of emergency responders and the public, and that responders have the absolute right to information about PU so they may take special precautions at incidents. Specifically, NASFM asked PHMSA to assign a North American Identification Number to PU foam; except shippers/carriers from requiring shipping papers, employee training, specific packaging requirements, and placarding; require carriers to display orange panels with the identification number to identify the presence of PU foam for initial responders; require transportation incidents involving PU foam fires to be reported to PHMSA; publish a safety alert identifying measures initial responders can take to protect themselves and the public during the initial response phase of the incident involving PU foam; and incorporate safety measures published in the safety alert into the Emergency Response Guidebook. PHMSA reported that it received 30 comments on NASFM's petition, and all but the comment from NASFM opposed classifying PU foam as a hazardous material. PHMSA generally agreed with those opposed to listing PU as a regulated hazmat.
Source: http://safety.blr.com/workplace-safety-news/transportation-safety/hazardous-materials-transportation/Polyurethane-Foam-Not-a-Hazmat/

For more stories, see items **16** and **41**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

8. *May 18, Toledo Blade* – (Michigan) **U.S. reports Fermi 2 worker used cocaine.** A letter from the Nuclear Regulatory Commission (NRC) disclosed that an operator for the Fermi 2 nuclear power plant in Frenchtown Charter Township, Michigan who failed a random drug test in May had tested positive for cocaine. A May 16 letter from the acting NRC reactor safety division director to the DTE Energy senior vice president and chief nuclear officer said the agency requested information from the utility regarding the operator's name, responsibilities, and whether he or she "used, sold, or possessed illegal drugs." The federal regulator gave DTE 30 days to respond. The agency's letter said it wants to know if the operator "was at the controls or supervising licensed activities while under the influence of cocaine" and, if so, what procedural errors might have been made. The NRC said it also wanted to know the operator's history of being tested for drugs, and how DTE would handle follow-up testing if that person were reinstated. The letter quotes a DTE official as saying the operator who failed the test was "not on shift" during the time it was administered. The employee's access to the plant was revoked. The government gives utilities 14 days to decide if it wants to suspend or fire operators who fail random drug tests, the NRC said. Under the latest NRC fitness-for-duty tests enacted in 2008, first-time offenders may be able to keep their jobs if they successfully pass treatment programs.
Source: http://www.toledoblade.com/local/2011/05/18/U-S-reports-Fermi-2-worker-used-cocaine.html

9. *May 18, Boston Globe* – (Massachusetts) **Equipment emits radiation at federal building.** A piece of surveying equipment slightly bigger than a shoebox emitted radiation and caused a scare at a federal building in Boston, Massachusetts, May 17, the Boston Fire Department (BFD) said. Firefighters were called to the Tip O'Neill Federal Building near the TD Garden at about 4:10 p.m. after radiation dosimeters of Federal Protective Service officers activated in a first-floor storage room, indicating the presence of radiation, the department said. A Level 3 hazardous materials response, the highest level, was declared, and a day-care center in the building was evacuated. No one was exposed to any radiation, said a BFD spokesman, and no decontamination was necessary. The surveying equipment was being removed by a licensed contractor and the Nuclear Regulatory Commission was called to the scene, the department said.
Source:
http://www.boston.com/news/local/massachusetts/articles/2011/05/18/equipment_emits_radiation_at_federal_building/

10. *May 17, Associated Press* – (Texas; National) **Texas House OKs taking in more radioactive waste.** Texas house members voted May 17 to let a remote low-level radioactive waste site in West Texas bury material from dozens of states. Under the bill approved 108-36, Dallas-based Waste Control Specialists may also set disposal fees for 36 states that were not part of an original deal between Texas and Vermont for the

waste dump in Andrews County, near the New Mexico border. Previously, environmental regulators were to determine the rates. Environmentalists said the bill would bring more radioactive waste to Texas than the state is prepared to handle, and that the liability after the company closes the site will fall to the state. The first low-level radioactive waste could be buried at the site by year's end, a Waste Control Specialists spokesman said. The senate, which approved the bill in April, must vote on it again because of house amendments. One of those requires the company to get an amendment or a modification to its current disposal license to include acceptance of non-party states' low-level radioactive waste. The Texas Low-Level Radioactive Waste Compact Commission had previously approved rules to accept the waste from the 36 states on a case-by-case basis. The low-level waste includes worker clothing, glass, metal, and other materials currently stored at nuclear power plants, hospitals, universities, and research labs. Federal waste will be disposed at the site but in a separate location on the property. The house bill requires that waste from the non-compact states take up no more than 30 percent of the dump's capacity. It also bans waste from foreign countries. The remaining capacity will be split between Texas (56 percent), and Vermont (14 percent).
Source: http://www.forbes.com/feeds/ap/2011/05/17/general-tx-xgr-radioactive-waste_8471526.html

[Return to top]

Critical Manufacturing Sector

11. *May 18, Fort Wayne Journal Gazette* – (Indiana) **Worker dies in fall as roof fails.** A 27-year-old man from Garrett, Indiana, fell to his death May 17 after the roof he was working on collapsed and his safety cable snapped. The man was cleaning the roof of a building in the Iron Dynamics building at Steel Dynamics in Butler at the time of the accident. He was working for the contract company Power Clean. About 9 a.m., the man walked onto a portion of the roof and the roof structure failed, a DeKalb County Sheriff's Department detective said. The man was wearing a harness and lanyard that was attached to a safety cable, but the safety cable snapped under his weight and he fell 100 feet to his death, according to the detective. Other people were working in the vicinity, but no one else was injured in the accident, he said. A company spokesman said Steel Dynamics is investigating the death. The Indiana Occupational Safety and Health Administration said it was informed of the death and sent an investigator to the plant. The investigation is ongoing, an official with the agency said.
Source: http://www.journalgazette.net/article/20110518/LOCAL07/305189970/1043/LOCAL07

For more stories, see items **16** and **29**

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Banking and Finance Sector

12. *May 18, Santa Maria Times* – (California) **Woman faces federal fraud charges.** A Nipomo, California woman who ran a bookkeeping service in Santa Maria pleaded not guilty May 16 to 18 federal counts involving fraudulent tax returns, identity theft and fraudulent loan applications. The 39-year-old woman was arrested May 16 by special agents with the Internal Revenue Service (IRS) Criminal Investigation Division and the FBI at her office in Santa Maria. She is charged with eight counts of making false claims to the IRS, three counts of aggravated identity theft, five counts of making false statements on loan applications, and two counts of making false statements to the FBI. The indictment alleges the woman stole several people's identities, and used their names and Social Security numbers on fraudulent tax returns to obtain refunds from the IRS. The returns allegedly listed income the taxpayers did not earn, and claimed credits for a brother and several children and grandchildren who were not the taxpayers' dependents. The indictment said the fraudulent tax refunds totaled $27,950, but it does not specify if all that money allegedly went to the woman. She is also charged with submitting false personal and corporate income tax returns to Santa Lucia Bank in applications for $1.64 million in loans. The indictment also charges the woman with lying to the FBI twice in 2007 about collaborating with loan officers to create false tax documents and provide false employment verification for borrowers.
    Source: http://www.santamariatimes.com/news/local/crime-and-courts/article_9709d43e-8116-11e0-ac91-001cc4c03286.html

13. *May 17, The Sacramento Bee* – (California) **Eight arraigned in Sacramento-area mortgage fraud scheme.** An indictment returned May 12 by a federal grand jury in Sacramento, California charges eight Sacramento-area residents with wire and mail fraud in connection with an alleged mortgage fraud scheme that involved multiple properties in the Sacramento area and operated from late 2006 to late 2007. The indictment alleges the defendants were responsible for originating more than $16.3 million in residential mortgage loans on 14 homes purchased through so-called straw buyers. All of the homes went into foreclosure, causing losses of approximately $9.6 million, according to a federal Department of Justice news release. According to the indictment, the suspects prepared loan applications containing materially false information straw buyers' income, employment, assets and liabilities, and intent to occupy the residences, and a real estate broker presented the fraudulent applications to lending institutions. They then allegedly created shell companies, or used companies that had no connection with the properties, for use in submitting invoices to falsely claim that they had made repairs to the properties. They then received payments from escrow to which they were not entitled, officials said.
    Source: http://blogs.sacbee.com/crime/archives/2011/05/eight-arraigned.html

14. *May 17, Associated Press* – (Nebraska) **Ex-Nebraska City broker pleads no contest to fraud.** The trial of one of two former Nebraska City, Nebraska brokers accused of bilking more than 150 investors out of more than $20 million abruptly ended May 17 when he pleaded no contest to four charges of securities fraud, prosecutors said. One of the suspects originally faced eight felony counts of intentional securities fraud. As part of the plea agreement, prosecutors amended the charges, so they were based on inadvertent omissions of information, not intentional acts. The man and his accomplice were accused of improperly selling risky investments in several interrelated Florida companies to investors. Prosecutors said the two invested clients' money in high-risk enterprises and never fully explained the risks even though the investors wanted conservative investments because most were near retirement age or already retired. "More than 100 Nebraskans trusted [the two] to invest money they had worked a lifetime to save," the Nebraska attorney general said in a statement. Last month, a federal judge awarded $30 million to more than 200 investors who claimed they had been defrauded by the pair. That ruling was part of a federal class-action lawsuit investors filed in 2007. Several other lawsuits and arbitration claims have been filed against the former brokers.
Source: http://www.businessweek.com/ap/financialnews/D9N9GHVO1.htm

15. *May 16, Softpedia* – (Alabama) **NACHA Spam Gang Starts Using Shortened URLs.** The malware distribution gang that sends spam e-mails purporting to come from the Electronic Payments Association (NACHA) has switched to using shortened URLs in its campaigns. Posing as NACHA is not a new technique. It has been used since November 2009, however, a new campaign has been going strong for the past few weeks. The fake e-mails bear many subjects and the same variety is kept for the spoofed addresses. The e-mails tell recipients their ACH (Automated Clearing House) transfers have been canceled or rejected by their financial institution and directs them to an URL for more details. They read: "The ACH transfer (ID: 65388185980), recently sent from your checking account (by you or any other person), was cancelled by the other financial institution. Please click here [link] to view details. If you have any questions or comments, contact us at info@nacha(dot)org. Thank you for using http://www(dot)nacha.org." The links lead to Web sites that prompt users with updates for Java which are actually variants of the notorious ZeuS baking trojan. According to the director of research in computer forensics at the University of Alabama at Birmingham (UAB), the gang behind this campaign was known for registering hundreds of domain names for each spam run. However, it recently switched tactics and is now abusing almost three dozen URL shortening services, many of which are obscure and are unlikely to respond to abuse reports. The 2mb.eu service was the most abused based on the spam e-mails collected and analyzed by the UAB department. More than 1,000 malicious shortened URLs have been observed in this campaign. Using this method, spammers are able to keep a high level of variation in their e-mails, but a low cost for their campaign.
Source: http://news.softpedia.com/news/NACHA-Spam-Gang-Starts-Using-Shortened-URLs-200695.shtml

For more stories, see items **1**, **25**, and **49**

[Return to top]

Transportation Sector

16. *May 18, Associated Press* – (National) **Mississippi River segment shut, then reopened to barges.** The U.S. Coast Guard (USCG) reopened the swollen Mississippi River north of New Orleans, Louisiana May 17, allowing cargo vessels on the nation's busiest waterway to pass one by one in the latest effort to reduce pressure from rising floodwaters. A 15-mile stretch at Natchez, Mississippi, had been closed earlier in the day, blocking vessels heading toward the Gulf of Mexico and others trying to return north after dropping off their freight. Had the channel remained closed, it could have brought traffic to a standstill up and down the mighty river, which moves about 500 million tons of cargo each year. And the interruption could cost the U.S. economy hundreds of millions of dollars for every day that it idled barges carrying coal, timber, iron, steel and more than half of America's grain exports. USCG officials said wakes generated by passing barge traffic could increase the strain on levees designed to hold back the river. Authorities were also concerned barges could not operate safely in the flooded river, which has risen to the level of some docks and submerged others. It was not clear how long barges would be able to move just one at a time through the section. The river is expected to stay high in some places for weeks. The USCG did not have comprehensive figures on how many vessels were immediately affected, but the agency stopped at least 10 near Natchez. In past closures, those numbers have grown quickly. In 2008, the agency halted 59 ships within a day of shutting down a stretch of the river near New Orleans because of a barge and tanker collision. On a typical day, 600 barges move up and down the river, according to a spokesman for the Mississippi Valley Division of the U.S. Army Corps of Engineers.
    Source:
    http://www.desmoinesregister.com/article/20110518/BUSINESS01/105180348/Mississippi-River-segment-shut-then-reopened-barges?odyssey=mod%7Cmostview

17. *May 18, WTAE 4 Pittsburgh* – (Pennsylvania) **Sky High: passenger on pot forced flight diversion.** A man who caused a cross-country flight to divert to Pittsburgh, Pennsylvania because his medical marijuana cookies made him act erratically has been sentenced to 5 years of probation. The 32-year-old man, apologized May 17 during his guilty plea to a charge of interfering with a flight crew on a US Airways trip from Philadelphia, Pennsylvania to San Francisco, California in January 2010. The U.S. attorney's office in Pittsburgh said his bizarre behavior began after takeoff. The crew reported the San Francisco man went to the bathroom and shouted and threw items before emerging partially clothed, then trying to "elbow" a flight attendant as she escorted him back to his seat. He told FBI investigators who met the flight at Pittsburgh International Airport that he was prescribed medical marijuana for carpal tunnel syndrome but had taken a double dose before boarding the plane. The U.S. district judge noted the man's actions appeared to be an aberration caused by the overdose of prescribed marijuana. In addition to probation, the convict was ordered to pay $6,804 in

restitution to US Airways.
Source: http://www.wtae.com/r/27936844/detail.html

18. *May 17, Los Angeles Times* – (California) **Suspected security breach at LAX briefly delays some passengers.** Passengers at a Los Angeles International Airport terminal, in Los Angeles, California were briefly delayed May 17 when security officials feared a man might be carrying an explosive package, law enforcement sources said. The man had passed his luggage through a scanner and left the area, officials said. Moments later, Transportation Security Administration officials thought the image looked suspicious and began searching for the passenger, an agency spokesman said. Airport police helped in the search, a Los Angeles Airport Police sergeant said.. Bomb squad experts who examined an image of the man's luggage later determined the package was not dangerous and the alert was canceled.
Source: http://latimesblogs.latimes.com/lanow/2011/05/suspected-security-breach-at-lax-briefly-delays-some-passengers.html

19. *May 17, Associated Press* – (National) **Amtrak chief says trains more vulnerable to terrorism than planes, wants to step up patrols.** Amtrak's president said he wants to step up security patrols of the passenger rail network and explore new technologies able to provide advance warning of track tampering following revelations that the terrorist group al-Qaida considered attacking U.S. trains. He told a U.S. Senate panel May 17 that the agency has expanded its use of explosive-sniffing dogs and is in close contact with U.S. and international security agencies. The Amtrak president said promising ultrasonic and laser technologies may enable detection of track problems far ahead of trains. But he cautioned that trains are more vulnerable to attack than planes because terrorists have more ability to access trains and track. He said more patrols of tracks are needed to identify specific points of vulnerability.
Source: http://www.washingtonpost.com/national/amtrak-chief-says-trains-more-vulnerable-to-terrorism-than-planes-wants-to-step-up-patrols/2011/05/17/AFMA6q5G_story.html

20. *May 17, KGUN 9 Tuscon* – (Arizona) **Sun Tran bus evacuated after man talked about bombs.** A Sun Tran bus in Tucson, Arizona was evacuated after a man aboard the bus began talking about bombing and suicide bombing. A Tucson police spokesman said the suspect boarded the bus at the Laos Transit Center near 6th Avenue and Irvington Road. He was carrying a bag and talking to himself about bombs and suicide bombs. The driver of the bus brought the vehicle to a stop near 6th Avenue and 26th Street. He along with all of the riders on the bus exited while the suspect remained aboard. When police arrived, they checked the passenger and bus. However, nothing suspicious was found. The suspect was identified as a man reported missing in California, the police spokesman said.
Source: http://www.kgun9.com/story/14664737/sun

For more stories, see items **1**, **7**, and **52**

[Return to top]

Postal and Shipping Sector

21. *May 17, Oshkosh Northwestern* – (Wisconsin) **Mailbox vandals confess to town of Berlin 'explosives'.** Four juveniles were nabbed by the Berlin Police Department and Green Lake County sheriff's investigators in Wisconsin in connection with a series of mailbox vandalisms, including several that were rigged with bottles containing mixtures of cleaning solvents that exploded. No one was hurt in the May 15 incidents, which law enforcement personnel were alerted to around 10:30 p.m. In all, four explosive devices were manufactured. Three exploded, damaging mailboxes. Officers recovered one that did not explode, according to a news release from the Green Lake County Sheriff's Office. The juveniles confessed their involvement in the vandalism spree. In addition to the mailboxes damaged by the explosions, about 20 others were damaged by juveniles wielding baseball bats. All four juveniles were referred to Green Lake County Social Services.
Source:
http://www.thenorthwestern.com/article/20110518/OSH0101/105180399/Mailbox-vandals-confess-town-Berlin-explosives-?odyssey=tab|topnews|img|FRONTPAGE

22. *May 17, Warwick Beacon* – (Rhode Island) **Car slams into Conimicut Post Office, facility could reopen today.** The Conimicut Post Office in Conimicut, Rhode Island, was surrounded by yellow police caution tape, and was temporarily closed after a vehicle ran into the building May 16. The post office supervisor of customer service, said the building was closed by the city after sustaining damages from the accident, which occurred shortly before noon. The accident is under investigation by the Warwick Police Department. Engineer teams were dispatched to inspect the building and make sure the structure is safe to reopen. "Optimistically, we're hoping to open tomorrow," the supervisor said May 16. "We hope to at least have the box section open so people can get their mail, but if we have to be closed for an extended period of time, which we don't anticipate, we have a contingency plan in place having experienced the floods last year." Broken glass from shattered windows as well as cracks in the brick wall could be seen from the outside of the building, and upon entering, where the mail boxes are located, a crack in the inner wall was visible above the doorway leading into the front desk area.
Source: http://www.warwickonline.com/view/full_story_news/13307024/article-Car-slams-into-Conimicut-Post-Office--facility-could-reopen-today?instance=secondary_stories_left_column

[Return to top]

Agriculture and Food Sector

23. *May 18, Santa Cruz Sentinel* – (California) **Investigators: Roofers sparked cold-storage fire in Watsonville.** Wind likely whipped a spark from a roofer's blowtorch into a hole in a cork-lined wall at the Apple Growers Ice and Cold Storage warehouse, igniting an April 20 blaze that gutted the building in Watsonville, California, a fire investigator said. The 4-alarm fire, which drew dozens of firefighters from 4 counties

and took 3 days to extinguish, was ruled accidental by investigators, a Watsonville fire marshal said. Kuhlman Roofing Co. completed replacement of a roof on a breezeway attached to the rear of the building earlier in the day, he said. The roofing job, the mild, breezy weather, and the dry cork inside the 83-year-old building created "perfect" conditions for the fire, the fire marshal said. S. Martinelli and Co. had about $5.5 million in juice and sparking cider stored at Apple Growers. The juice-maker also had deposits on 6,000 bins of apples stored in the building by independent growers.
Source: http://www.thecalifornian.com/article/20110518/NEWS01/105180319

24. *May 18, Alton Telegraph* – (Illinois) **Firefighters work grease fire at Alton McDonald's.** Firefighters responded May 18 to a suspected grease fire at the McDonald's restaurant in Alton, Illinois. Smoke came through the roof just after 7:30 a.m. Flames were reported on an outside vent, and a hose was needed to address the situation. The building was evacuated, and firefighters were looking at the possibility there was an active fire in the void below the roof. The Madison County Health Department was notified as a matter of routine because of a mandatory inspection necessary after restaurant fires. Morningstar Drive was closed at the parkway to protect hoses run by the firefighters.
Source: http://www.thetelegraph.com/news/firefighters-54077-grease-alton.html

25. *May 17, Temecula Patch* – (California) **Fake bomb robber killed in police shootout.** A man who robbed a Temecula, California, bank with a fake bomb was killed in a shootout with police. The shootout happened around 10 p.m. May 14 inside a busy Ralph's grocery store at 655 S. Grand Avenue in Glendora, according to a local police press release and Los Angeles County sheriff's detectives. Glendora officers confronted the man in the store's parking lot. He then ran inside and fired at the officers, using a checkout stand for cover. Officers returned fire, critically wounding him, police officials said. The man died in a hospital of gunshot wounds at 11 a.m. May 16, according to the coroner's office. Nobody else was hurt in the shootout. The gun battle was the climax of a month-long investigation by Temecula and Glendora investigators, a sheriff's sergeant said in an announcement. The man used a fake bomb when he robbed the U.S. Bank at 33145 Temecula Parkway April 15. Glendora police were also searching for the man on suspicion of committing two armed robberies in their city, one at a Subway restaurant and one at a Kohl's store, according to the sergeant.
Source: http://temecula.patch.com/articles/temecula-bank-robberies-fake-phony-bomb-shootout-glendora-killed-by-police

26. *May 17, Associated Press* – (Ohio) **83,000 chickens die in Darke County barn fire.** Authorities estimate that about 83,000 chickens died May 17 in a barn fire at an egg farm in western Ohio. WHIO-TV said about 70 firefighters were called out shortly before 4 a.m. to fight the fire near Versailles in Darke County. The barn is on a farm owned by Kissinger Brothers Poultry, and it was fully engulfed when firefighters arrived. Fire officials said the barn was a total loss and estimate damage at about $1.5 million. Authorities said the cause of the fire is under investigation.

Source: http://www.timesreporter.com/news_mobile/x243994041/83-000-chickens-die-in-Darke-County-barn-fire

27. *May 17, KHOU 11 Houston* – (International) **Mexican bologna popular with smugglers.** U.S. Customs and Border Protection (CBP) officers discovered nearly 400 pounds of bologna hidden in a pickup truck May 13. People regularly try to smuggle the Mexican lunch meat into the United States for relatives to resell to customers who have a craving for bologna from south of the border. The 33-year-old driver from Ciudad Juarez, Mexico, stashed the 35 rolls of the popular "Chimex" brand bologna behind the seat of his 2003 Dodge Ram pickup truck. "This seizure really stands out because when we seize bologna it is usually a small quantity, or at most a roll or two," the CBP's Santa Teresa port director said. The border crossing is about 13 miles west of El Paso, Texas. According to CBP officials, the bust is the largest in the El Paso area since officers seized 81 rolls weighing 756 pounds at an international bridge in 2003. "This is a prohibited product because it is made from pork and has the potential for introducing foreign animal diseases to the U.S. pork industry," the director said. Authorities said Mexican bologna is sometimes resold in other parts of the country at deli counters in small grocery stores that cater to immigrants or on the black market. This batch of bologna was not refrigerated and could have posed a health risk for consumers. The man was fined $1,000 and released. The contraband bologna was seized by CBP and destroyed.
Source: http://www.khou.com/community/blogs/angela-kocherga/Mexican-Bologna-popular-with-border-smugglers-121960429.html

28. *May 16, Food Business Review* – (National) **Togo's pastrami recalled due to Listeria contamination.** Food company Togo's recalled its pastrami, as the products have the potential to be contaminated with Listeria Monocytogenes. According to the company, the affected products, about 15,900 pounds, had been distributed in California, Arizona, Nevada, Oregon, and Washington. The recalled deli foods comprised Olympic Gold Beef Pastrami, Rose & Shore N.Y. Style Pastrami, Cooked Angus Roast Beef, and Togo's Pastrami. The products, supplied by Rose & Shore Meat Company were investigated by U.S. Food and Drug Administration officials.
Source: http://chilledanddelifood.food-business-review.com/news/togos-pastrami-recalled-due-to-listeria-contamination-160511

For another story, see item **16**

[Return to top]

Water Sector

29. *May 18, Environmental Leader* – (Idaho) **Environmental enforcement: US Silver Corp. settles alleged water violations for $87k.** The U.S. Environmental Protection Agency (EPA) announced that U.S. Silver Corporation, owner and operator of the Coeur and Galena Mines and Mills near Wallace, Idaho, in the state's "Silver Valley," has agreed to pay $87,000 in penalties to settle alleged violations of the Clean Water

Act, Environmental Leader reported May 18. The agreement, detailed in a consent agreement and final order between the EPA and U.S. Silver, resolves the company's alleged National Pollution Discharge Elimination System permit violations and unpermitted discharges at the mines and mills, which the EPA said occurred from 2008 to 2010. EPA officials familiar with the case confirm U.S. Silver's alleged violations included unpermitted discharges of mine tailings, and exceeding the national discharge permit's effluent limits for copper, lead, and mercury multiple times. In addition to paying the $87,000 penalty, U.S. Silver recently made structural improvements to its tailings pipelines to reduce the risk of future spills, and encouraged employees to become more vigilant in preventing and reporting accidental spills.
Source: http://www.environmentalleader.com/2011/05/18/environmental-enforcement-us-silver-corp-settles-alleged-water-violations-for-87k/

30. *May 17, Southern Pines Pilot* – (North Carolina) **Southern Pines reports wastewater spill.** A wastewater spill May 16 in Southern Pines, North Carolina, dumped about 1,500 gallons into Swann's Lake, according to a press release from the town of Southern Pines. The spill took place from a sewer cleanout behind 485 Midland Road that fed through a drainage pipe and into Swann's Lake along Boiling Springs Circle. The discharge was first discovered at 11 a.m. and was abated around 12:30 p.m. The Southern Pines Public Utilities notified the North Carolina Division of Water Quality's Fayetteville regional office May 17 of the wastewater spill.
Source: http://www.thepilot.com/news/2011/may/17/southern-pines-reports-wastewater-spill/

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

[Return to top]

Public Health and Healthcare Sector

31. *May 17, New York Times* – (National) **Fewer emergency rooms available as need rises.** Hospital emergency rooms, particularly those serving the urban poor, are closing at an alarming rate even as emergency visits are rising, according to a report published May 17. Urban and suburban areas have lost a quarter of their hospital emergency departments over the last 20 years, according to the study published in The Journal of the American Medical Association. In 1990, there were 2,446 hospitals with emergency departments in non-rural areas. That number dropped to 1,779 in 2009, even as the total number of emergency room visits nationwide increased by roughly 35 percent. Emergency rooms at commercially operated hospitals and those with low profit margins were almost twice as likely as other hospitals to close, the researchers found. So-called safety-net hospitals that serve disproportionate numbers of Medicaid patients, and hospitals serving a large share of the poor were 40 percent more likely to close. In addition, hospital emergency rooms in the most competitive markets were 30 percent more likely than others to close. The closings take a toll on the quality of care in all emergency rooms, an assistant professor of emergency medicine at the University of California, San Francisco, and the lead author of the study said. "Some people think,

'As long as my emergency room isn't closing, I feel O.K. and protected,' " she said, "But even if they don't lose the E.R. in their own neighborhood, they do experience the effect of fewer emergency rooms — the waits get longer and longer, and people's outcomes get worse."
Source: http://www.nytimes.com/2011/05/18/health/18hospital.html?_r=2

32. *May 17, WCMH 4 Columbus* – (Ohio) **4 Ohio doctors, 1 pharmacy lose licences for controlled substances.** The U.S. Drug Enforcement Administration (DEA) has announced that four doctors and a pharmacy operating in Scioto County, Ohio, have had their DEA Certificate of Registration suspended. The Special Agent in Charge said the DEA served Immediate Suspension Orders (ISO) on four physicians and on Prime Pharmacy of Portsmouth. This administrative action suspends the physicians' and pharmacy's authority to prescribe or dispense Schedule II-V controlled substances. The ISOs are based on a preliminary finding by DEA that the continued registration of the doctors and pharmacy constitutes an imminent danger to public health and safety. According to the DEA, one of the doctor's is one of the largest dispensers of controlled substances in the United States. Two other doctors, both of whom previously worked at Southern Ohio Complete Pain Management in Portsmouth, are responsible for the prescribing of hundreds of thousands of oxycodone products and anti-anxiety medications over the past 2 years. The suspension order at Prime Pharmacy prohibits the employees from continuing to possess, order, or dispense Schedule II – Schedule V controlled substances, such as hydrocodone and oxycodone. In addition, the DEA served notice of an Order to Show Cause on Physicians Pharmacy of Piketon. This is a business that has applied for a DEA Certificate of Registration to handle controlled substances. The physicians and businesses received written notice of the factual and legal basis for this action. All will be given an opportunity for an administrative hearing on the ISOs and the Order to Show Cause. At that time, the physicians, and businesses listed above may contest whether the suspension orders should be lifted, and their certificates of registration should be reinstated.
Source: http://www2.nbc4i.com/news/2011/may/17/4-ohio-doctors-1-pharmacy-lose-licence-controlled--ar-492425/

33. *May 17, Federal Bureau of Investigation* – (New Jersey) **New Jersey couple guilty of selling counterfeit prescription drugs manufactured in India.** A husband and wife from Closter, New Jersey, admitted May 17 to selling counterfeit prescription drugs manufactured in India to customers in the United States, a U.S. attorney said. The woman and her husband, an Indian national, pleaded guilty to one count of unlicensed distribution of pharmaceuticals. A third individual from India pleaded guilty December 15, 2010, and was sentenced March 22 to 8 months in prison. The three were all previously arrested and charged by complaint April 2, 2010. According to documents filed in this case and statements made in Camden federal court: one woman offered "generic" forms of patented pharmaceutical products for sale over the Internet, the source of which was an Indian company. When contacted by an undercover law enforcement officer, she provided a price list of products offering for sale "Generic Viagra," "Generic Cialis," and "Generic Levitra," each of which is a patent-protected erectile dysfunction (ED) drug manufactured in the Untied States. Over the course of

several months, she and her husband negotiated with the undercover officer for the sale of more than 300,000 tablets of counterfeit drugs, including the ED drugs, as well as counterfeit versions of Abilify, Lexapro, and Plavix. All of the counterfeit drugs were shipped from a business in India, where the third individual lived and worked before traveling to the United States on a business visa April 2, 2010 — the day before he was arrested.
Source:
http://7thspace.com/headlines/382690/new_jersey_couple_guilty_of_selling_counterfeit_prescription_drugs_manufactured_in_india_.html

34. *May 15, BBC News* – (International) **Malaria blocks 'super-infection'.** The malaria parasite can ensure it keeps a host body all to itself by preventing further malarial infections, according to international researchers. The parasite initially reproduces in the liver and moves into the blood. A study on mice, published in Nature Medicine, showed the parasite can trigger iron deficiency in the liver and therefore prevent more infections. The researchers were looking at super-infections, when a patient already infected with malaria is infected with another batch of malaria parasites. In experiments on mice, researchers showed that parasites in the blood were able to stimulate the production of the hormone hepcidin, which regulates iron levels. This reduced the level of iron in the liver, preventing other malaria parasites from reproducing in the organ. A doctor from the Weatherall Institute at Oxford University, England, who was part of the Medical Research Council team, said, "Now that we understand how malaria parasites protect their territory in the body from competitor parasites, we may be able to enhance this natural defense mechanism to combat the risk of malaria infections." Malaria is often accompanied by anemia, which is treated with iron supplements. In this study, mice given iron supplements were more susceptible to additional infections. "We may need to look again at the advisability of iron supplementation programs in malaria-endemic regions, as possible increased risk of infection may need to be weighed against benefits," he said.
Source: http://www.bbc.co.uk/news/health-13387983

[Return to top]

Government Facilities Sector

35. *May 17, KWCH 12 Wichita* – (Kansas) **Illegal worker pleads guilty to using false identity to access McConnell Air Force Base.** The U.S. attorney's office in Wichita, Kansas, announced May 16 that a concrete worker employed by Cornejo & Sons, Inc. who tried to gain entry to McConnell Air Force Base using a false identity, pleaded guilty to document fraud. The 34-year-old Mexican national, who was in the United States unlawfully and has worked for Cornejo since 2003, was arrested March 3 by U.S. Air Force security personnel, who believed the man was using a false identity when he reported to the base to do contract work for Cornejo. Agents from Homeland Security Investigations (HSI) investigated and took custody of the man. The plea agreement calls for a sentence of 12 months in federal prison, to be followed by

deportation. Once deported, the man will be banned for life from the United States.
Source: http://articles.kwch.com/2011-05-17/identity_29554307

36. *May 17, Kaspersky Lab threatpost* – (International) **Hack targets NASA's Earth observation system.** A hacker claims that a security hole in a server at NASA's Goddard Space Flight Center has exposed data related to a satellite-based Earth observation system used to aid in disaster relief. The hacker, who uses the handle "Tinkode" has published a screen capture from what he claims is a File Transfer Protocol (FTP) server at NASA's Goddard Center. The hack comes exactly a month after the same hacker exposed a similar hole in a server operated by the European Space Agency. The screenshot from the server at the Goddard Space Center was published May 17. It shows a directory tree from the server, servir(dot)gsfc.nasa.gov, which appears to be connected with NASA's SERVIR program. It is not clear what the purpose of the server is or the nature of the security hole exploited by Tinkode. SERVIR is a joint program between NASA, USAID, CATHALAC, and other non profit groups that uses data from land based radar and geosynchronous satellites to aid in natural disaster analyses, environmental monitoring, health risk assessments, and issues related to climate change and biodiversity.
Source: http://threatpost.com/en_us/blogs/hack-targets-nasas-earth-observation-system-051711

37. *May 17, CNET News* – (Massachusetts) **Massachusetts agency says virus led to data breach.** A virus that infected as many as 1,500 computers in Massachusetts unemployment offices may have allowed criminals to steal Social Security numbers and other data of individuals and businesses, a state agency warned May 17. The W32(dot)QAKBOT data-stealing virus infected computers on the network of the department of unemployment assistance and career services, as well as computers at one stop career centers, according to a statement from the Massachusetts Labor and Workforce Development agency. It was unclear how many individuals and employers might be affected. The virus only affects people who had their files manually accessed and employers who manually filed quarterly statements at an infected computer between April 19 and May 13, the agency said. "There is a possibility that as a result of the infection, the virus collected confidential claimant or employer information. This information may include names, Social Security Numbers, Employer Identification Numbers, email addresses, and residential or business addresses," the statement said. "It is possible that bank information of employers was also transmitted through the virus. Only the 1,200 employers that manually file could be impacted by the possible data breach." The agency is notifying people who may have been affected and is working with the Massachusetts attorney general's office to investigate the breach.
Source: http://news.cnet.com/8301-27080_3-20063712-245.html

38. *May 17, WSBT 22 South Bend* – (Illinois; Michigan) **Illinois man arrested for Watervliet school threats.** Police arrested a 26-year-old Illinois man after they said he made threats against Southwest Michigan high school students. The man is in the Cook County Jail. He faces three charges, including making a threat of terrorism, using a computer during a threat, and unlawfully posting a message. Police said he sent

messages on Facebook threatening students at Watervliet High School in Watervliet, Michigan, but they still do not know what connection he has with the town or school. He could be brought to Michigan as the week of May 16 to face charges.
Source: http://www.southbendtribune.com/sbt-illinois-man-arrested-for-watervliet-school-threats-20110517,0,961879.story

39. *May 17, Hasbrouck Heights Patch* – (New Jersey) **Wood-Ridge Homeland Security agent accused of stealing government property, selling it on eBay.** A 47-year-old Wood-Ridge, New Jersey resident, a longtime supervisory special agent with DHS's Immigration and Customs Enforcement (ICE), was arrested May 17 on charges of theft for allegedly stealing government property and selling it on eBay, according to a statement from the U.S. Attorney's Office - District of New Jersey. The man was scheduled to appear before a U.S. district judge in federal court May 17 in Newark. He was charged with one count of theft of government property, according to the statement released by the U.S. attorney's office. A criminal complaint from the court states the man, who was responsible for obtaining, storing, and controlling ICE equipment at the ICE offices in New York, had regularly stolen property between December 2004 and February 2011. The complaint went on to state the man allegedly maintained an eBay account in the name of an elderly relative through which he sold approximately $37,000 worth of ICE property. The complaint said the stolen items included printer cartridges, film, batteries, camera lenses, combat lights for ICE's M-4 rifles, and an immersion suit designed to prevent hypothermia in cold water. According to the complaint, agents searched the man's Wood-Ridge home in February and found numerous items of ICE property, including personal computers, printers, keyboards, police batons, flashlights, work gloves, safety glasses, life-jackets, helmets, handcuffs, gun holsters, camera lenses, emergency lights and sirens, and 2-way radio systems — items with a total value of about $40,000. The man has been responsible for obtaining, storing, and controlling office equipment and supplies since the 1990s, and has been on administrative leave since February.
Source: http://hasbrouckheights.patch.com/articles/wood-ridge-homeland-security-agent-accused-of-stealing-government-property-selling-it-on-ebay

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

[Return to top]

Emergency Services Sector

40. *May 18, Times of Trenton* – (New Jersey) **Police station and squad cars vandalized, officer assaulted during suspect arrest.** A man who alerted police to trouble through a call box used rocks to smash windows and the windshields of two patrol cars outside the West District police station in Newark, New Jersey, May 17 when no one came out to talk to him, authorities said. The precinct building, which is unoccupied overnight, and the cars sustained thousands of dollars worth of damage, police said. The suspect was taken into custody after having alerted police to trouble through a call box that has a direct line to dispatchers. The building has a security system, but it was not activated,

according to police. The vandalism at the precinct on Artisan Way occurred just before 6 a.m., a police spokesman said. The suspect, who lives in the area, allegedly started pelting the building with softball-sized rocks when no one came out to talk to him. Damaged were the two front doors, a large 8-by-10 foot window, and the windshields. The rocks went through one pane but did not pass through to the other side, the spokesman said. The station was locked, and the suspect did not gain entry inside. Officers sent to the scene confronted the man and placed him under arrest. The suspect was charged with third-degree criminal mischief, aggravated assault on a police officer, and weapons offenses.
Source: http://www.nj.com/news/times/regional/index.ssf?/base/news-23/1305697504184150.xml&coll=5

41. *May 18, Associated Press* – (Alabama) **Ala. county touts 800-megaherz radio system.** In the wake of the April tornadoes that flattened many areas of northern Calhoun County, Alabama, local officials have touted the region's 800-megahertz digital radio system for its effectiveness in coordinating disaster response, Associated Press reported May 18. Communication between various police agencies and first responders in other Alabama cities hit by the tornadoes broke down after the storms knocked out electronic networks. But the top-of-the-line, 10-towered radio system Calhoun and Talladega counties share never faltered, emergency management officials said. The expensive radio system — funded by federal money from the Chemical Stockpile Emergency Preparedness Program as a disaster-response tool to be used in the case of an accident at the chemical weapons incinerator — worked just as officials hoped it would in the face of a large-scale emergency. In a May 16 press release from the Alabama Department of Homeland Security, the governor of Alabama noted the need for a statewide, interoperable communication system for public safety workers. A communication break-down in the wake of disaster can mean confusion, redundancy in search-and-rescue efforts and — at the very worst — the loss of life as a result, police officials said.
Source: http://www.stamfordadvocate.com/news/article/Ala-county-touts-800-megaherz-radio-system-1384634.php

For more stories, see items **6**, **7**, and **31**

[Return to top]

Information Technology Sector

42. *May 18, Help Net Security* – (International) **New vulnerability reporting framework.** The Industry Consortium for Advancement of Security on the Internet (ICASI) published of its Common Vulnerability Reporting Framework (CVRF) Version 1.0. CVRF is an XML-based framework that enables stakeholders across different organizations to share critical vulnerability-related information in an open and common machine-readable format. This format replaces the myriad of current nonstandard reporting formats, thus speeding up information exchange and processing. "CVRF represents a true milestone in industry efforts to raise and broaden awareness of

security vulnerabilities," said the president of ICASI and director of IT Policy and Information Security at IBM. "With the use of CVRF, the producers of vulnerability reports will benefit from faster and more standardized reporting. End users will be able to find, process and act upon relevant information more quickly and easily, with a higher level of confidence that the information is accurate and comprehensive."
Source: http://www.net-security.org/secworld.php?id=11041

43. *May 18, H Security* – (International) **Opera 11.11 closes a critical hole.** With the update to version 11.11, Opera developers closed a critical security hole that enables attackers to inject malicious code. The vulnerability is found in the code for processing framesets: certain frame constructions cause a memory error that eventually allows attackers to inject malicious code.
Source: http://www.h-online.com/security/news/item/Opera-11-11-closes-a-critical-hole-1245275.html

44. *May 16, Softpedia* – (International) **Google denies Chrome sandbox breach.** Google Chrome's security engineers reject the claim that French vulnerability research outfit VUPEN Security broke out of the browser's reputed sandbox. Google's experts argued his was not an attack against the Chrome sandbox itself, but against the Flash Player plug-in bundled with the browser. VUPEN's founder and head of research does not agree with the counter-claims by Google engineers. "Nobody knows how we bypassed Google Chrome's sandbox except us and our customers, and any claim is a pure speculation," he said in a statement. VUPEN has already announced that, according to company policy, it will not disclose details about the exploited vulnerabilities to Google. Instead, the company will share the intelligence with its government customers. Such action is received with much criticism from users, however, as many 0-day exploits are being sold in a legitimate manner.
Source: http://news.softpedia.com/news/Google-Denies-Chrome-Sandbox-Breach-200585.shtml

45. *May 16, Softpedia* – (International) **Security updates for Adobe Audition, Flash Media Server and RoboHelp.** Adobe has released security updates for several products, including Audition, Flash Media Server, and RoboHelp, that address critical vulnerabilities that could compromise systems they run on. Two flaws were patched in Adobe Flash Media Server (FMS) for Windows and Linux, one that could be exploited by attackers to execute arbitrary code on the underlying system. Identified as CVE-2010-3864, the vulnerability is rated as critical and is described as a memory corruption issue. The second flaw, CVE-2011-0612, can lead to a denial of service condition if corrupted XML data is parsed by the server. Adobe said users should install Flash Media Server version 4.0.2 or Flash Media Server version 3.5.6, depending on the branch they are currently running. Two vulnerabilities were also patched in Adobe Audition, the company's audio editing product, that could be exploited to execute arbitrary code. Identified as CVE-2011-0614 and CVE-2011-0615, the flaws are described as memory corruption issues and were discovered by Zero Science Lab and Core Security Technologies. The vulnerabilities can be exploited by convincing victims to open maliciously-crafted Audition Session (.ses) files. Audition Session (.ses) file

format is no longer a supported format beginning with Adobe Audition CS5.5. Only Adobe Audition 3.0.1 and earlier versions for Windows are affected by these vulnerabilities, and the vendor said users should switch to use of the XML session format instead of .ses. Also, a manual patch was released for RoboHelp 8, RoboHelp 7, RoboHelp Server 8, and RoboHelp Server 7, that are affected by a cross-site scripting vulnerability. The flaw, CVE-2011-0613, is rated as important and was reported by Jardine Software Inc. It can be fixed by replacing wf_status.htm and wf_topicfs.htm with the patched versions provided by Adobe.
Source: http://news.softpedia.com/news/Security-Updates-for-Adobe-Audition-Flash-Media-Server-and-RoboHelp-200537.shtml

46. *May 14, Softpedia* – (International) **Apache patches denial of service flaw in HTTP server.** The Apache Project has released version 2.2.18 of its Web server software package to address a vulnerability that could lead to a denial of service condition. The flaw, identified as CVE-2011-0419, is located in the apr_fnmatch() function of the Apache Portable Runtime. It can be exploited remotely by sending specially crafted requests to Apache Web servers configured with mod_autoindex enabled. The Apache developers encouraged users to upgrade. For those who cannot upgrade, Apache said users can mitigate the risks of the vulnerability by setting the ‘“gnoreClient” option of the “IndexOptions” directive. Because the flaw is actually located in the Apache Portable Runtime (APR), which is also used in other projects in addition to the Apache HTTP Server, third-party developers are also advised to upgrade the runtime to version 1.4.4 in their applications. The Apache HTTP Server is the most widely used Web server software and has played an important role in the growth of the World Wide Web.
Source: http://news.softpedia.com/news/Apache-Patches-Denial-of-Service-Flaw-in-HTTP-Server-200418.shtml

47. *May 13, Softpedia* – (International) **Large video game publisher loses data to hackers.** Hackers broke into servers belonging to Eidos Interactive, a reputed game publisher now owned by Square Enix, and stole sensitive data. The hackers who instrumented the attack seem to be affiliated with the Anonymous splinter group that recently took over AnonOps, the hacktivist collective’s IRC network. The target appears to be the Deus Ex Human Revolution Web site. The morning of May 12, the first page of the Web site displayed a message listing the handles and names of the hackers who hacked the site. However, according to IRC logs, the real hackers went by the handles of evo and n` (nigg), two Anonymous members. The handles and names placed on the defaced page were intentional and designed to cause problems for those individuals. The logs leaked by someone who monitored the hackers’ chat room reveale vo had particular plans for the deusex.com site. The techniques described are commonly used by cyber criminals to infect computers in drive-by download attacks, which suggests evo might be familiar with this type of activity. Nigg disagreed with the idea because there was not enough time to put it into practice. Instead, they went for the defacement and leaking of captured information. A torrent was uploaded to The Pirate Bay claiming to contain 370 CVs and the Web site’s user database. Square Enix later confirmed eidosmontreal.com, and two product Web sites were compromised by a

group of hackers. As a result, the company said, up to 350 CVs and 25,000 e-mail addresses used by people to register for updates were stolen.
Source: http://news.softpedia.com/news/Large-Video-Game-Publisher-Loses-Data-to-Hackers-200385.shtml

48. *May 12, SC Magazine Australia* – (International) **AusCERT: Cisco IP phones prone to hackers.** Contact centers and businesses using a Cisco Internet phone were at risk of having communications intercepted and confidential information leaked, a hacking group demonstrated. A security consultant said VoIP phone systems could turn on their users, hacked to become networked listening devices or "bugs," wiretapped remotely, or silenced, blacking out communications. Contact centers that often use Internet-protocol phones because they were cheap to run, were especially at risk, he said. The researcher, director of the penetration tester HackLabs in Sydney, Australia, demonstrated how phone conversations were illictly recorded, injected with sound, or redirected to expensive and elusive offshore premium numbers. Similarly, a distributed denial-of-service attack could take a phone fleet offline, he said, noting he had seen them cripple networks at Australian companies. The weaknesses result from Cisco's reliance on Web functions that gave users functions at the cost of easier penetration for hackers. A Cisco spokesman said it was serious about security and advised users to apply the relevant recommendations in the manual to secure their systems.
Source: http://www.scmagazine.com.au/News/257265,auscert-cisco-ip-phones-prone-to-hackers.aspx

For more stories, see items **15**, **36**, **37**, **49**, and **51**

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

49. *May 18, Help Net Security* – (National) **SpyEye Trojan attacks Verizon's online payment page.** Trusteer discovered a configuration of the SpyEye Trojan targeting Verizon's online payment page and attempting to steal payment card information. The attack took place between May 7 and May 13. The chief technology officer of Trusteer explained that, "SpyEye uses a technique called 'HTML injection' to modify the pages presented in the victim's browser, in this particular case the injected HTML is used to capture credit card related data. The attack is invisible to Verizon customers since the malware waits for the user to logon and access their billing page and only then injects an authentic-looking replica Web page that requests this information. Since the user has logged on and has navigated to the familiar billing page, they have no reason to suspect

this request for payment information is suspicious," she added. This practice allows criminals to commit card non present fraud on the Internet, and also makes it more difficult for banks to identify the source of fraudulent transactions since they cannot trace it back to a specific computer.
Source: http://www.net-security.org/malware_news.php?id=1726

50. *May 17, Television Broadcast* – (National) **FCC cracks down on rogue broadcasters.** Federal Communications Commission (FCC) agents have been busy in May, issuing more than $250,000 in fines as part of an effort to shut down rogue broadcasters. A majority have targeted pirate radio operations. As of May 17, the FCC had issued $258,000 in fines; $141,000 for operation of unlicensed radio transmitters. On May 5, alone, the commission fined five pirates a total of $50,000. Other violations involve failure to maintain functional Emergency Alert System equipment, inadequately maintained transmitter and tower facilities, excessive power levels, and improper record-keeping. Piracy was most prevalent in the eastern portion of the United States.
Source: http://www.televisionbroadcast.com/article/120506

51. *May 17, IDG News Service* – (International) **Some sites struggle to stay up due to Heroku attack.** A potential Denial-of-service attack (DDoS) on Heroku, the Ruby platform-as-a-service provider now owned by Salesforce.com, is creating availability issues for its customers. The problems started May 16 when Heroku reported a small number of users, primarily those that point a root domain to Heroku via static Internet Protocol addresses, were getting connection errors. Via its status page, Heroku later told customers it was working with its network service provider to mitigate availability issues coming from what it believed was a distributed DDoS. "The current attack protection procedures have reduced the effects of this attack to intermittent issues," the status page said. The company Loqize.me, which uses Heroku and had some issues, advised customers via Twitter to try reloading if they were unable to access the site. Another company, Rexly, apologized to customers having trouble using its service due to Heroku's "hiccups." NationBuilder.com warned users about issues related to Heroku's service.
Source:
http://www.computerworld.com/s/article/9216795/Some_sites_struggle_to_stay_up_due_to_Heroku_attack

52. *May 17, Associated Press* – (International) **US official: solar storms expected to peak in 2013 with potentially devastating effect.** A senior official at the U.S. National Oceanic and Atmospheric Administration (NOAA) said solar storms pose a growing threat to critical infrastructure such as satellite communications, navigation systems and electrical transmission equipment. The NOAA Assistant Secretary said the intensity of solar storms is expected to peak in 2013 and countries should prepare for "potentially devastating effects." Solar storms release particles that can temporarily disable or permanently destroy fragile computer circuits. A former NASA astronaut who in 1984 became the first woman to walk in space, told a United Nations weather conference in Geneva on May 17 that "it is not a question of if, but really a matter of when a major

solar event could hit our planet."
Source: http://www.washingtonpost.com/world/us-official-solar-storms-expected-to-peak-in-2013-with-potentially-devastating-effect/2011/05/17/AF9lHh5G_story.html

[Return to top]

Commercial Facilities Sector

53. *May 18, Philadelphia Inquirer* – (Pennsylvania) **7 cars set on fire in West Philly.** Residents of one West Philadelphia, Pennsylvania neighborhood awoke May 18 to find 7 motor vehicles parked on the street had been set on fire. The fiery outbreak, including a string of cars on Georges Lane at Arlington, and a cluster a block away at West Berks Street, was ruled an arson by fire marshals. Firefighters got the call at 4:34 a.m. and quickly put out the fires. A local resident said she was startled awake by an explosion about 4:30 a.m. and feared more blasts would follow. Police said 5 vehicles on the 1900 block of Georges Lane, 1 on the 1800 block of Georges Lanes, and 1 on the 5300 block of West Berks Street were damaged by fire.
Source: http://www.philly.com/philly/news/122141904.html

54. *May 18, Quincy Patriot Ledger* – (National) **Man crushed, killed by winch at marina.** Officials May 18 are investigating a deadly incident at a marina in Winthrop, Massachusetts. The victim was at the marina May 16 to help a woman launch a boat when the winch suddenly gave way. "It appears two bolts failed, causing the machine to lurch to the right, pinning the gentleman against the dwelling," said the Winthrop fire chief. The Winthrop building inspector said the winch required a permit, but none were on file. "It tells me it probably wasn't reviewed by the building inspector at that time, and probably didn't have any engineering as to properly load that winch back to the earth," he said. The building inspector said the bolts were not enough to secure the 3,500-pound winch. Seacoast Contractor, the company that built the pad said the previous building inspector did not require a permit. State police have taken the bolts to be inspected. The Occupational Safety and Health Administration also is investigating.
Source: http://www.patriotledger.com/topstories/x1292317682/Man-crushed-killed-by-winch-at-marina

55. *May 17, WMAQ 5 Chicago* – (Illinois) **No injuries in West Side industrial fire.** No one was injured as 125 firefighters battled a fire at a west side Chicago, Illinois asphalt company May 17. A still and box alarm was called for a fire in the 4700 block of West Roosevelt Road shortly before 1 p.m., a fire media affairs spokesman said. A second alarm was called about 25 minutes later. Several tankers were on fire and 125 firefighters helped to extinguish the blaze, he said. The fire was struck out about 1:50 p.m., the spokesman said.
Source: http://www.nbcchicago.com/news/local/west-side-fire-122038194.html

For more stories, see items **9** and **57**

[Return to top]

National Monuments and Icons Sector

56. *May 18, Associated Press* – (Arizona) **Arizona wildfire increases to nearly 31,000 acres.** As of May 18, the wildfire burning in Arizona near the Cochise County community of Portal has burned 31,000 acres of dead brush, grass, and trees. The U.S. Forest Service (USFS) said the Horseshoe Two wildfire is 25 percent contained. Almost 800 firefighters are battling the wildfire. The USFS said crews were working in extreme terrain making it difficult to construct a fire line capable of stopping the fire. Winds were gusting May 17 up to 40 mph early and then calmed to 35 mph that afternoon. Most of the active fire is located within the wilderness boundary. Source: http://www.kold.com/Global/story.asp?S=14667737

[Return to top]

Dams Sector

57. *May 18, Austin American-Statesman* – (Texas) **Engineers find large cracks in Barton Springs Pool dam.** Cracks as long as 15 feet have formed in the downstream dam of Barton Springs Pool in Austin, Texas, and an engineering firm estimates it will cost $130,000 to fix them. The city's parks and recreation department hopes to make the repairs as soon as possible, but said the cracks do not pose an immediate risk to the dam, water quality, or the pool. According to the engineering report, the condition of part of the downstream dam is "unsatisfactory" because it has two 15-foot horizontal cracks leaking water. Filling the cracks with grout or epoxy could keep the dam in good shape for another two decades, the report said. If left as is, the leaking water could cause steel rebar inside the concrete to rust and expand, causing further problems, a parks department division manager said. The engineers said damage likely would not occur for another 5 to 50 years, but they urged the city to fill the cracks sooner. The engineer said the pool's upper dam, near the shallow end, is fine, the division manager said. Both dams are 80 years old, and the cracks are the result of basic wear and tear. Source: http://www.statesman.com/news/local/engineers-find-large-cracks-in-barton-springs-pool-1481760.html

58. *May 18, Reuters* – (International) **China acknowledges downside to Three Gorges dam.** China's landmark Three Gorges Dam project provides benefits to the Chinese people, but has created a myriad of urgent problems from the relocation of more than 1 million residents to risks of geological disasters, the Chinese government said May 12. The statement from China's State Council, or cabinet, marked a rare acknowledgment of the issues that have shadowed the world's largest dam, an engineering feat designed to tame the Yangtze River that snakes from the Tibetan plateau to Shanghai. China's premier presided over the meeting that produced the statement, which also said problems existed for down-river transport, irrigation and water supplies. Problems emerged at various stages of project planning and construction but could not be solved immediately, and some arose because of "increased demands brought on by economic and social development," the statement said. The government said it would continue to address the problems caused by the dam, and vowed to set-up disaster alert systems and

increased funding for environmental protection. The dam has cost over $37.47 billion and forced the relocation of 1.3 million people to make way for the reservoir. Towns, fields and historical and archaeological sites have been submerged, just as pollution and geological threats have risen around the slopes around the 410-mile reservoir.
Source: http://www.reuters.com/article/2011/05/18/us-china-dam-idUSTRE74H30720110518?rpc=401&feedType=RSS&feedName=GCA-GreenBusiness&rpc=401

For another story, see item **16**

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

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